Smart Contract-Based Blockchain Solution to Reduce Supply Chain Risks

Fabian Dietrich, Ali Turgut, Daniel Palm, Louis Louw

Smart contract-based blockchain solution to reduce supply chain risks

Fabian Dietrich[1,3], Ali Turgut[2], Daniel Palm[1,4] [0000-0003-1485-8078] and Louis Louw[3] [0000-0001-9789-5661]

[1] ESB Business School, Reutlingen University, Alteburgstr. 150, 72762 Reutlingen, Germany
[2] Department of Industrial Engineering, Stellenbosch University, 145 Banghoek Rd., 7600, Stellenbosch, South Africa
[3] Steinbeis Innovation gGmbH, Alteburgstr. 150, 72762 Reutlingen, Germany
[4] Fraunhofer Institute for Manufacturing Engineering and Automation, Alteburgstr. 150, 72762 Reutlingen, Germany

fabian.dietrich@reutlingen-university.de

Abstract. Companies are becoming aware of the potential risks arising from sustainability aspects in supply chains. These risks can affect ecological, economic or social aspects. One important element in managing those risks is improved transparency in supply chains by means of digital transformation. Innovative technologies like blockchain technology can be used to enforce transparency. In this paper, we present a smart contract-based Supply Chain Control Solution to reduce risks. Technological capabilities of the solution will be compared to a similar technology approach and evaluated regarding their benefits and challenges within the framework of supply chain models. As a result, the proposed solution is suitable for the dynamic administration of complex supply chains.

Keywords: Blockchain, Smart Contract, Supply Chain Risk Management, Sustainability, Supply Chain Control.

1 Introduction

Companies are becoming increasingly aware of the potential risks arising from supply chains (SCs). Studies reveal that SC risks and associated business interruptions are considered to be one of the most important global business risks [1, 2]. This results in a growing need for proactive risk management in the SC across industries. Companies need to respond to these challenges in order to fully identify and manage risks in their SCs in order to understand and manage the risks and vulnerabilities [3].

Innovative and Industry 4.0 technologies like tracking and tracing with RFID, sensors and IoT-devices can be used to overcome these challenges [4, 5]. One of the current emerging technologies is blockchain technology, a distributed and immutable database that allows transactions to be conducted directly and transparently between parties [6] while at the same time permitting the programming of algorithms and rules of so-called

'smart contracts' [7]. Smart contracts are computer protocols which are developed and used to run decentralized applications on the blockchain [8].

Christopher and Peck [9] proposed to dividing risks in a SC context into three main categories: organizational risk sources that are internal to the company, network risk sources that are external to the company but within the supply network, and environmental risk sources that are external to the network. This classification clarifies the relevant dimensions of potential disruptions in a SC environment and thus provides the basis for a comprehensive risk analysis. The three main categories can be further broken down into five different areas of the SC where risks may occur (see **Fig. 1.**).

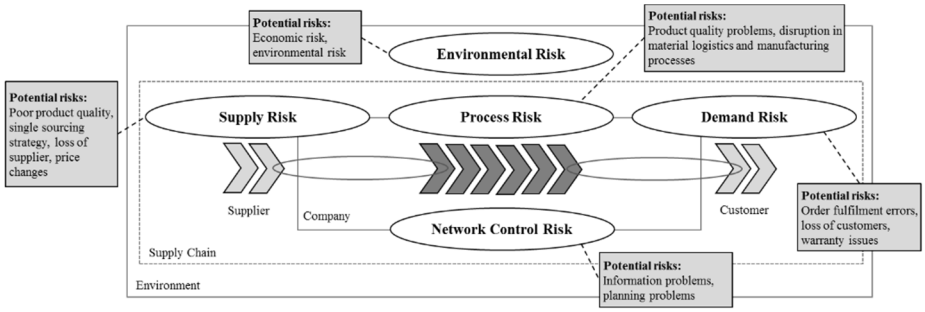

Fig. 1. Areas of supply chain risks (own illustration based on [4, 9, 10])

