A Soulbound Token-based Reputation System in Sustainable Supply Chains

Massimiliano Pirani, Alessio Cacopardo, Alessandro Cucchiarelli, Luca Spalazzi
Università Politecnica delle Marche, Ancona, Italy
m.pirani@univpm.it, a.cacopardo@univpm.it, a.cucchiarelli@univpm.it, l.spalazzi@univpm.it

Abstract

This paper aims to provide novel insights in the use of recent advances about non-fungible and Soulbound tokens, as they are a growing reality in the context of the DLT framework. In particular, this work discusses how these technological provisions can enable a renovated and strengthened role of the Internet of Everything concept in the complex processes of the Industry 5.0, where the social, societal, and technical dimensions merge into an irreducible applicative context. The potentialities of the approach are expressed by means of a simple but meaningful example on an industrial case study concerning the food supply chain.

1 Introduction

Internet of Everything (IoE) can be defined as the "*the seamless interconnection and autonomous coordination of massive number of computing elements and sensors, inanimate and living entities, people, processes and data through the Internet infrastructure*"[1]. Industry 5.0, on the other hand, must go "*beyond efficiency and productivity as the sole goals [...] putting research and innovation at the service of the transition to a sustainable, human-centric and resilient [$\cdots$] industry*"[2] [11]. As Industry 5.0 integrates and extends the distinctive features of Industry 4.0, existing distribution and decentralisation paradigms must be equipped with sustainability-related features. New systemic engineering design approaches have to take into account a strengthened focus on the IoE concept as it aims at the networked connection of people, process, data, and things that is a crucial and enabling aspect for Industry 5.0 [15]. This also requires the inclusion of added dimensions in design like ethics and values that are the key factors in enabling human–machine symbiosis in Industry 5.0 [18]. In this context, where numerous independent actors and with opposing interests operate, utmost trust between the actors that compose the overall process is a growing need. Along this direction, distributed ledger technologies (DLTs) and in particular Blockchains can provide valid technological support. The distributed nature of DLTs along with *tokenization* provide the enabling technologies in all those cases in which no actor can assume the role of controller vis-à-vis the others. Nevertheless, most of the works dealing with DLTs focus on trust of data and communication (because of the immutability and traceability of transactions guaranteed by blockchains) (e.g., see [14, 25, 27]). Recently, some work has proposed using DLT to improve the trust and compliance of business processes (e.g., for orchestration and collaboration see [24, 20, 7], for choreography see [22, 23]). Up-to-now, only a few papers focused on trust management in case of heterogeneous society of human actors and artificial entities that purposefully are brought together into a complex process. At this point, some research questions arise:

RQ1 Can DLT be a key technology for the IoE paradigm?

RQ2 Can tokens be used to represent and manage trust?

RQ3 If so, what kind of tokens are more appropriate: fungible or non-fungible, transferable or non-transferable?

In an attempt to answer the above questions, this research investigates the possibilities of Blockchain technologies in integrating the multiple information dimensions created in a food supply chain process. The work is in fact related to the research and innovation activities conducted within the European project ENOUGH [12], in which support from digitisation is sought for the goals of environmental sustainability along with the social and moral incentives of reputation of the variety of participants in a supply chain process in the food sector. In the specific project on sustainable food supply chain, the primary need is a treatment of GHG emissions (in CO2 equivalents) and the reputation of the elements acting in the supply chain. At the same time, there is a need to avoid a centralized approach because this is seen as detracting from the motivation of the participating nodes, which typically, in this type of process, prefer to act autonomously and privately, while appreciating a recognition of their reputation with respect to the quality objectives of their productions and

[1] `https://ioe.org/`

[2] `https://research-and-innovation.ec.europa.eu/research-area/industrial-research-and-innovation/industry-50_en`

the achievement of sustainability goals. The Blockchain can offer a framework for decentralization and distribution that can address these requirements.

