Enabling Sustainability Due Diligence in Value Chains Through DLT-Based Governance

Jan Zedel[1][a] and Felix Eppler[2][b]
[1]*Department of Information Systems, Freie Universität, Berlin, Germany*
[2]*Department of Business Management, Julius Maximilians Universität, Würzburg, Germany*

Keywords: Sustainable Supply Chains, Corporate Sustainability Due Diligence Directive, CSDDD, Supply Chain Due Diligence, Distributed Ledger Technology, Token Curated Registries.

Abstract: The European Union's Corporate Sustainability Due Diligence Directive (CSDDD) represents a transformative approach to ensuring sustainable and ethical supply chain practices. However, the directive introduces complexities and significant efforts in the compliance processes of affected companies. This paper explores the question of how decentralized resource pooling can lead to more efficiency and lower costs in the compliance processes of the CSDDD. We propose a novel solution leveraging distributed ledger technology (DLT), specifically a token-curated registry (TCR) solution augmented with shielded transactions to ensure participant anonymity and trust. Our proposed approach could reduce redundancies, increase transparency, and facilitate a more robust risk analysis over the whole value chain. Our paper follows a design science research approach where we (1) identify the challenges posed by companies that fall under the new CSDDD regulation framework, (2) define the objectives of a distributed ledger-based solution and (3) design and develop a technical framework based on a TCR to handle parts of the CSDDD in an efficient and cost-effective way, setting a precedent for future empirical studies and practical implementations in the field of distributed ledger-based information systems in the field of sustainability corporate governance.

1 INTRODUCTION

Regulators and government bodies around the world are increasingly addressing corporate sustainability issues in an effort to align business activities with international sustainability initiatives (i.e., the United Nations Sustainable Development Goals (SDGs) and the Paris Agreement on climate change). In Europe in particular, the Corporate Sustainability Due Diligence Directive (CSDDD) is becoming a key regulatory framework for promoting corporate responsibility across value chains in the EU and beyond (Lafarre, 2023).

The CSDDD, proposed by the European Commission in February 2022 and consolidated by a preliminary political agreement on December 14, 2023, sets out a comprehensive approach to enhance environmental and social impacts throughout supply chains, targeting both EU companies and non-EU companies operating in the EU. It introduces phased compliance obligations, initially targeting companies with significant staff and turnover, and outlines a wide range of requirements - from identifying and mitigating adverse human rights and environmental impacts to establishing robust reporting mechanisms on due diligence measures (European Parliament, 2023; Sørensen, 2022).

Under the CSDDD, companies are generally required to:

1. Identify actual or potential adverse human rights and environmental impacts in their supply chain.
2. Take actions to prevent or mitigate potential negative impacts.
3. End or minimize actual negative impacts.
4. Establish a supply chain workers' rights complaints procedure.
5. Implement a climate transition plan aligned with the Paris Agreement for certain large companies.
6. Monitor and report publicly on the effectiveness of their due diligence policies and measures.

[a] https://orcid.org/0000-0002-6009-9722
[b] https://orcid.org/0009-0000-1833-8446

Zedel, J. and Eppler, F.
Enabling Sustainability Due Diligence in Value Chains Through DLT-Based Governance.
DOI: 10.5220/0012633700003690

In *Proceedings of the 26th International Conference on Enterprise Information Systems (ICEIS 2024) - Volume 2*, pages 696-702
ISBN: 978-989-758-692-7; ISSN: 2184-4992

Failure to comply with the CSDDD could result in penalties, including fines of up to 5% of global revenue, and has implications for companies' operations and supply chains, necessitating significant adjustments for businesses to meet these new standards (European Comission, 2022). Admittedly, the detailed criteria for full compliance with the CSDDD remain somewhat vague and are likely to be clarified once the directive enters into force and is transposed into national law by EU member states.

Some EU member states, however, have already implemented their own legislation on sustainability due diligence in supply chains. These include Germany, which has introduced its own *Act on Corporate Due Diligence Obligations in Supply Chains* (Lieferkettensorgfaltspflichtengesetz, LkSG), providing valuable insights and precedents for specific measures that companies must undertake to ensure compliance with environmental and social standards in their supply chains (Weihrauch et al., 2023; Rühmkorf, 2023).

