POLITECNICO DI TORINO
Repository ISTITUZIONALE

A Privacy-Preserving Blockchain Framework for Sustainable Supplier Evaluation in the Textile Industry

Original
A Privacy-Preserving Blockchain Framework for Sustainable Supplier Evaluation in the Textile Industry / Butera, A., Romani, N., Meneguzzo, S., Gatteschi, V.. - (2025), pp. 24-32. (GoodIT '25: International Conference on Information Technology for Social Good Antwerp (BEL) September 3 - 5, 2025) [10.1145/3748699.3749769].

Availability:
This version is available at: 11583/3016393 since: 2026-10-07T09:53:32Z

Publisher:
Association for Computing Machinery

Published
DOI:10.1145/3748699.3749769

Terms of use:

This article is made available under terms and conditions as specified in the corresponding bibliographic description in the repository

Publisher copyright

(Article begins on next page)

16 November 2026

A Privacy-Preserving Blockchain Framework for Sustainable Supplier Evaluation in the Textile Industry

Alberto Butera
Politecnico di Torino
Turin, Italy
alberto.butera@polito.it

Noemi Romani
Politecnico di Torino
Turin, Italy
noemi.romani@polito.it

Silvio Meneguzzo
Univeristà di Torino
Turin, Italy
silvio.meneguzzo@unito.it

Valentina Gatteschi
Politecnico di Torino
Turin, Italy
valentina.gatteschi@polito.it

Abstract

In recent years, there has been a growing emphasis on sustainability. Consequently, errors in supplier selection can compromise key aspects such as product quality and reputation while also risking regulatory penalties. At the same time, to demonstrate their sustainability, suppliers must share sensitive data, necessitating appropriate handling. Consequently, there is a strong need for a solution that can rapidly assess supplier sustainability while safeguarding sensitive information. This paper proposes a novel methodology for evaluating suppliers within supply chains, applicable across various industries. This approach aims to assign a sustainability index to each supplier, reflecting their performance in terms of environmental, social, and economic aspects. To ensure privacy and data confidentiality, the solution utilizes homomorphic encryption, which secures supplier information while allowing for the verification of both the sustainability index and the underlying algorithm by storing them on a public blockchain. This work successfully demonstrates the feasibility of integrating homomorphic encryption with blockchain technology to calculate sustainability indices from encrypted key performance indicators (KPIs) without compromising data confidentiality.

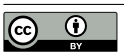
CCS Concepts

• **Software and its engineering** → **Software system structures**;
• **Security and privacy** → Cryptography.

Keywords

Supply Chain, Supplier Selection, Sustainability Index, Blockchain, Smart Contract, Homomorphic Encryption

ACM Reference Format:
Alberto Butera, Noemi Romani, Silvio Meneguzzo, and Valentina Gatteschi. 2025. A Privacy-Preserving Blockchain Framework for Sustainable Supplier Evaluation in the Textile Industry. In *International Conference on Information Technology for Social Good (GoodIT '25), September 03–05, 2025, Antwerp, Belgium.* ACM, New York, NY, USA, 9 pages. https://doi.org/10.1145/3748699.3749769



This work is licensed under a Creative Commons Attribution 4.0 International License.
GoodIT '25, Antwerp, Belgium
© 2025 Copyright held by the owner/author(s).
ACM ISBN 979-8-4007-2089-5/25/09
https://doi.org/10.1145/3748699.3749769

1 Introduction

In today's business landscape, companies that provide goods and services strive to optimize the efficiency and delivery of their products by leveraging supply chains that enable precise management of each production stage, from raw material acquisition to final product delivery. Simultaneously, the growing need for sustainable technological processes drives governments worldwide to enforce regulations that set requirements and constraints on production, protecting human rights (including labor rights), environmental protection, climate resilience, inclusive economic growth, and ethical business practices. A key directive addressing these concerns is the European Union's Corporate Sustainability Due Diligence Directive (CSDD) [1], which came into effect on 25 July 2024. This directive requires large companies to implement due diligence measures that identify and mitigate negative human rights and environmental impacts across their supply chains.

In response, businesses are increasingly adopting sustainable supply chain models characterized by environmentally friendly, transparent, and circular processes. This transition entails reducing environmental impacts throughout the supply chain, ensuring product and labor transparency, and incorporating methods for dismantling products to recover and reuse raw materials.

To facilitate this transformation, various organizations have published practical guidelines for designing and implementing sustainable supply chains. For instance, the UN Global Compact's guide [2] outlines ten core principles and provides a comprehensive roadmap for achieving compliance with sustainability requirements.

Regulations and best practices require companies to ensure that their suppliers adhere to applicable sustainability standards. However, supplier evaluation currently relies on extensive analysis of reports, a process often slowed by limited access to verifiable data. Additionally, suppliers frequently resist sharing certain internal data due to confidentiality concerns, making comprehensive assessments difficult. As a result, there is a pressing need for a solution that enables efficient evaluation of supplier sustainability while safeguarding sensitive information.

This paper examines two critical aspects: the complexity of supplier selection [11] and the transparency and accessibility of supply chain information. To address these challenges, we leverage blockchain technology to enhance transparency while employing homomorphic encryption to protect sensitive data sharing. The added value of this work lies in combining techniques that provide

transparency (such as blockchain) with cryptographic techniques that reduce the sharing of sensitive information. Through our system, suppliers can demonstrate their sustainability without sharing sensitive data. Additionally, one of the key contributions of this paper is the proposal of a sustainability index that enables objective and standardized evaluation of suppliers across the supply chain. This methodology allows for the rapid evaluation of supplier sustainability while safeguarding confidential information, thereby addressing both the complexity and transparency challenges inherent in sustainable supplier selection. Finally, this approach directly supports "SDG 12 - Responsible Consumption and Production" by enabling companies to make informed decisions about supplier sustainability, fostering more sustainable business practices, and promoting accountability in global supply chains.