The original contribution of this work is to explore an appropriate use of the *token* technology from the DLT context in order to convey the multiple dimensions of information needed by a trustable complex process in which the sources and sinks of information are the typical (possibly autonomous) actors of heterogeneous nature. In particular, to explore the possibilities in this context of the non-fungible (NFT) and non-transferable *Soulbound* token (SBT)[3], which use and wide adoption are still matter of interesting inquiries.

A second contribution of this work is to provide both general and practical account on the computation of a reputation value by means of a suitable mix of NFT and SBT properties as they comply, in a complex distributed industrial process scenario, with oracular and local properties of a participant and with a global contractual consensus, respectively.

While the context of use here is a sustainable food supply chain, the proposed approach can be generalized to other sectors concerning the Industry 5.0 and services or engineering processes where the social dimension meets the objectives of environmental sustainability and productivity. Other affine supply chains can be addressed like consumer goods, clothing, engineering processing like constructions, or services like healthcare and assistance.

The paper is structured as follows. Section 2 presents a brief account on related work. In Section 3, the architecture of the proposed solution is exposed. In Section 4, the implementation of the solution through smart contracts is detailed, which is continued with a case example in Section 5. Finally Section 6 is left for conclusion and perspectives.

2 Related Work

The notion of *trust* involves beliefs and expectations, with a certain level of confidence, about the dependability (especially reliability and security), competence, and other characteristics of an entity or data [6]. The notion of *reputation* is related to the notion of trust and can be considered an opinion on trust [16]. There are several works on trust management systems (TMSs) [1], these works can be roughly divided into works dealing with policy-based TMSs and works dealing with reputation-based TMSs. *Policy-based trust models* use policy rules that determine whether to trust an entity or data [6, 16]. Based on this approach, trust is a sort of Boolean value: a *true* value for those who respect the policies and a *false* value for those who do not respect them. *Reputation-based trust models* use past behavior (especially during interactions) and data gathered from other sources (recommendations from other entities included) to determine whether to trust an entity or data [6, 16]. Based on this approach, trust is measured with a score according to a given scale.

DLTs are related to trust management from two different perspectives [4]. On the one hand, what mechanisms allow users to trust a DLT, in particular what is transcribed in the public ledger. From this perspective, the trust is a matter of the consensus algorithm adopted by the DLT infrastructure (e.g., see [26]). On the other hand, what DLT-based mechanisms allow users to trust other users. From this perspective, a DLT is exploited to enforce trust. From this second perspective, thanks to their ability to ensure immutability and traceability of transactions and to their consensus mechanisms, DLTs have found wide application for policy-based trust management (e.g. see [9, 14, 25]). In contrast, DLTs have so far found only a few applications to the reputation-based approach [16, 19, 3, 17, 21, 28]. On the one hand, most of them deal with trust of data, especially in a IoT scenario, and of the sensors that produce them [3, 17, 16, 2]; some of them also propose some penalty mechanisms [2]. On the other hand, Wu and Zhang [28] deal with trust of actors.

The works presented by Malik et al. [19] and by Putra et al. [21] are very close to ours in intention and kind of trust model adopted. Indeed, according to those works, the reputation is based on the combination of two aspects: sensor data and ratings by human actors. Sensor data are used as indicator of the quality of the food products, and the reputation of a commodity is traced throughout the supply chain. Ratings attributed by buyers and regulators to the sellers, commodity reputations, and the reputation history are used to compute the current reputation of a seller. Furthermore, Putra et al. [21] also takes into account that commodities can be used to produce new commodities. Moreover, both works measure reputation as an overall score that masks the different characteristics that contribute to reputation and do not consider penalising mechanisms.