Based on the high-level requirements of the CSDDD and the more specific guidelines of the LkSG, the practical difficulties are many: ensuring comprehensive risk analysis, implementing preventive and corrective measures, extending due diligence to indirect suppliers, and maintaining robust documentation of compliance. These requirements require significant resource allocation and carry the risk of severe penalties for non-compliance, creating an urgent need for innovative solutions that can effectively address these complexities. Our paper and proposed proof-of-concept application seek to pioneer a systematic approach to managing compliance due diligence processes across the supply chain. This application not only facilitates compliance with LkSG and CSDDD requirements but also demonstrates the potential for scalable, innovative solutions in navigating the landscape of corporate sustainability regulations.

2 METHODOLOGY

The research findings presented here are based on a Design Science Research (DSR) methodology outlined by Hevner et al. (Hevner et al., 2004). The primary objective is to delineate prescriptive knowledge related to the development of a distributed ledger (DLT)-based application tailored to the specified use case of providing a technical framework to support the fulfillment of the requirements of the CSDDD. The procedural approach follows the principles of a generic DSR research process, as outlined by Gleasure (Gleasure, 2013). This methodology establishes a symbiotic relationship between the clarification of the problem and the articulation of its corresponding solution, thereby contributing substantively to the design knowledge within the domain, as stipulated by Venable (Venable, 2006).

The initial phase of the research involves the identification and specification of requirements. This foundational step is integral to the subsequent iterative process, wherein design principles are judiciously applied to delimit the solution space progressively. Noteworthy in this endeavor is incorporating additional conceptual frameworks strategically employed to address and resolve any potential conflicts. This novel integration represents a significant augmentation to the originally posited design principles for the application domain.

The resultant outcomes are systematically formalized through a comprehensive description of a so-called token-curated registry (TCR) model. Subsequently, a validation process follows, wherein meticulous verification is conducted to ensure adherence to the specified requirements. Following the taxonomy articulated by vom Brocke and Maedche (Vom Brocke and Maedche, 2019), the presentation of the research outcomes is organized into six distinct dimensions. The DSR grid system is employed to categorize and articulate the content presentation in a structured manner, thereby enhancing clarity and comprehensibility.

Problem Description
Companies operating within the European Union face escalating compliance challenges due to the impending enforcement of the CSDDD and existing national regulations like the LkSG. The rigorous requirements of these directives include identifying and mitigating adverse impacts on human rights and the environment, establishing complaint procedures, and aligning with climate goals. This surge in regulatory demands and potential fines for non-compliance poses a significant burden, necessitating substantial resource allocations for due diligence processes. Addressing requirements such as regular risk analyses, implementation of preventive and corrective measures, and extended due diligence to indirect suppliers presents intricate challenges.

Input Knowledge
The requirements outlined in the LkSG serve as the foundational basis for deriving technical specifications. These requirements function as fundamental knowledge for conceptualizing an application capable of fulfilling the specified criteria.

Key Concepts
The model adapted for the specific use case is a TCR implemented within a DLT environment, including Zero-Knowledge Proofs (ZKPs) for privacy purposes.

Solution Description
The application is exemplified through two core scenarios, the processes and users of which will be elucidated in order to explicate the fundamental logic for a prospective implementation as smart contracts.

Output Knowledge
The elucidated scenarios serve as illustrative instances demonstrating the application's contribution to the satisfaction of stipulated requirements. Furthermore, this discourse encompasses an examination of the ramifications and prospective developmental trajectories rooted in the underlying conceptual framework. The delineated solution domain substantiates the formation of the resultant design knowledge.

3 INPUT KNOWLEDGE

In the German Supply Chain Due Diligence Act (BfJ, 2021)), the due diligence obligations are:

- (1) Establishment of a risk management system to manage risks in supply chains.
- (2) Designation of internal roles responsible for ensuring compliance with these due diligence obligations.
- (3) Conducting regular risk analyses to identify potential risks.
- (4) Issuance of a policy statement publicly declaring a commitment to uphold human rights and environmental standards.
- (5) Implementation of preventive measures both in their own business operations and with direct suppliers.
- (6) Implementation of corrective measures in response to identified violations.
- (7) Creation of a mechanism for reporting and addressing grievances within the supply chain.
- (8) Extension of due diligence to encompass risks associated with indirect suppliers.
- (9) Maintaining records of due diligence activities and publicly reporting on them.