The rest of the paper is organised as follows: Section 2 presents a review of the literature on solutions for supplier selection, Section 3 introduces the main concepts, technologies and use case, Section 4 describes the implementation of the tool we propose, Section 5 reports the results of the cost analysis carried out for the implemented solution. Finally, Section 6 presents the limitations and discussion, and Section 7 provides the conclusions.

2 Related works

As mentioned in the previous section, one of the ongoing issues in developing a sustainable supply chain is selecting suppliers that comply with current regulations and sustainability standards. Supplier selection is one of the most crucial processes for companies, as it directly impacts key aspects such as production costs, product quality, and delivery times. Furthermore, sustainability has become a key evaluation criterion in supplier selection over the past few years. Selecting an unsuitable supplier can compromise the entire supply chain, leading to lower product quality and increased legal risks. For this reason, research in this field is active and evolving, with researchers and developers aiming to improve the effectiveness of the selection process.

Several solutions have been proposed in the literature, including the use of multi-criteria decision-making (MCDM) methodologies, machine learning models, and blockchain technology. Studies employing MCDM methodologies frequently utilize fuzzy techniques to address uncertainty and imprecision in the data. For instance, Ecer et al. [7] focus on selecting sustainable suppliers for a healthcare supply chain in India, proposing an integrated framework that uses the Logarithmic Methodology of Additive Weights (LMAW) to calculate the weights of the selection criteria and the Technique for Order Preference by Similarity to Ideal Solution (TOPSIS) to evaluate and select the suppliers. Hendiani and Walther [10] aim to reduce errors arising from human judgment by proposing a new MCDM approach called VIFCLDTIS (interval-valued intuitionistic fuzzy cumulative likelihood-based distance to ideal solution), which calculates sustainability indicators for each supplier and ranks them according to their proximity to an adjustable ideal solution. Regarding the textile industry, Sithi et al. [14] present a comprehensive framework for evaluating sustainable suppliers, integrating Triple Bottom Line (TBL: economic, environmental, and social) principles with SWARA (Stepwise Weight Assessment Ratio Analysis) methods for assigning weights to criteria, and TOPSIS for supplier ranking. On the other hand, Vaezi et al. [15] employ a hybrid Best-Worst Method (BWM) for criteria weighting and Multi-Objective Optimization based on Ratio Analysis (MULTIMOORA) for supplier evaluation and ranking. Zekhnini et al. [17] present a Fuzzy Inference System (FIS)-based decision support system for evaluating and selecting suppliers, introducing the concept of "viability" as a new key criterion that encompasses digitization, resilience, and sustainability, in addition to traditional primary criteria.

Other works propose approaches based on machine learning and artificial intelligence (AI). For example, Abbasian et al. [3] combine supervised and unsupervised algorithms, including K-means clustering and Random Forest classification and prediction. This improves accuracy by reducing dimensionality via principal component analysis. Pap et al. [13] do not describe the specific AI methodology in detail, but instead mention the use of an AI-assisted method and compare the results obtained with MCDM approaches.

Finally, other literature works focus more on ensuring principles such as transparency and security for the supplier evaluation and selection process by leveraging blockchain technology. Haffar and Özceylan [9] propose and implement a blockchain-based system designed specifically to automate the supplier selection process in sustainable and 'lean-agile' (combining lean and agile principles) supply chains via smart contracts. This system considers a wide range of supplier evaluation criteria, including economic, environmental, social, and leagility factors, as well as a reputation system based on mutual ratings between buyers and sellers. Vaezi et al. [15] use MCDM methodologies (as described above) and integrate them with blockchain technology to emphasise its advantages, including information security, transparency, traceability, decentralization and smart contract enablement. Modares et al. [12] utilize blockchain to enhance information sharing among supply chain stakeholders, thereby increasing transparency and accountability, with the goal of facilitating more informed supplier selection.

Although the studies described above propose innovative methods for selecting supply chain suppliers and seek to ensure the transparency and security of the data used to define evaluation criteria (in the case of blockchain-based solutions), none of the cited works analyze the problem of suppliers sharing sensitive data. While some data must be made public by regulation, other data (varying by use case) is critical for more accurate supplier evaluation, but could also provide competitors with valuable information for industrial espionage purposes. Therefore, it is crucial to enable potential suppliers to demonstrate their validity and sustainability while ensuring they are confident that their data cannot be exploited by third parties for purposes other than evaluation and selection. The solution proposed by this paper uses homomorphic cryptography to calculate a sustainability index from the KPIs for supplier evaluation, publishing the final score and calculation algorithm on the blockchain while keeping the input data encrypted.

3 Background

This paper presents a methodology to evaluate suppliers in a supply chain that can be applied to any industry. However, to create a working and testable prototype, a specific use case is considered, focusing on the textile sector. This led to determining which industry-specific KPIs to use in calculating sustainability indices.

To keep supplier KPI data private, the solution leveraged homomorphic encryption properties, which enable calculations to be performed on encrypted data to obtain the same results as if the calculations were performed with unencrypted data. The algorithm and the final calculation results are uploaded to a public blockchain, making them accessible to everyone and promoting transparency between parties. The rationale behind the use case, the selected KPI, and the technological choices made in developing the proposed solution are presented in the following sections.

3.1 Use Case

The textile and clothing sector is one of the most important sectors in the European manufacturing industry. It plays a significant role in economic and social welfare. However, its importance also makes it one of the sectors with the largest negative environmental impact globally. This importance also makes it one of the sectors with the largest negative social impact, particularly in developing countries. Therefore, increasing sustainability in this sector is a crucial consideration for governments seeking to regulate further the industry and researchers seeking innovative and efficient ways to mitigate its negative impact.

One reason the sector struggles to become more sustainable is the complexity of its supply chain. It is long and diverse, and the various stakeholders involved can be scattered around the world. There is a clear need for solutions that simplify and accelerate the processes of the textile supply chain while enhancing its sustainability.