Recapping, it is worthy to mention that none of the aforementioned works takes into account a multi-dimensional rating mechanism related simultaneously to environmental, social, economic, and technical sustainability, such as the total GHG emission of a process in parallel to trust and quality under health, work-place, safety, and many other aspects of sustainability in Sustainable-Development-Goals (SDG)[4] sense. Furthermore, none of them appears to be adopting non-fungible tokens (NFTs) as a mechanism for reputation [5]. This represents a limit, as reputation tokenization in a DLT system could be used as a built-in incentive mechanism for the constructive system dynamics of an emerging virtuous behavior that extracts trust from a complex distributed process like supply chains.

3 Architecture and workflow

To deal with simplicity, but without loss of generality, let us illustrate the planned architecture through an instance of it with a typical set of participants in the food supply chain. In Figure 1, are depicted the major components in the architecture of an application that has the aim to use and integrate the NFT and SBT technology for a society of actors that becomes trusted having the IoE as the major communication means. IoE unifies human and automated actors into a source of data for the sensing and measurement of performances. In the figure, they are indicated as *sensors* but they have to be intended as systematic process of measurement of quality of a process coming from statistics on real-time and raw data. Usually these kind of measurements become performance indicators and can be unified, normalized, and constructed in

[3] https://wiki.rugdoc.io/docs/introduction-to-soulbound-tokens/

[4] https://www.undp.org/sustainable-development-goals

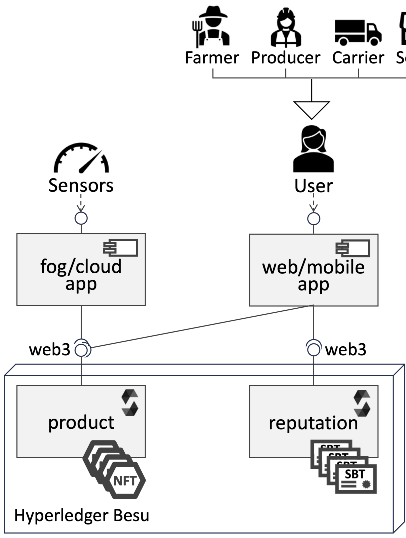

Figure 1. System architecture in the Food Supply Chain scenario

many ways [8]. Performance indicators rate the effectiveness (towards some collectively agreed goal) of a production process that ends up with a product; "production" intended in its wide extended sense (it could be also a mere service in some cases). The figures obtained with indicators constitute the part that can be accounted in an immutable NFT, which subsequently is prone to be transferred across the multiple steps of the whole process and participants.

In the same Figure 1, a list of classical set of participants in the overall process is shown, namely: a farmer, a producer, a carrier, and seller, in order to minimally represent four fundamental steps in the supply chain as primary and secondary production, transport, and retail, respectively. These users are then associated with an SBT. The information bound to them is a combination of systematic performance measurements due to trading and production on the NFT side, and a more subjective consensus vote that each of the participants can express basing on not well-formalizable but agreeable criteria, eventually summing up to a reputation value of a participant.

Previous structural view must be accompanied by a dynamic description of information flow to better reveal the dynamics of interaction between the parts, as done in Figure 2. In this figure, the cycle of the information transfer for the NFT and the role of SBT can be better inferred. Although for the sake of simplification, a daisy chain structure is shown, other topologies and more networked and distributed information loops are possible. Nevertheless, here it is shown how the systematic rating on performance about a product is conveyed into a set of NFTs, which bear multiple performance dimensions like CO_2 footprint and quality for a certain production. This information is coupled with a reputation value provided as a feedback by the participant who is knowledgeable (and so a stakeholder) in the chain of the interested processes. The coupling of systematic performance ratings and socially generated information will constitute the content of the SBT that is forever associated to a participant.

After any step of production, a NFT can be transferred to a subsequent production step, and the NFT value is in some way inherited from the owner of the subsequent step, all the way through to the final user. This creates a great bond of trust between the participants who are interested, by their own reputation, in influencing improvement at all stages of the supply chain.