While some of the requirements listed in the LkSG, such as the establishment of risk management (1), the designation of internal responsibility (2), and the issuance of a policy statement (4), may be relatively manageable internally, the others pose more complex challenges.

Our application aims to improve efficiency, transparency, and compliance in the value chain by leveraging the added values offered by DLT-based TCR. We are focusing on the specific challenges posed by requirements (3), (5), (6), (7), (8), and (9). Our approach emphasizes not only meeting the regulatory standards but also driving efficiency and sustainability in supply chain operations.

4 KEY CONCEPTS

The centerpiece of our research is designing and developing a DLT-based TCR system tailored specifically for the decentralized risk analysis of suppliers under the CSDDD. DLT generally promises to increase transparency, efficiency, and accountability across complex supply chain networks (Kumar and Sahu, 2023), which is critical to meeting the demands of today's sustainability regulations, but research has mainly focused on the product level (Gomes and Romão, 2023; Marjanović et al., 2023) rather than the specific actors involved in a supply chain itself. Our approach is conceptualized to tackle the inefficiencies in the current due diligence processes by leveraging the inherent features of DLT and the novel mechanics of TCRs.

At its core, the TCR is a list of suppliers maintained by a network of companies (token holders) with a vested interest in the accuracy and integrity of the registry. Companies can submit assessments of their suppliers, which are then vetted and curated by other token holders. The use of tokens creates an economic incentive for token holders to curate the list responsibly since the value of their tokens is intrinsically linked to the quality of the TCR.(Kaur and Visveswaraiah, 2021) The proposed application is composed of several key components and features that facilitate decentralized risk analysis:

- **Token Economy.** Tokens are used as a mechanism to incentivize honest participation and curation of the registry.
- **Voting Mechanism.** Token holders participate in governance by voting on the inclusion or exclusion of suppliers based on their compliance assessments.

- **Stakeholder Engagement.** The system encourages active engagement from all stakeholders, including companies, suppliers, and third-party auditors.

The system integrates cryptographically secured proofs to ensure privacy and minimize moral hazard. ZKPs allow a company to prove that its assessment is valid without revealing the underlying data. Moreover, transactional data is shielded to prevent the attribution of alterations in token balances or voting activities to a specific participant within the network (Ren et al., 2019). This ensures that while the integrity of the risk analysis is verifiable, the sensitive details remain confidential, thus preventing any potential biases or retaliatory actions.

5 SOLUTION DESCRIPTION

We adopt the TCR model, as elucidated by Goldin (Goldin, 2017), to suit our specific use case. The TCR is collectively maintained by a set of users who are either suppliers or customers within a designated supply chain. The registry comprises curated suppliers evaluated by participating customers in accordance with CSDDD regulations. These users can assume three distinct roles within the application, namely:

1. Applicant (Supplier). The applicant, a supplier, seeks inclusion in the system and subsequent listing on the registry.
2. Voter (Customer). The voter participates in voting scenarios, expressing assessment results on whether a supplier should or should not be listed on the registry.
3. Challenger (Customer). The challenger has the capacity to instigate a vote by asserting that an established supplier should be excluded from the registry.

The application facilitates two distinct scenarios, where a supplier applies to be on the curated list (Figure 1), or a customer challenges an existing supplier entry (Figure 2). Both processes initiate a voting period during which customers may cast votes on the inclusion or exclusion of the supplier from the registry.

Perspective of the Applicant

Scenario ”Application”: In the initial stage, the applicant requests inclusion in the list of suppliers meeting the requirements outlined in CSDDD regulations. The applicant is required to deposit tokens as a stake, which remains locked for the entire duration the supplier chooses to be on the list. The submission of the application triggers a voting period during which voters determine the supplier’s inclusion. If the applicant is rejected, the tokens are refunded; if accepted, the applicant is incorporated into the list, and the tokens remain staked.