To identify the benchmark KPIs for this use case, the KPIs identified by Alves et al. [4] are considered. In the paper, the authors establish that the sustainability index comprises two factors: one related to KPIs concerning environmental and circular scores, and the other related to KPIs concerning economic and social scores. Consequently, they classified the identified KPIs into two categories:

- **Environmental and Circular Score (ECS)**: This category is specific to the product or batch being produced. The data collected relates to a wide range of activities, including logistics activities such as transportation and productive activities such as spinning, weaving, dyeing, finishing, and textile or clothing manufacturing.
- **Economic and Social Score (ESS)**: This category comprises economic and social parameters of companies engaged in the value chain. These parameters include the number of employees, salaries, salary differences, age, types of employment contracts, work schedules, training, the company's economic situation, certifications, and social initiatives.

Starting from the selected KPIs, a new approach is proposed for calculating the sustainability index as the sum of the scores obtained from the KPIs of the two categories. For each category, a subset of the most important KPIs concerning the presented use case is selected and listed in Table 1.

Category	KPI
ECS	Water consumption
ECS	Quantity of recycled water
ECS	Electricity consumption
ECS	Self-consumption of renewable energy
ECS	Natural gas consumption
ECS	Steam consumption
ESS	Total number of employees
ESS	Total number of women
ESS	Total number of men
ESS	Number of women in functions (non-top managem.)
ESS	Number of men in functions (non-top managem.)
ESS	Average salary of women (non-top managem.)
ESS	Average salary of men (non-top managem.)

Table 1: KPIs subset for ECS and ESS categories

3.2 Homomorphic Encryption

Homomorphic encryption is an advanced form of cryptography that enables computations to be performed on encrypted data without decryption, ensuring the same outcome as with decrypted data. This property is particularly valuable when third parties must process data while maintaining data confidentiality and security. The concept was first developed by Craig Gentry in 2009 and published in the article "Fully Homomorphic Encryption Using Ideal Lattices" [8]. Since then, several variants and optimizations of this encryption technique have been proposed to improve its computational efficiency and applicability to real-world scenarios. The most widely used types of homomorphic encryption are currently as follows:

- Partially Homomorphic Encryption: This type supports specific operations on encrypted data, such as addition or multiplication, but not both simultaneously. The reduced set of operations makes it much more computationally efficient.
- Fully Homomorphic Encryption (FHE): This type supports any operation on encrypted data, providing complete flexibility. However, it requires a high computational capacity, necessitating continuous optimization for its integration into practical use cases.

Our solution uses homomorphic encryption to ensure that suppliers in the supply chain can demonstrate their sustainability by publicly disclosing only the data that they are explicitly required to publish by regulations. All other data that is critical to sustainability analysis can remain private, thus eliminating the possibility of it being used for predictive analysis by competitors.

3.3 Blockchain

Blockchain technology represents the best technology currently available for achieving a high level of data transparency and accessibility. Due to its decentralized and immutable structure, all participants in the network can access any transaction or data recorded on the blockchain, and this information cannot be deleted or altered. This feature increases trust in shared information. In addition, uploading new data is tracked by recording which account uploaded it, thus ensuring the non-repudiation of what is recorded on the blockchain. Finally, as a distributed system, blockchain eliminates the single point of failure problem, ensuring greater resilience than classical databases. Even if one or more nodes in the network stop working, the system's integrity is preserved, and data remains accessible at all times.

Blockchains can be classified into several categories based on their structure, level of decentralization, and accessibility. The main ones are as follows:

- Public: open to anyone and completely decentralized. Any participant can read, write, and verify transactions without authorization.
- Private: managed by a central organization or entity and restricts access to authorized participants only. This category is often used in enterprise settings to streamline internal processes.
- Hybrid: combine features of public and private blockchains, allowing controlled access while retaining some aspects of decentralization (e.g., limited-access data writing but free reading).

We opted for a public blockchain in our solution to ensure the highest level of transparency and accessibility for users. The sustainability indices calculated by our solution, along with the algorithm used to calculate them, must be public and searchable by any user. Furthermore, a public blockchain-based solution is easier to adopt and integrate into existing systems as it is already operational.

There are several existing public blockchains, each with different characteristics. We chose the Ethereum blockchain [6] because, in addition to storing data, it allows executable code scripts, known as smart contracts, to be uploaded. These smart contracts allow functions to be executed automatically when certain programmed conditions are met. The most popular programming language for writing Ethereum smart contracts is Solidity, a Turing-complete language inspired by JavaScript and Python. We chose this blockchain for the following reasons:

- The Ethereum ecosystem is the most popular and widely used platform for developing smart contracts. It has a large community of developers and active users who continually contribute to improvements on the network. Solidity is a well-established programming language for which numerous testing tools have been developed to identify bugs and vulnerabilities. Additionally, the ecosystem is widely supported by comprehensive official documentation.
- Although Solidity is a complete language with extensive libraries, it has limitations when it comes to supporting advanced cryptographic techniques, such as homomorphic encryption. To address this shortcoming, we integrated the product developed by Zama, a team of cryptography and computer security developers and researchers, into our solution. Zama designed FHEVM [16], an innovation that extends the capabilities of the Ethereum blockchain by adding support for FHE. This enabled us to program functionality into our smart contract that processes encrypted data.

4 Implementation

This section provides an overview of our solution's general architecture, listing its main components and explaining how they function. It then delves into the implementation of smart contracts, stakeholder interaction with components, and the registration process for suppliers, data uploading, and sustainability index calculation.

4.1 General Overview

As discussed in Section 3, our proposed solution aims to accelerate the supplier selection process for companies in a supply chain while ensuring the confidentiality of suppliers' sensitive data used to calculate the sustainability index. Figure 1 illustrates the overall architecture, depicting the main components of our system and their interactions with each other.