4 Implementation via Smart Contracts

The previous scenario is surely prone for an exploitation of well-known technologies in the Blockchain. By means of suitable Smart Contract mechanism, the architecture and the workflow can be realized with a multi-signed pattern and collaboration between the participants of the supply chain. To provide an example, a de-facto standard library from OpenZeppelin[5] was used to implement the Smart Contracts enabling elements of the previous architecture.

In the following, are reported some of the code snippets concerning the Product Contract and key part of the Solidity language code that represent a key for our discussion. The first being under focus is:

```
contract Product is ERC721,
                    ERC721URIStorage,
                    Ownable
```

This Solidity code makes the contract inherit from ERC721 to generate NFT (Non-Fungible Token) tokens and deem the product *Ownable* to increase overall security.

In the following code snippet it is shown how the Resource structure is defined. A Resource is a description of activities and products needed to compose a certain product at certain a step of the chain:

- *name*, represents the resource's name;
- *activityList*, represents the descriptive list of activities to create the resource;
- *activityGHGList*, represents the list of GHG emission related to the activities to create the resource;
- *otherResourceList*, other resources IDs used (if used) to create the link to other production steps in the chain;
- *GHG*, total GHG emission for the resource in CO2 equivalents;

```
struct Resource
{
  string name;
  string[] activityList;
  uint[] activityGHGList;
  uint[] otherResourceList;
  uint GHG;
}
```

The transfer of the Resource, and consequently the NFT token associated, is only allowed to the owner of the contract (through the *OnlyOwner* modifier), in this way the application can control the exchange of products, as follows:

```
function _beforeTokenTransfer(
    address from, address to,
    uint firstTokenId, uint batchSize
) internal virtual override onlyOwner
{
  super._beforeTokenTransfer(
    from, to,
    firstTokenId, batchSize
```

[5] https://www.openzeppelin.com/

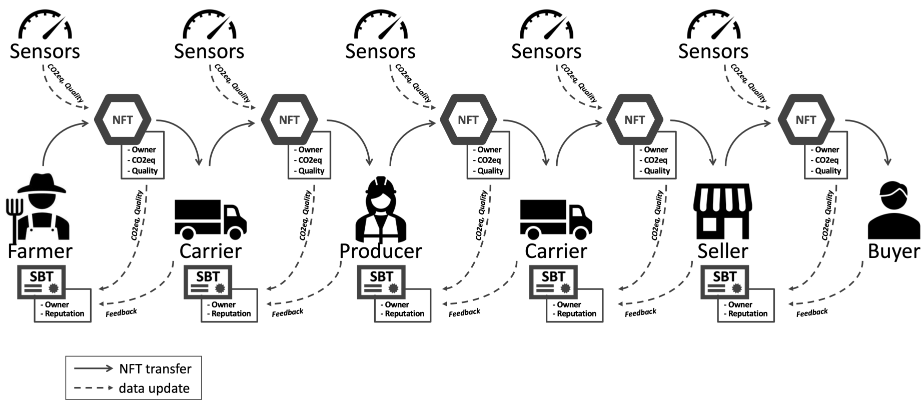

Figure 2. General workflow in the Food Supply Chain scenario

```
  );
}
```

Another pillar in the architecture presented in section 3, is the Reputation Contract. Still this contract inherits from ERC721 to generate NFT tokens (in particular Soulbound) and is Ownable to increase security.

```
contract Reputation is ERC721,
                       ERC721URIStorage,
                       Ownable
```

In this case, a function is devoted to valuation of reputation (*reputationCalc*) and another one for valuation of the trust (*trustCalc*). The functions are requested as parameters in the constructor.

```
function(
   uint[] memory, uint[] memory, uint[] memory
) external pure returns(uint) _reputationCalc;
function(
   uint[] memory, uint[] memory, uint[] memory
) external pure returns(uint) _trustCalc;

constructor(
  function(
    uint[] memory, uint[] memory, uint[] memory
  ) external pure returns(uint32) reputationCalc,
  function(
    uint[] memory, uint[] memory, uint[] memory
  ) external pure returns(uint) trustCalc
) ERC721("Trust", "TRS")
{
  _reputationCalc = reputationCalc;
  _trustCalc = trustCalc;
}
```