Based on the potential of the blockchain technology, research approaches use the technology as an innovative solution for challenges in the area of Supply Chain Risk Management (SCRM). Layaq et al. [11] for example, examined the potential of the blockchain in the area of supply risks which revealed that the use of blockchain and smart contracts can lead to improvements in material and information flows in order to reduce disturbance risks. This is enabled by increasing visibility (accessing or sharing information with participants of the SC network [12]), transparency (disclosure of information to all stakeholders, including customers [13] and transaction automation along the SC. Due to their structural design, traditional SCRM tend to take action reactively after damage has occurred. With blockchain technology it is possible to design action proactively and preventively as well as manage non-physical risks – such as cyberattacks or miscommunications – more efficiently [14].

This paper focuses on the area of network control risks, since the proposed smart contract-based blockchain solution aims to enhance the transparency and efficiency of information flows. Therefore, the paper briefly presents current problems with conventional token standards in this context. Subsequently, a new extended token-based approach is proposed. Finally, the characteristics of the two solutions are compared.

2 Background and rationale of the paper

Nowadays, companies have to deal with the growing interests of customers, governments, and non-governmental organizations in having a greater transparency of brands,

manufacturers, and producers throughout the SC [15, 16]. As a result, social and environmental sustainability issues have become increasingly important for manufacturers in order to maintain the flawless reputation of their brand [17]. However, as SCs become more global, many suppliers in the network can be located in developing economies where governments have only limited ability and willingness to enforce their own laws [16]. In addition to the risk of being unintentionally involved in social and environmental sustainability issues, a lack of transparency also increases the probability of counterfeit components being introduced into a SC. For example, the counterfeiting of electronic parts causes potential risks including safety and loss of profits to companies, as well as maligning the reputation of manufacturers and distributors [18–20]. It can therefore be summarized that the dispersed nature of today's SCs creates increasing levels of network control risks for multinational businesses, making transparency of SCs both critical and complex [21, 22]. Notably, the problem of incorporating tampered counterfeit parts in assemblies introduces a vulnerability that must be prevented and a gap in present research [18].

In particular, when applying the blockchain technology to SC management, companies have high expectations to solve transparency and auditability issues of complex collaborative SCs [7, 23]. A first approach by Abeyratne et.al. proposes that physical assets in combination with their 'unique digital profiles' on the blockchain can solve transparency problems of manufacturing SCs [24]. Based on this approach, Westerkamp et.al. developed a solution using special non-fungible tokens in order to represent batches of manufactured products on the blockchain [25]. However, conventional non-fungible token standards such as the ERC-721 [26] are not specifically designed to map SCs. In combination with the immutability of the blockchain technology [25], non-fungible tokens enable a static reconstruction of SCs but show weaknesses when mapping dynamic changes in the composition of products or the structure of the SCs.

3 Extended token-based solution

This paper proposes a new solution aiming to create a smart contract with a static address on the network, but still enabling a dynamic mapping of changes in the SC. In conventional token standards, a transaction to change a token's ownership does not send the token itself to a new address; it is an interaction with the token contract assigning a new owner address to the token. This fundamental functionality of tokens is used to create a new approach specifically designed to adopt supply chain characteristics.

From the very beginning, this extended smart contract-based approach includes the identification and mapping of all stakeholders in the supply chain. For this purpose, the SC participants are divided into SC partners (suppliers, producers and service providers), customers and certifiers [25, 27]

Similar to the token standard-based approach [25], the creation of virtual identities on the blockchain is strictly connected to dependencies reflected in their 'recipes'. In this context, a distinction can be made between two types of assets:

- *Assets without dependencies*: can be created without depending on previous actions (e.g. raw materials or certificates).
- *Assets with dependencies*: can only be created when previous actions have been successfully conducted.

In order to map SC processes, the virtual identities of assets must have the same ownership and conversion characteristics as their physical counterparts. They must be able to change their owners when the physical product is transferred in the SC or sold. Furthermore, the virtual identities must be able to be summarized when combining several components into a new product. These events can then be tracked in the blockchain and are accessible for all partners in the SC. All nodes of the network agree on a common time by implementing a consensus algorithm. As a result, the immutability of the network guarantees that a certain event on the network happened at a certain time **Fig. 2**.