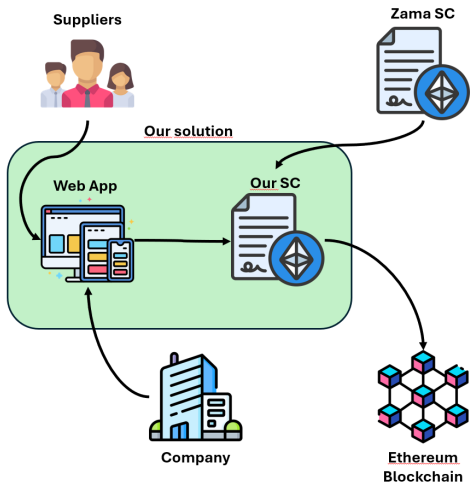


Figure 1: General architecture

Suppliers use the web application to register and upload data to the platform. In addition to simplifying interaction between users and the smart contract via a graphical user interface (GUI), the web app encrypts suppliers' data using the Zama library before forwarding it to the smart contract. It should be noted that this approach requires suppliers to trust the web application for secure data encryption, which represents a potential centralization point that could be mitigated through decentralized distribution mechanisms such as IPFS or open-source verification in future implementations. The smart contract, which is deployed on the Ethereum blockchain, stores the vendors' identifiers and their uploaded data exclusively in encrypted form. This ensures that the data is not publicly exposed in plain text. Additionally, it calculates the sustainability index using the encrypted data and stores the result. Before users read it, the result is decrypted and displayed in plain text. Suppliers can always access their own data, while no one else can access any supplier's data unless the supplier has given permission for their data to be read.

4.2 Smart Contract

The Smart Contract is responsible for managing suppliers' data and calculating the sustainability index, while ensuring the confidentiality of suppliers' data. Indeed, once the sustainability index has been computed and stored on the blockchain, it becomes publicly accessible. However, the numeric values used by the algorithm to calculate the sustainability score are stored in encrypted form. Given the public nature of the Ethereum blockchain, particular attention was paid to the manner in which data is stored within

the smart contract, with a view to providing both transparency and preserving supplier privacy. From a supply-chain perspective, transparency can be defined as the ability of brands or retailers to select suppliers based on a publicly available sustainability index. This index is intended to align with sustainability standards, encompassing social, economic, and environmental dimensions, and thereby promote the principles of a circular economy. From the suppliers' perspective, the transparency concept can be understood to relate to the algorithms implemented to compute the index, as well as to the willingness to make the numeric values of the KPIs used in the computation publicly accessible to all parties. Indeed, the pursuit of transparency is juxtaposed with the concomitant insistence on data privacy. Table 2 provides an overview of the data stored in the smart contract, distinguishing between data stored in plaintext and that stored in encrypted form. Before embarking on a detailed exposition of data storage methodologies, it is essential to provide a comprehensive explanation of the algorithm used to calculate the sustainability index. The final score is calculated as a weighted sum of two different indices: the *SEI_index* (Social & Economic Sustainability Index) and the *CEI_index* (Circular Economy & Environmental Sustainability Index). The former, used for evaluating social and economic sustainability, is based on company-related data, as shown in 3 (e.g., average salary, number of women). The latter provides a measure of environmental sustainability and support for the circular economy. The arithmetic average of the indices associated with each production batch from the supplier is calculated and updated for each new production batch. Reference KPIs are shown in 4 (e.g., water consumption, electricity consumption). As demonstrated in Table 2, the overall sustainability score SI (Sustainability Index) associated with the supplier is stored as plaintext data, whereas the two contributions given by the SEI index and the CEI index are stored as ciphertext data. Indeed, the implementation of the Zama library facilitates the management of encrypted data. This process enables the attainment of a result that is analogous to that which would be obtained by manipulating the original data as plaintext. Regarding the Supplier, it was decided that the wallet address would be stored as plaintext data only. All data involved in the numeric computations must be stored as encrypted, including the overall Sustainability Index, the annual SEI index, the updated CEI index, and the arrays containing all the scores already computed and stored on the blockchain. The datasets can be distinguished between those involved in measuring economic and social sustainability and those involved in measuring environmental sustainability and supporting the circular economy. However, as demonstrated in Table 2, both datasets encompass publicly accessible information (e.g., the supplier ID, the production batch ID, the names of the KPIs involved in computation) and data stored in encrypted form (e.g., the numeric values associated to the KPIs, and the corresponding CEI index or SEI index). It is noteworthy that the decision was taken to adopt the Zama Library and implement fully homomorphic encryption of data, with the objective of ensuring the privacy of sensitive data for suppliers. Concurrently, by disclosing the algorithm and the comprehensive sustainability index, the system fosters transparency not only for suppliers but also within the broader supply chain context. Regarding the transparency of the implemented algorithm, it is achieved at the blockchain level by providing suppliers with the ability to inspect the mechanism and data behind the assigned index. This is because the logic is defined by the methods included in the Smart Contract, which are visible to all parties. Each supplier is permitted to examine the scores achieved by competing entities, which are stored on the blockchain. Should the situation require it, the user (supplier, brand, retailer, or company) is also permitted to request access to the numeric values that underpin the calculated scores of other suppliers. In terms of privacy preservation, this is achieved at the blockchain level by storing the Sustainability Index as plaintext data only, without making the data leading to those indices visible to all. If a user attempts to access the numeric values used for the index computation, they will only be able to do so if the supplier has already granted them permission to do so. In the absence of such a foundation, the ability to proceed is impeded.

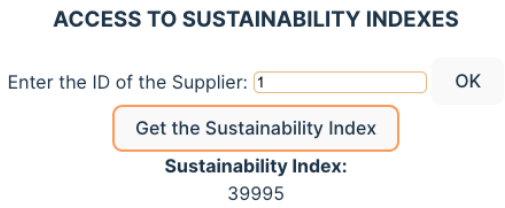


Figure 2: Supplier Registration

4.3 User Interaction with the Web App and the Smart Contract

This section provides a comprehensive explanation of the steps to take to participate in the described process and interact with the smart contract. Once they have accessed the website, users can choose to register as a supplier or request access to the sustainability indices of already registered suppliers, depending on whether they are a supplier or a different entity (brand, retailer, company).