A Trust certification is first assigned to a certain actor in form of a Soulbound token, which is non-transferable and, in this very case, also non-burnable, as set in:

```
function _beforeTokenTransfer(
  address from,
  address to,
  uint tokenId,
  uint batchSize
) internal override(ERC721)
{ require(from == address(0),
          "Token not transferable!");
  super._beforeTokenTransfer(
    from, to, tokenId, batchSize);
}
```

With the former basic positions, it is now possible to define a performance-based reputation penalty algorithm. It can then be used to prevent opportunistic behaviour of a participant in the supply chain process. Performance-based reputation will be based on a value that is composed from a couple of essential components $< Rt(t), Rf(t) >$, where: the first component concerns the transferable part that depends on the current and the history of systemic measurements from the processing and transferred NFTs; the second one refers to the record of feedback received through a voting system up to the current time. The value of reputation that comes from the coupling of the two dimensions is the essence of the SBT that remains associated to a participant. A comprehensive $Rp(t)$ value can be obtained as a function of both the components, in general as a function or relation, $Rp(t) = R(Rt(t), Rf(t))$ in order to define a certain thresholds that is used to ban a non-well-performing and not-trustable user of the chain. Time series records since the beginning of a participant in the process chain might remain wholly available both for the computation of $Rt(t)$ and $Rp(t)$, or a certain temporal window τ might be used as a forgetting parameter. The $Rt(t)$ is a vector of indicators (performance components) that in our simple example in Figure 2 are the CO_2 equivalents and a measure of quality (against some conformity benchmark). However, these components can be multiple to include characteristics as health, shelf-life, organic, hazard analysis and critical control points (HACCP), fair-trade, etc. depending on the aims and principles of the supply chain. Moreover, the Rt integrates and inherits the effects of previous production steps as they are encoded in the informational content of the NFTs of other (preceding) participants along the value chain. The formalization of the $Rt(t)$ can then assume a rather complicated form, which in general can be simplified with a hierarchy of self-similarly normalized comprehensive indicators, as discussed by authors in [8]. The details on these expressions, their computational cost and implications are beyond the scope of this work. The current aim is to focus on the purposeful merge of transferable and non-transferable features of reputation. Thus, in its quite generic form, it can be let that Rp, the reputation functional, be a statistical functional (for example, being Rp a standard deviation over performance value records or the result of a federated machine learning process). Rp should in general depend on the dynamic evolution (history) of both the reputation values due to feedback and the values of Rt received along.

In order to let a shared policy determine or drive, in an automated way, the overall trust of the participants (as a an enforcement of a law), a suitable counter can detect how many times a (shared and agreed) performance threshold is overcome and, in case, eventually a participant undergoes a banning process – as exemplified by the pseudocode of Algorithm 1. There, R and P are the operators (functionals) that generate respectively Rp and Rt. $Rt_{new}[participant](t)$, $Rf_{new}[participant](t)$ are the data associated to the arrival of a new value of performance or reputation that triggers the contract. The *participant* index identifies the interested participant. $NFT[\{participants\} \setminus participant](t-1)$ is a vector of NFT values at time $(t-1)$ transferred by (possibly all) other antecedent participants in the chain. When available, the $Rt[participant](t-1, \cdots, t-\tau)$ and $Rf[participant](t-1, \cdots, t-\tau)$) are the time series of performance and reputation in a temporal window that goes from $t-1$ to $t-\tau$, being τ a chosen agreed value depending on implementation capability and dynamic properties. Then $reputation\_miss\_counter[participant]$ is incremented if the $reputation\_min\_threshold$ is not reached, and the number of these events are counted and checked against the $threshold\_counter$.