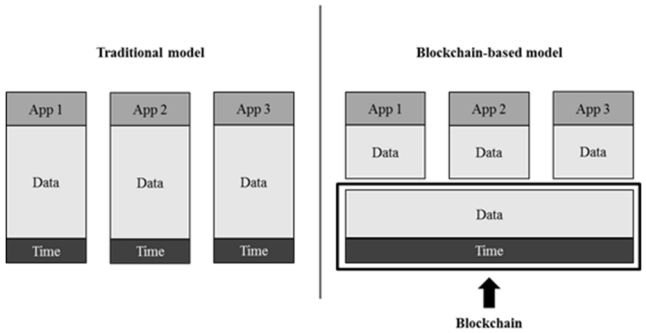

Fig. 2. Blockchain technology as verified public timestamps (based on Grossman [28])

To ensure this traceability by using the blockchain technology, a link between the blockchain and the physical product must be established. Accordingly, this approach assumes that all data can refer to an asset itself. For this purpose, the smart contract generates unique identification identities (IDs). A unique ID refers to the virtual identity of an asset. For the uniqueness of these IDs the extended solution proposes hashing the asset's information. Therefore, Hash IDs are a logical result of their input data and provide initial information about the origin, composition, and time of creation. Hash IDs can also be referred to as the smart contract version of conventional primary keys. Within the smart contract, these Hash IDs refer to the virtual identity of their physical counterparts. Similar to other blockchain approaches, these Hash IDs can be attached to the physical parts in the form of barcodes, RFIDs or QR codes [24]. The smart contract logic of a function creating an asset with dependencies is shown in **Fig. 3**. To map such a logic, it requires the modelling, planning, and definition of further various smart contract functions. Therefore, it is necessary to carefully design all required conditions to create the virtual identity of an asset and its associated Hash ID. The creation of assets is firmly bound to the address of the responsible entity. This means that only a selected authorized entity is able to create the respective virtual identity. The address of the creator is then authorized to send this virtual identity to a new owner. As soon as

the transaction has been successfully confirmed by the network, only the new owner has the rights to cause further actions related to the sent virtual identity. In this way, the same functionality in terms of asset 'moving' and asset 'recipes' as with non-fungible token standards can be achieved, except that there is now more scope to link the respective smart contract functions to defined authorities and to execute dynamic adjustments.

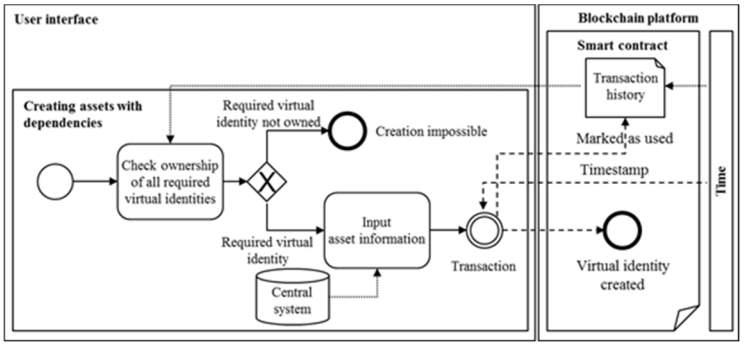

Fig. 3. Model to create virtual identities for assets with dependencies

Since the structure of SCs is subject to dynamic influences, the smart contract must also allow dynamic changes of its content. This not only affects the modification of structural elements but also the composition of products. An initial design of such a dynamic smart contract structure is presented in section 3.1.

3.1 Holistic smart contract structure

The assigned authorities and the functions for creating virtual identities are embedded into algorithms allowing the mapping of dynamic changes in the SC while the smart contract's address remains static. For these complex algorithms, this paper proposes to include existing approaches to continuously update and generate smart contracts [27, 29]. **Fig. 4** shows the design of the holistic smart contract structure.