4.3.1 Supplier.

- **Supplier registration**
  As shown in Figure 2, A user must call the *addSupplier* method of the Smart Contract through the web app's GUI. The function requires the supplier's ID, which will serve as a unique identifier. Additionally, the function automatically initializes specific parameters, such as the *is_Supplier* flag, which indicates whether the wallet address is associated with a supplier.
- **Dataset creation**
  To invoke the storage of a dataset contributing to the computation of the SEI Index, the user must call the *addDataset_SocialEconomicSustainability* function (3). To invoke the storage of a dataset contributing to the computation of the CEI Index, the user must call the *addDataset_CirculateEnvironmentalSustainability* function (4). These functions require the following as input values: a dataset ID, the names of the KPIs, the encrypted numeric values of the KPIs, and an input proof associated with the encrypted values. Regarding the CEI Dataset, a production batch ID is also required. The encrypted values and the input

Clusters	Data	Encrypted Data	Plaintext Data
Supplier	Supplier Address		X
Supplier	Overall Sustainability Index	X	
Supplier	SEI Index	X	
Supplier	CEI Index	X	
Supplier	Array Of SEI Scores	X	
Supplier	Array Of CEI Scores	X	
Dataset for Social & Economic Sustainability	Supplier ID		X
Dataset for Social & Economic Sustainability	Dataset SEI index	X	
Dataset for Social & Economic Sustainability	Array Of Numeric Values	X	
Dataset for Social & Economic Sustainability	KPIs	X	
Dataset for Env. Sustainability & Support to Circular Economy	Supplier ID		X
Dataset for Env. Sustainability & Support to Circular Economy	Production Batch ID		X
Dataset for Env. Sustainability & Support to Circular Economy	Dataset CEI index	X	
Dataset for Env. Sustainability & Support to Circular Economy	Array Of Numeric Values	X	
Dataset for Env. Sustainability & Support to Circular Economy	KPIs	X	

Table 2: Storage of data

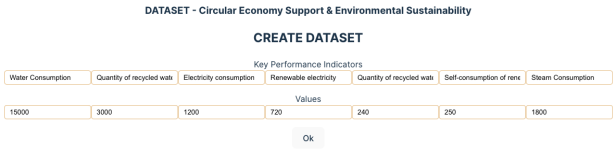


Figure 3: Dataset for SEI Index

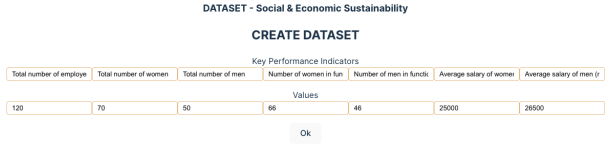


Figure 4: Dataset for CEI Index

proof are obtained by implementing the Zama *encryption* operation directly through the web app's GUI. The user must enter the numeric values of the KPIs into a form, which will first be encrypted by implementing the Zama *encryption* of inputs. A zero-knowledge proof is then generated to prove the integrity of that data. Finally, the encrypted values and the input proof are passed as input values to the Smart Contract. The Smart Contract methods then automatically initialize the attributes of the datasets to be stored on the blockchain. Additionally, a call to the internal functions is made to associate the encrypted numeric values with their corresponding identifiers and compute the sustainability score to be assigned to the dataset. Finally, after updating the individual SEI or CEI index assigned to the supplier, the overall sustainability index is recalculated.

- **Grant access to dataset's numeric values**
  As shown in Figure 5, the supplier must call the *grantAccess* function. This function requires a wallet address as an input

Figure 5: Grant access to a different user

value, corresponding to the user to whom the supplier wants to grant access. Through the Zama library and the Zama *allow*, and *allowThis* methods, this function automatically grants the Smart Contract and users access to the parameters passed as input values to the Zama methods (e.g., dataset numeric values). It is worth noting that this mechanism increases data privacy preservation. Only the dataset creator or users granted access by the creator are allowed to access the numeric values as plaintext data.

- **Update of the Overall Sustainability Index**
  The supplier must call the *computeSustainabilityIndex* function. This function requires the supplier ID as an input value. It automatically computes the supplier's overall sustainability as a weighted sum of the SEI and CEI indices corresponding to the ID. First, it retrieves the SEI and CEI indices associated with the supplier. Then it uses the *plaintextSEIFactor* and the *plaintextCEIFactor*, which are the weights defined for the two contributions and publicly stored in the Smart Contract. For this testing phase, we decided to set the *plaintextSEIFactor* equal to 0,6 and the *plaintextCEIFactor* equal to 0,4. The choice of weights was made at a high level, with the aim of testing the algorithm and defining a final index as a weighted average of the two contributions. At this testing stage, we decided to give more weight to the SEI contribution to enhance the concept of economic and social sustainability.

4.3.2 *All the users (Supplier - Brand – Retailer – Company – users).*

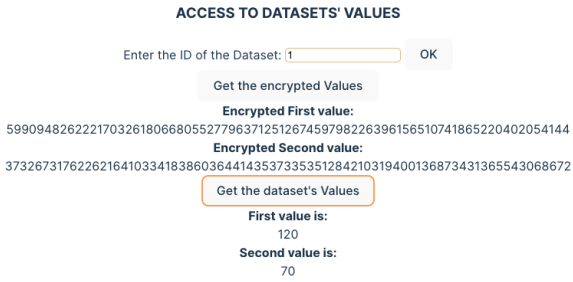


Figure 6: Accessing Dataset numeric values

- **Access to datasets' numeric values**
  The user must call the *getNumericValues* function. This function requires the dataset ID and enables suppliers to check the plaintext numeric values involved in computing the sustainability index assigned to the dataset. This is made possible by a Zama operation called *reencryption*. Decrypted numeric values are only shown in the web app's GUI if the user created the dataset or has requested and obtained access to these values (6). Otherwise, the access is denied, as shown in Figure 7. It is worth noting that this mechanism prevents the compromise of suppliers' sensitive data. At the same time, it provides suppliers with the opportunity to review the data involved in the computation, thereby ensuring the transparency of the algorithm.