Algorithm 1: An algorithm for banning a bad-performing participant

```
Input Event: Rt_new[participant](t) ||
             Rf_new[participant](t)
Data: Rt[participant](t−1, ··· , t−τ);
      Rf[participant](t−1, ··· , t−τ) ;
      NFT[{participants} \ participant](t−1);
      reputation_min_threshold; threshold_counter;
      reputation_miss_counter[participant]
Result: reputation_miss_counter[participant] ;
        Rp(t); Rt(t)
Rt[participant](t) ← P( Rt_new[participant](t),
    Rt[participant](t−1, ··· , t−τ),
    NFT[{participants} \ participant](t−1) );
Rp[participant][t] ← R( Rt[participant](t),
    Rf_new[participant](t),
    Rf[participant](t−1, ··· , t−τ) ) ;
if Rp[participant](t) < reputation_min_threshold
 then
   reputation_miss_counter[participant] ++;
   if reputation_miss_counter[participant] >
    threshold_counter then
     ban the participant
   end
end
```

5 A Case Example

To materialize the argument with a minimal example, let us imagine the scenario in the context of Figure 2: a food supply chain case study. We will focus on the second participant in the chain, the *carrier*.

A food product's quality is systematically affected by the temperature, detected by three sensors that should travel remaining within a range of $[5, 10]$ degrees for preserving quality and health of supplied food. Another system is a temperature regulator (a cooling system) of which the energy efficiency is rated. Last performance rating could rate the punctuality of the transport. These sources of data can be treated and processed as oracular values in connection to a NFT of the carrier which will include also the NFT of the preceding participant (the *farmer*). Indeed, NFTs must be transferable so that they can be inherited by subsequent products along the supply chain, even if the initial and primary producer ceases operations or is replaced. This usually requires a normalization of the values by means of an adimensional indicator, for example using the form of a real ranging in $[0, 1]$ [8]. Moreover, in our example only one of the possible multiple dimensions of the performance parameters are used, assigning them here to a generic unique quality measurement. Thus, the overall rating values ranges from a minimum to a maximum, and the overall reputation value might be calculated using the following (very essential, for the sake of this example) formula:

$$\begin{aligned} Rp(t) \quad = \quad & avg(\ Rt_{reg}(t) + \sum_{i=1}^{3} Rt_{sens(i)}(t) + \sum_{k=0}^{\tau} Rf(t-k) + \\ & + Rt_{trans}(t) + NFT_{farmer}(t-1)\ ) \end{aligned} \tag{1}$$

where $Rp(t)$ is reputation at time t, $Rt_{reg}(t)$ is the temperature regulator rating, $Rt_{sens}(t)$ is the sensor's quality rating, $Rt_{trans}(t)$ is the transport quality rating, and avg is simply an average.

Let us suppose for this example that all the participants agree to set the reputation counter threshold ($threshold\_counter$ in Algorithm 1) to 30 at deployment time. If the reputation value elapses this threshold the owning participant may no longer perform operations in the chain. This is just a trivial example of centralized policy decision about reputation. In the most general case it can be set by the outcome of a consensus decision, which can be dynamically evolved in time. Reputation, as a whole, remains as an SBT, but the factors that create and update it are provided by the related NFTs. For the case example we used the Hyperledger Besu private blockchain. The source code of this example and some hints to use it can be found in the following repository: https://github.com/bdnqmt/GHG-Chain.

6 Conclusions and Future Work

This work tries to answer the three research questions presented in the introduction. As regards RQ1, thanks to the case study of the food supply chain provided by the European project ENOUGH, this work has shown how DLTs find a natural application in typical scenarios of Industry 5.0 and IoE where multiple, autonomous entities with often conflicting objectives coexist and none of them can assume the role of controller of the others. Thanks to these very characteristics, this approach can also be applied to other similar scenarios, such as the consumer goods and services industry, healthcare, and the construction industry [22, 13]. As for RQ2, tokens have proven to be of great utility for trust management. Responding to RQ3, this work proposes the use of

NFT and SBT, as fungible tokens can be useful when the accumulated trust makes sense to be spent as a currency. This is an aspect that deserves to be investigated in the future. In this scenario, trust is a score assigned to assets and participants that can only vary based on their behavior and history.