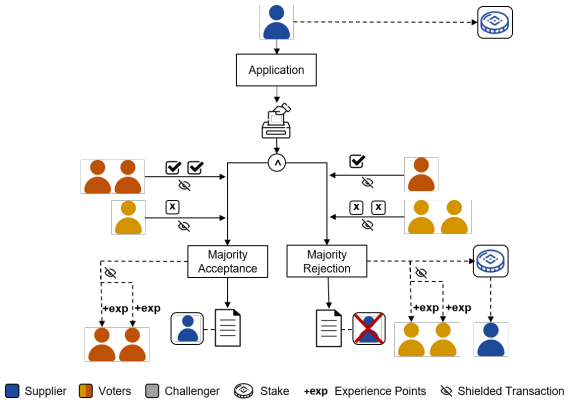

Figure 1: Application.

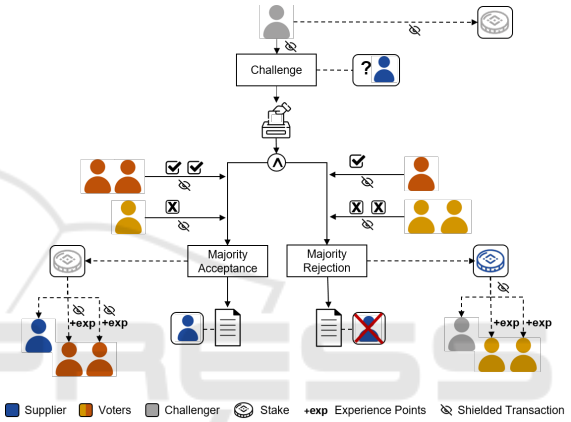

Figure 2: Challenge.

Scenario ”Challenge”: When a supplier faces a challenge for exclusion from the list, a voting period commences, during which voters decide on the supplier’s status. If the majority votes for exclusion, the supplier forfeits tokens to the challenger and voters. If the majority votes for the supplier’s retention on the list, the supplier gains a portion of the tokens staked by the challenger.

Perspective of Voter

Scenario ”Application”: Voters participate in a vote to determine whether a supplier should initially be included in the list. Voters are entitled to vote after conducting a risk assessment based on CSDDD regulations. The vote should align with the outcome of their assessment. Voters favoring the majority vote earn experience points, granting them in-

creased weight in future votes, thereby incentivizing continued participation.

Scenario ”Challenge”: In the event of a challenge, participating voters reassess the challenged supplier and vote accordingly. Winning voters in the majority vote share the stake of either the supplier or the challenger in equal parts. Additionally, participation in the vote earns experience points.

Perspective of Challenger

Scenario ”Challenge”: Instances may arise where a customer suspects a listed supplier’s non-compliance with CSDDD regulations and advocates for their exclusion. By providing a stake and initiating the challenge, the customer assumes the role of a challenger. If the majority votes to ban the challenged supplier, the challenger is remunerated, akin to voters. Conversely, if the majority votes to retain the supplier on the list, the challenger loses their stake to the voters and the challenged supplier.

6 OUTPUT KNOWLEDGE

6.1 Evaluation

In the following, we argue how the proposed application supports the fulfillment of the LkSG and, by extension, the CSDDD requirements:

1. **Facilitation of Comprehensive Risk Analysis.** The presented application advocates for the systematic conduct of risk analyses (3). Customers are incentivized, both monetarily and non-monetarily (in the form of experience points), to monitor their suppliers. In instances where uncertainties arise concerning a supplier, it is imperative to discern and identify associated risks. This discernment serves as a crucial factor in making decisions that yield profitability or, in the case of the challenger, prevent potential losses. The described mechanisms aim to harness collective intelligence from various stakeholders, enhancing the accuracy and robustness of risk assessments.
2. **Streamlining of Preventive and Remedial Measures.** The application functions as a risk mitigation measure (5), as suppliers face the potential loss of funds at any given moment, thereby incentivizing their consistent adherence to specified requirements. Moreover, the exclusion of a previously listed supplier through a formal election mechanism serves as a remedial measure (6) in instances where users identify violations. The application enables companies to respond promptly and efficiently to identified risks and violations.
3. **Efficient Complaints Management.** Upon the initiation of a voting period by a challenger, a notification is visible on the ledger to inform other users that a specific supplier may potentially fail to meet the defined requirements. Consequently, the execution of a challenge functions as a reporting mechanism, wherein the adequacy of a supplier is subject to reevaluation. Notably, the notification within the application is characterized by transparency and immediacy, ensuring that all users are promptly informed of the pertinent developments (7).
4. **Expansion of Due Diligence to Indirect Suppliers.** Due to the specifications inherent in the distributed ledger, the application facilitates the ability of users to access the risk assessments pertaining to all suppliers recorded within the system. Consequently, risks affiliated with indirect suppliers can be passively appraised (8). Nevertheless, it is imperative to emphasize that such an assessment does not absolve any company from the responsibility of conducting its individual due diligence.
5. **Robust Documentation and Reporting Capabilities.** The inherent data structure of the distributed ledger facilitates the meticulous traceability of activities pertaining to risk assessments (9). Furthermore, the dissemination of the data affords a specific degree of persistence, and the information is openly accessible within the supply chain network, thereby permitting any interested party to generate reports on activities.

An assessment was undertaken through a qualitative approach involving a series of interviews with three distinguished experts in the realm of sustainable supply chain management (SSCM) within manufacturing industries. The ensuing feedback can be categorized into three distinct dimensions:

1. **Conceptual Soundness.** The proposed application appears to offer a viable framework for addressing the requirements of the LkSG and potential challenges related to CSDDD compliance. Particularly, the economic incentive structures embedded within the application may facilitate a transparent and collaborative approach in assessing social or environmental risks associated with suppliers. Nevertheless, the determination of remuneration for users of the application necessitates careful consideration to avoid favoring a specific equilibrium. Additionally, there exists ambi-

guity regarding whether suppliers would perceive the benefits of participating in such a system, given the perpetual jeopardy of financial losses contingent upon majority votes from customers. The advantages for a supplier, arising from an enhanced appeal to new customers through participation, must outweigh the associated risks of potential monetary losses.

2. **Practical Usability.** Incorporating the application into current company structures poses a significant challenge. Typically, there is a long-term commitment to existing solutions. New applications need to work well with the systems already in place. Despite many proofs of concept, the adoption of DLT in industrial applications is still a ways off. Systems should be implemented in a way that is easy for users, and users should be able to understand the technology involved.
3. **Risk Analysis Efficacy.** The collaboration involved in the proposed approach may encourage suppliers to more willingly or strictly follow regulations. This increased compliance can be linked to the reduced chance of unnoticed rule violations, thanks to multiple risk assessments. Combining assessments from various customers also strengthens the overall evaluation of suppliers. Moreover, the resulting transparency builds trust among everyone involved, enhancing the effectiveness of decision-making and allowing for efficient reassessment.

7 CONCLUSIONS

The proposed application presents a new approach to managing risk analysis in compliance with the CSDDD. The implementation of the TCR system has the potential to optimize the CSDDD compliance processes by significantly reducing redundancies in supplier risk analysis. Through a decentralized and collaborative approach, companies will be able to share and access supplier assessments, thereby improving efficiency, transparency, and potentially the overall quality of risk analysis.

The integration of TCRs and ZKPs into compliance processes underscores the transformative role of information systems in sustainability efforts. This research exemplifies how innovative applications of distributed systems can address complex challenges in supply chain management, setting a precedent for further explorations in the domain.

While our study offers valuable insights, it is not without limitations. The evaluation is based primarily on expert feedback, which, while expertly informed, may not fully capture the practical complexities of implementing the TCR system in diverse corporate environments. Additionally, the proposed design has not yet been empirically tested in a real-world setting, which is necessary to validate its efficacy and feasibility.

Future research should aim to empirically test the TCR system in a real-world environment to validate the findings. Moreover, it is imperative to develop mechanisms to ensure good acting within the system and discourage malicious behavior. Potential avenues include incorporating monetary or reputational stakes for users, where non-compliance or bad acting could lead to tangible losses, thereby aligning the interests of all consortium members with the overarching goals of the application.