- **Access to the overall Sustainability Index**
  The user must call the *getSustainabilityIndex* function. This function requires the supplier ID as an input value and returns the decrypted overall sustainability index as an output value. This value is obtained through the Zama *reencryption* operation. This function can be called by any user and does not implement any constraints. It is worth remarking that this mechanism ensures transparency within the system. Each supplier can check their own sustainability index and access those of their competitors. Other entities (e.g., brands, companies, retailers) can access the sustainability indices stored on the blockchain to select the suppliers.

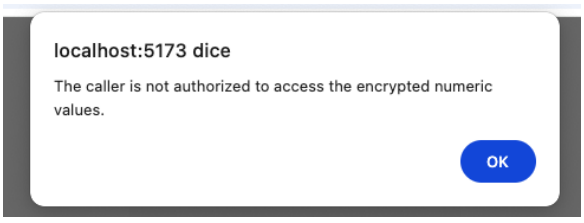


Figure 7: Access denied

5 Test and Results

The smart contract was deployed on Sepolia, Ethereum's official test network, which provides a realistic testing environment without incurring mainnet costs. Sepolia was chosen because it is the most up-to-date test network available, closely reflecting Ethereum mainnet conditions, supporting the Zama FHEVM library required for homomorphic encryption, and providing a stable testing environment. We tested the full supplier workflow, from registration to sustainability index computation and reading the final index. We verified that the encryption and decryption functions performed as expected (see Fig. 6) and that the index computation yielded the correct value after executing the algorithm. We also tested our smart contract using Slither, one of the most widely used testing tools for Solidity smart contracts, to identify and avoid known vulnerabilities. As shown in Fig. 8, the output reports that our smart contract contains 0 high-severity issues, 11 medium-severity issues, and 1 low-severity issue.

```
root@7b59e89b35ba:/share# slither --print human-summary myContract.sol
'solc --version' running
'solc myContract.sol --combined-json abi,ast,bin,bin-runtime,srcmap,srcmap-runtime,userdoc,devdoc
INFO:Printers:
Compiled with solc
Total number of contracts in source files: 17
Source lines of code (SLOC) in source files: 9638
Number of  assembly lines: 0
Number of optimization issues: 1
Number of informational issues: 70
Number of low issues: 1
Number of medium issues: 11
Number of high issues: 0

+--------------------------+-------------+------+-----------+--------------+----------+
| Name                     | # functions | ERCS | ERC20 info | Complex code | Features |
+--------------------------+-------------+------+-----------+--------------+----------+
| ZamaFHEVMConfig          |           2 |      |           |           No |          |
| EthereumZamaFHEVMConfig  |           1 |      |           |           No |          |
| ZamaGatewayConfig        |           2 |      |           |           No |          |
| EthereumZamaGatewayConfig |           1 |      |           |           No |          |
| IKMSVerifier             |           1 |      |           |           No |          |
| IGatewayContract         |           1 |      |           |           No |          |
| Gateway                  |          22 |      |           |           No | Assembly |
| ITFHEExecutor            |          31 |      |           |           No |          |
| IACL                     |           5 |      |           |           No |          |
| Impl                     |          38 |      |           |           No | Assembly |
| Common                   |           1 |      |           |           No |          |
| TFHE                     |        1186 |      |           |           No |          |
| myContract               |          43 |      |           |           No |          |
+--------------------------+-------------+------+-----------+--------------+----------+
INFO:Slither:myContract.sol analyzed (17 contracts)
root@7b59e89b35ba:/share#
```

Figure 8: Slither output report

The medium-severity issues identified by Slither primarily relate to potential reentrancy vulnerabilities detected in functions that interact with the TFHE library for homomorphic encryption operations. However, these flagged issues do not represent actual security vulnerabilities in our implementation context. Reentrancy attacks occur when external contracts can recursively call back into the original contract before the first execution completes, potentially manipulating state variables. In our case, the detected external calls are to the trusted Zama TFHE library functions (such as *TFHE.add*, *TFHE.allow*, and *TFHE.asEuint32*), which are deterministic cryptographic operations that do not allow arbitrary code execution or callback mechanisms. Furthermore, our contract implements the *nonReentrant* modifier from OpenZeppelin's ReentrancyGuard on critical state-changing functions. The TFHE library operations are essential for homomorphic encryption functionality and pose no reentrancy risk, making these Slither warnings false positives in our specific use case.

Finally, a cost analysis was conducted because Ethereum requires payment of a fee for sending transactions or performing smart contract functions. These fees serve to pay the nodes that validate transactions and prevent scripts that could crash the system, such as infinite loops, from being executed. The cost of executing functions is measured in units of gas. The cost of gas varies over time, primarily due to the network's congestion level at that time. Additionally, it is possible to pay a higher amount per gas unit to prioritize transaction execution. At the time of testing (May 26, 2025), the average price per gas unit was 3 gwei, equivalent to approximately $0.000008. The execution cost of the main functions of the smart contract can be calculated by multiplying the gas price by the number of gas units required for execution. Table 3 shows the value of all main functions in gas units and the cost of execution in dollars.