Future work will of course strengthen the experimental outcome of the approach with data from the real field. Moreover, the inquiry on the *reputation* computation can be deepened in many ways, to consider both neat mathematics or machine learning approaches. A challenging and still open problem to discuss and investigate in the context of NFT and SBT is the so-called *oracle problem* [10], in order to balance at best the off-chain and on-chain partitions of a DLT in the IoE context. Another challenge to consider is keeping DLT sustainable. While consensus protocols as proof-of-work have an unsustainable carbon footprint, there are now several efforts to drastically reduce CO_2-equivalent emissions while ensuring similar levels of security[6]. Finally, it should be considered that, to date, joining such a supply chain is on a voluntary basis. On the one hand, this can be seen as a limitation, as there is no guarantee that policy-makers are willing to impose a DLTs-based approach. An help in this direction could come from joining the European Blockchain Services Infrastructure (EBSI)[7] framework in its future evolutions. On the other hand, this can also be seen as an opportunity as in this way virtuous supply chains can be rewarded by final consumers.

7 Acknowledgments

This research is supported by the EU H2020 Project: ENOUGH (GA 101036588).

8 References

[1] M. Aaqib, A. Ali, L. Chen, and O. Nibouche. Iot trust and reputation: a survey and taxonomy. *Journal of Cloud Computing*, 12(1), 2023.

[2] S. Alam, S. Zardari, and J. A. Shamsi. Blockchain-based trust and reputation management in siot. *Electronics*, 11(23):3871, 2022.

[3] Y. Bai, K. Fan, K. Zhang, X. Cheng, H. Li, and Y. Yang. Blockchain-based trust management for agricultural green supply: A game theoretic approach. *Journal of Cleaner Production*, 310, 2021.

[4] A. Batwa and A. Norrman. Blockchain technology and trust in supply chain management: A literature review and research agenda. *Operations and Supply Chain Management: An International Journal*, 14(2):203–220, 2021.

[5] E. Bellini, Y. Iraqi, and E. Damiani. Blockchain-based distributed trust and reputation management systems: A survey. *IEEE Access*, 8:21127–21151, 2020.

[6] M. Bishop. *Computer Security: Art and Science. 2nd Edition*. Pearson, 2019.

[7] P. Bodorik, C. G. Liu, and D. Jutla. TABS: Transforming automatically BPMN models into blockchain smart contracts. *Blockchain: Research and Applications*, 4(1):100115, 2023.

[8] A. Bonci, S. Longhi, and M. Pirani. Prospective ISO 22400 for the challenges of human-centered manufacturing. *IFAC-PapersOnLine*, 52(13):2537–2543, 2019.

[9] P. Burgess, F. Sunmola, and S. Wertheim-Heck. Blockchain enabled quality management in short food supply chains. volume 200, pages 904–913. Elsevier B.V., 2022.

[10] G. Caldarelli. Understanding the blockchain oracle problem: A call for action. *Information*, 11(11):509, 2020.

[11] DG RTD, EU Commission. Industry 5.0 - Towards a sustainable, human-centric and resilient European industry. Available at `https://op.europa.eu/en/publication-detail/-/publication/468a892a-5097-11eb-b59f-01aa75ed71a1/` (2023/05/31), 2021.

[12] ENOUGH, g. a. No 101036588. European Food Chain Supply to Reduce GHG Emissions by 2050. Available at `https://enough-emissions.eu/` (2023/05/31).

[13] F. Esmaeilnezhadtanha, A. Hasani, S. Hakak, and T. R. Gadekallu. Blockchain-based cyber physical systems: Comprehensive model for challenge assessment. *Computers and Electrical Engineering*, 103:108347, 2022.