Future iterations could incorporate stakeholder-driven governance models, reward users' contributions and reliability, and penalize dishonest behavior. Exploring the use of smart contracts to enforce rules and automate incentive structures could provide a robust framework for maintaining integrity within the system.

While there are challenges to be addressed and tested, the potential benefits for CSDDD compliance and the broader field of information systems are substantial. By continuing to explore and refine this approach, the corporate world may benefit from more resilient, transparent, and efficient sustainability practices.

REFERENCES

BfJ (2021). Gesetz über die unternehmerischen Sorgfaltspflichten zur Vermeidung von Menschenrechtsverletzungen in Lieferketten (Lieferkettensorgfaltspflichtengesetz - LkSG) § 3 Sorgfaltspflichten. https://www.gesetze-im-internet.de/lksg/_-_3.html, accessed on 2024-01-03.

European Comission (2022). Proposal for a Directive of the European Parliament and of the Council on Corporate Sustainability Due Diligence and amending Directive (EU) 2019/1937. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX\%3A52022PC0071, accessed on 2024-01-03.

European Parliament (2023). Corporate due diligence rules agreed to safeguard human rights and environment. https://www.europarl.europa.eu/news/en/press-room/20231205IPR15689/corporate-due-diligence-rules-agreed-to-safeguard-human-rights-and-environment, accessed on 2024-01-03.

Gleasure, R. (2013). What is a 'wicked problem' for is research? In *Proceedings of the 2nd international SIG Prag workshop on "IT Artefact Design & Workpractice Improvement"*. The 2nd international SIG Prag

workshop on "IT Artefact Design & Workpractice Improvement" : ADWI 2013 ; Conference date: 05-06-2013 Through 05-06-2013.

Goldin, M. (2017). Token-Curated Registries 1.0. https://medium.com/@ilovebagels/token-curated-registries-1-0-61a232f8dac7, accessed on 2024-01-03.

Gomes, J. and Romão, M. (2023). Supply chain traceability using blockchain. *Operations Management Research*.

Hevner, A. R., March, S. T., Park, J., and Ram, S. (2004). Design science in information systems research. *MIS Quarterly*, 28(1):75–105.

Kaur, J. and Visveswaraiah, B. (2021). A brief survey of token curated registries. *Emerging Technologies in Data Mining and Information Security: Proceedings of IEMIS 2020, Volume 1*, pages 189–202.

Kumar, A. and Sahu, A. (2023). Blockchain applications in supply chain management: a systematic review of reviews. *Global knowledge, memory and communication*.

Lafarre, A. (2023). Mandatory corporate sustainability due diligence in global value chains: The long-awaited european solution compared to existing international standards. *Ondernemingsrecht*, 2023(5):229–237.

Marjanović, J., Dalcekovic, N., and Sladić, G. (2023). Blockchain-based model for tracking compliance with security requirements. *Computer Science and Information Systems*.

Ren, Z., Zha, X., Zhang, K., Liu, J., and Zhao, H. (2019). Lightweight protection of user identity privacy based on zero-knowledge proof. In *2019 IEEE International Conference on Systems, Man and Cybernetics (SMC)*, pages 2549–2554. IEEE.

Rühmkorf, A. (2023). Article: The german supply chain law: A first step towards more corporate sustainability. *European Company Law*, 20:6–14.

Sørensen, K. E. (2022). Corporate sustainability due diligence in groups of companies. *European Company Law*.

Venable, J. (2006). The role of theory and theorising in design science research. In *Proceedings of the 1st International Conference on Design Science in Information Systems and Technology (DESRIST 2006)*, pages 1–18. Citeseer.

Vom Brocke, J. and Maedche, A. (2019). The dsr grid: six core dimensions for effectively planning and communicating design science research projects. *Electronic Markets*, 29:379–385.

Weihrauch, D., Carodenuto, S., and Leipold, S. (2023). From voluntary to mandatory corporate accountability: The politics of the german supply chain due diligence act. *Regulation & Governance*, 17(4):909–926.