Function	Gas Units	Cost (USD)
Contract Deployment	3,500,000	$26.78
addSupplier(1)	158,031	$1.21
addDataset_SEI(...)	2,201,355	$16.84
addDataset_CEI(...)	2,122,877	$16.24
computeSustainabilityIndex(...)	390,460	$2.99
grantAccess(...)	264,532	$2.02
requestSustainabilityIndex(...)	55,000	$0.42

Table 3: Complete cost analysis testing (May 26, 2025: 3.0 gwei, ETH $2,550)

The cost analysis revealed that the solution is highly economically viable. Based on actual testing conditions, supplier registration costs $1.21, and uploading a complete set of KPIs costs $16.84 for SEI datasets and $16.24 for CEI datasets, resulting in a total workflow cost of $39.30 per supplier evaluation. This represents a significant cost advantage compared to traditional supplier evaluation methods, which typically involve manual assessments, third-party audits, extensive documentation review, and on-site inspections. While alternative EVM-compatible blockchains, such as Polygon, could potentially reduce costs further, the current cost structure already makes the solution highly competitive and economically attractive for widespread industry adoption. However, at present, the solution utilizes a limited number of KPIs, and the algorithm used to calculate the sustainability index may become significantly more computationally demanding, necessitating additional considerations for large-scale deployment.

6 Discussion

While our proposed framework demonstrates the feasibility of integrating homomorphic encryption with blockchain technology for the sustainable evaluation of suppliers, several important considerations about incentives and limitations require further study.

6.1 KPI Coverage

The current implementation focuses on a limited subset of KPIs specific to the textile industry, covering only thirteen indicators across environmental, circular economy, and economic/social categories. This selective approach simplified prototype development and enabled the validation of proof of concept. However, a comprehensive sustainability assessment requires a broader range of metrics to capture the full spectrum of environmental, social, and governance (ESG) factors. The modular design of our system will facilitate future expansion without requiring fundamental architectural changes. Nevertheless, the computational complexity increases proportionally with the number of KPIs incorporated, so careful consideration of performance optimization is necessary as the system scales up.

6.2 Algorithm Improvement

The current sustainability index calculation uses a simple weighted sum approach. While this methodology provides a basic overview of supplier sustainability levels, it fails to capture the complex interdependencies that often exist between different sustainability metrics. For example, improvements in energy efficiency may be correlated with reduced water consumption, and these synergistic effects should be reflected in the assessment algorithm. As our implementation uses FHE, there are no limitations on the types of mathematical operations that can be performed on encrypted data. Future work should therefore focus on developing more sophisticated algorithms that account for KPI correlations, nonlinear relationships, and threshold effects while maintaining computational efficiency through careful optimization.

6.3 Environmental Sustainability Considerations

The apparent contradiction of using blockchain technology to promote sustainability given blockchain's reputation for environmental impact merits clarification. Environmental concerns are primarily associated with blockchains employing proof-of-work consensus mechanisms, which require substantial computational power for mining operations. Our solution leverages Ethereum, which transitioned from proof-of-work to proof-of-stake consensus in September 2022, resulting in a reduction of approximately 99.95% in energy consumption [5], making it comparable to the energy consumption of a small data center. This transition makes Ethereum an environmentally sustainable platform for sustainability-focused applications, aligning the technological infrastructure with the environmental goals of the solution. In addition, our solution can be considered more sustainable than traditional supplier evaluations since steps such as physical site visits and audits, manual data processing and verification, and paper documentation and shipping can be avoided, reducing the total CO2 produced.

6.4 Suppliers Incentive Mechanisms

While companies benefit from faster supplier evaluation processes, reduced assessment costs and automated compliance with regulations (e.g. the EU Corporate Sustainability Due Diligence Directive), our solution provides several incentives for suppliers. Transparent sustainability indices create market incentives: higher scores command better pricing, preferred supplier status and favourable contract terms. The public nature of the indices generates competitive pressure, encouraging industry improvements and providing a sustainability benchmark against competitors. Poor performers face market pressure to improve or risk losing business, while high

performers gain a competitive advantage by demonstrating their sustainable performance.

7 Conclusion

This work presents an innovative blockchain-based framework that addresses persistent challenges in sustainable supplier selection within the textile industry supply chain. The proposed approach integrates the properties of homomorphic encryption with the characteristics of a public blockchain to ensure supplier privacy and transparency while simultaneously accelerating the supplier selection process by companies. This work successfully demonstrates the feasibility of calculating sustainability indices from encrypted KPIs without compromising data confidentiality.

The framework provides several significant contributions to sustainable supply chain management. First, it accelerates the selection process by eliminating the need for direct communication between individual suppliers or manual data collection through online research. Companies can now rely on public sustainability indices stored on the blockchain. Additionally, the solution eliminates trust dependencies between suppliers and purchasing companies, as data is never shared in plain text, thereby allowing the elimination of any potential Non-Disclosure Agreements (NDAs).

The implementation demonstrates that it is possible to integrate homomorphic cryptography with blockchain technology to create a transparent system without compromising the privacy of sensitive data. Testing on the Sepolia testnet confirmed the correct functionality of all core components, including supplier registration ($1.21), dataset uploading ($16.84 for SEI and $16.24 for CEI datasets), and sustainability index computation ($2.99), resulting in a total workflow cost of $39.30 per supplier evaluation. Security analysis using Slither revealed no high-severity vulnerabilities, with medium-severity warnings being false positives related to trusted TFHE library interactions.

However, the current trust model relies on both the client-side web application and the underlying FHEVM infrastructure, which could be enhanced through commit-reveal schemes combined with ZK-SNARKs to provide end-to-end verifiability and reduce the need for trust assumptions. Moreover, several limitations still need to be resolved before practical deployment becomes viable. Future implementations should focus on integrating more comprehensive KPIs for sustainability evaluation, as the 13 indicators used in this work may not be exhaustive. Additionally, designing more sophisticated algorithms than simple weighted sums is necessary to obtain more meaningful indices that account for the complex interdependencies between sustainability factors. The modular architecture facilitates these enhancements without requiring fundamental changes to the core framework.