[14] M. Kjaer. Analyzing the use of blockchains for challenges in inter-organizational business processes. pages 137–140. Institute of Electrical and Electronics Engineers Inc., 2023.

[15] J. Leng, W. Sha, B. Wang, P. Zheng, C. Zhuang, Q. Liu, T. Wuest, D. Mourtzis, and L. Wang. Industry 5.0: Prospect and retrospect. *Journal of Manufacturing Systems*, 65:279–295, 2022.

[16] Y. Liu, J. Wang, Z. Yan, Z. Wan, and R. Jantti. A survey on blockchain-based trust management for internet of things. *IEEE Internet of Things Journal*, 10(7):5898–5922, 2023.

[17] Y. Liu, C. Zhang, Y. Yan, X. Zhou, Z. Tian, and J. Zhang. A semi-centralized trust management model based on blockchain for data exchange in iot system. *IEEE Transactions on Services Computing*, 2022.

[18] F. Longo, A. Padovano, and S. Umbrello. Value-oriented and ethical technology engineering in Industry 5.0: A human-centric perspective for the design of the factory of the future. *Applied Sciences*, 10(12):4182, 2020.

[19] S. Malik, V. Dedeoglu, S. S. Kanhere, and R. Jurdak. Trustchain: Trust management in blockchain and iot supported supply chains. In *2019 IEEE International Conference on Blockchain (Blockchain)*, pages 184–193. IEEE, 2019.

[20] J. Mendling, I. Weber, W. V. D. Aalst, J. V. Brocke, C. Cabanillas, F. Daniel, S. Debois, C. D. Ciccio, M. Dumas, S. Dustdar, et al. Blockchains for business process management-challenges and opportunities. *ACM Transactions on Management Information Systems (TMIS)*, 9(1):1–16, 2018.

[21] G. D. Putra, C. Kang, S. S. Kanhere, and J. W.-K. Hong. Detrm: Decentralised trust and reputation management for blockchain-based supply chains. In *2022 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pages 1–5. IEEE, 2022.

[22] L. Spalazzi, F. Spegni, A. Corneli, and B. Naticchia. Blockchain based choreographies: The construction industry case study. *Concurrency and Computation: Practice and Experience*, page e6740, 2021.

[23] F. Spegni, L. Fratini, M. Pirani, and L. Spalazzi. ChoEn : A smart contract based choreography enforcer. In *BRAIN 2023: Fourth Workshop on Blockchain theoRy and ApplicatIoNs, IEEE PERCOM 2023 The 21th International Conference on Pervasive Computing and. Communications, in press*, pages 1–8. IEEE, 2023.

[24] A. B. Tran, Q. Lu, and I. Weber. Lorikeet: A model-driven engineering tool for blockchain-based business process execution and asset management. In *BPM (Dissertation/Demos/Industry)*, pages 56–60, 2018.

[25] P. Vilchez, S. Jacques, F. Freitag, and R. Meseguer. Loratrust: Blockchain-enabled trust and accountability service for iot data. *Electronics (Switzerland)*, 12(9), 2023.

[26] K. Wang, S. P. Xu, C.-M. Chen, S. H. Islam, M. M. Hassan, C. Savaglio, P. Pace, and G. Aloi. A trusted consensus scheme for collaborative learning in the edge ai computing domain. *IEEE Network*, 35(1):204–210, 2021.

[27] M. Wang, Z. Zhou, and C. Ding. Blockchain-based decentralized reputation management system for internet of everything in 6G-enabled cybertwin architecture. *Journal of New Media*, 3(4):137, 2021.

[28] Y. Wu and Y. Zhang. An integrated framework for blockchain-enabled supply chain trust management towards smart manufacturing. *Advanced Engineering Informatics*, 51, 2022.

[6] `https://digiconomist.net/`

[7] `https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Home`