Acknowledgments

This study was carried out within the MICS (Made in Italy – Circular and Sustainable) Extended Partnership and received funding from the European Union Next-GenerationEU (PIANO NAZIONALE DI RIPRESA E RESILIENZA (PNRR) – MISSIONE 4 COMPONENTE 2, INVESTIMENTO 1.3 – D.D. 1551.11-10-2022, PE00000004). This manuscript reflects only the authors' views and opinions, neither the European Union nor the European Commission can be considered responsible for them.

References

[1] [n. d.]. Directive EU 2024/1760 EN EUR Lex. https://eur-lex.europa.eu/eli/dir/2024/1760/oj/eng. Accessed: 2025-05-20.

[2] [n. d.]. Supply Chain Sustainability Guide. https://unglobalcompact.org/library/205. Accessed: 2025-05-22.

[3] Mahyar Abbasian and Amin Jamili. 2025. A Hybrid Machine Learning Approach to Evaluate and Select Agile-Resilient-Sustainable Suppliers Considering Supply Chain 4.0: A Real Case Study. *Process Integration and Optimization for Sustainability* 9, 2 (May 2025), 717–735. doi:10.1007/s41660-025-00483-1 Company: Springer Distributor: Springer Institution: Springer Label: Springer Number: 2 Publisher: Springer Nature Singapore.

[4] Luís Alves, Miguel Sá, Estrela Ferreira Cruz, Toni Alves, Marcelo Alves, João Oliveira, Manuel Santos, and António Miguel Rosado da Cruz. 2023. A Traceability Platform for Monitoring Environmental and Social Sustainability in the Textile and Clothing Value Chain: Towards a Digital Passport for Textiles and Clothing. *Sustainability* 16, 1 (Dec. 2023), 82. doi:10.3390/su16010082

[5] Rameez Asif and Syed Raheel Hassan. 2023. Shaping the future of Ethereum: exploring energy consumption in Proof-of-Work and Proof-of-Stake consensus. *Front. Blockchain* 6 (Aug. 2023).

[6] Vitalik Buterin. 2014. Ethereum Whitepaper: A Next-Generation Smart Contract and Decentralized Application Platform. https://ethereum.org/content/whitepaper/whitepaper-pdf/Ethereum_Whitepaper_-_Buterin_2014.pdf Accessed: 2025-05-04.

[7] Fatih Ecer, Gholamreza Haseli, Raghunathan Krishankumar, and Mostafa Hajiaghaei-Keshteli. 2024. Evaluation of sustainable cold chain suppliers using a combined multi-criteria group decision-making framework under fuzzy ZE-numbers. *Expert Systems with Applications* 245 (July 2024), 123063. doi:10.1016/j.eswa.2023.123063

[8] Craig Gentry. 2009. Fully homomorphic encryption using ideal lattices. In *Proceedings of the forty-first annual ACM symposium on Theory of computing (STOC '09)*. ACM, 169–178. doi:10.1145/1536414.1536440

[9] Samer Haffar and Eren Özceylan. 2024. Blockchain-Based System for Supplier Selection in Sustainable and Leagile Supply Chains. *IEEE Access* 12 (2024), 139883–139911. doi:10.1109/ACCESS.2024.3467059

[10] Sepehr Hendiani and Grit Walther. 2025. Towards sustainable futures: Rethinking supplier selection through interval-valued intuitionistic fuzzy decision-making. *International Journal of Production Economics* 285 (July 2025), 109620. doi:10.1016/j.ijpe.2025.109620

[11] Vipul Jain, Lyes Benyoucef, and S.G. Deshmukh. 2009. Strategic supplier selection: some emerging issues and challenges. *International Journal of Logistics Systems and Management* 5, 1/2 (2009), 61. doi:10.1504/ijlsm.2009.021645 Publisher: Inderscience Publishers.

[12] Azam Modares, Nasser Motahari Farimani, and Farzad Dehghanian. 2025. A New Vendor Managed Inventory for Perishable Products Considering Supplier Selection. *Process Integration and Optimization for Sustainability* 9, 1 (March 2025), 57–74. doi:10.1007/s41660-024-00457-9 Company: Springer Distributor: Springer Institution: Springer Label: Springer Number: 1 Publisher: Springer Nature Singapore.

[13] József Pap, Csaba Makó, Adrián Horváth, Zoltán Baracskai, Tamás Zelles, Judit Bilinovics-Sipos, and Sándor Remsei. 2025. Enhancing Supply Chain Safety and Security: A Novel AI-Assisted Supplier Selection Method. *Decision Making: Applications in Management and Engineering* (2025), 22–41. doi:10.31181/dmame8120251115

[14] Sanjucta Saha Sithi, Mst Anjuman Ara, Ahnaf Tahmid Dhrubo, Abid Hasan Rony, and Md Abdus Shabur. 2025. Sustainable supplier selection in the textile industry using triple bottom line and SWARA-TOPSIS approaches. *Discover Sustainability* 6, 1 (Dec. 2025), 1–23. doi:10.1007/s43621-025-01206-9 Company: Springer Distributor: Springer Institution: Springer Label: Springer Number: 1 Publisher: Springer International Publishing.

[15] Ali Vaezi, Erfan Rabbani, and Seyed Ahmad Yazdian. 2024. Blockchain-integrated sustainable supplier selection and order allocation: A hybrid BWM-MULTIMOORA and bi-objective programming approach. *Journal of Cleaner Production* 444 (March 2024), 141216. doi:10.1016/j.jclepro.2024.141216

[16] Zama. 2025. fhEVM - Confidential Smart Contracts using Fully Homomorphic Encryption. https://docs.zama.ai/fhevm Accessed: 2025-05-25.

[17] Kamar Zekhnini, Abla Chaouni Benabdellah, Anass Cherrafi, Imane Bouhaddou, and Surajit Bag. 2025. Viable industrial supplier performance evaluation using fuzzy inference system: a case of the automotive industry. *Journal of Business & Industrial Marketing* 40, 4 (May 2025), 941–962. doi:10.1108/jbim-12-2022-0555 Publisher: Emerald.