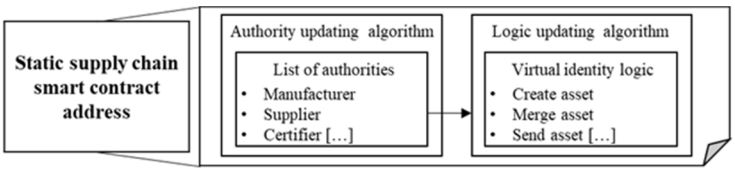

Fig. 4. Holistic smart contract structure

Such a structure allows a wide range of possibilities in terms of the allocation of authorities, which is determined in the dynamic updating algorithm related to the list of authorities. It is possible to virtually represent decentralized and open SCs with an even distribution of power, as well as strictly regulated SC structures with only one central authority. As illustrated in **Fig. 4**, this determines to what extent the authorities can have an impact on changes in the virtual identity logic.

It is important to state, that such smart contract constructs are affected by the immutability of the blockchain technology. Consequently, any eventuality that could affect the SC or product structure must be considered in the program code before its deployment. If, for example, the addition of new suppliers is not taken into account in the code, they cannot be added. A new smart contract with a new address must be deployed. Furthermore, the proposed structure allows involving privacy approaches to encrypt the content of the smart contract [30]. In this way, the interactions with the contract would remain visible to the public to provide SC transparency. The content of these transactions, however, would be encrypted and only visible for a defined group of authorities.

4 Comparison of solutions and conclusion

This section compares the characteristics of blockchain-based Supply Chain Control Solutions. On the one hand, these are the characteristics of the ERC-721-based smart contracts [26] (non-fungible token-based standard) which was adopted by Westerkamp et al. [25] for manufacturing SCs and on the other hand, the characteristics of the extended token-based solution proposed in this paper (see **Table 1**).

Table 1. Comparison of blockchain-based Supply Chain Control Solutions

	Advantages	Disadvantages
Conventional token-based solution	No central authority necessary, changes in the Supply Chain (SC) can be decided decentrally and must be made downstream.	End producer can only react to changes in the SC and product changes require new tokens downstream. This leads to high change effort in complex SCs.
	Fast technical implementation.	Structural changes in the SC difficult to implement (the more complex the SC, the more difficult).
	Standardized tokens (e.g. ERC-721) freely accessible to the public.	Privacy is not given in public networks.
	No predefined SC-structure necessary. Tokens can be sent freely and without restrictions.	Data waste of worthless tokens in the system.
Extended token-based solution	Definition of authorities facilitates coordination of SC partners.	More elaborate planning necessary since all change contingencies must be considered in advance.
	Complex SCs can be mapped easier through central control.	Not necessarily open to the public; private, semi-private or public smart contract on a public blockchain possible.
	Parts of the smart contract can be encrypted for the public (only accessible for selected partners) .	Possibly no balanced distribution of power in the administration of the smart contract (some authorities may receive additional power over the SCs).
	Enabling product and structure changes by continuously updating the smart contract.	The complexity of the technical implementation increases with the degree of individualization of the solution.

An analysis of the two solutions in terms of suitability for SC types (see, for example, Lee [31]) shows that the conventional non-fungible token standard is mainly suitable for simpler SCs following an efficient strategy with a single source approach with a low number of changes over time. This makes it much easier to implement and manage downstream changes in the SC. In responsive scenarios the flexibility also means that the product must be constantly adapted and changed according to the requirements of the customer [31]. Therefore, a responsive strategy is preferably suitable in combination with the proposed smart contract-based solution allowing continuous configurations. This also applies to companies choosing more flexible strategies, such as the risk-

hedging strategy and agile strategy. Especially in complex SCs, this solution allows a continuous administration of the SC and the adoption of structural changes. To what extent the changes of such complex SCs can be foreseen when designing the smart contract, should be further investigated. The limitations of the dynamics in the SC in terms of product composition and SC structure also need to be researched. Since the flexibility and the resulting complexity of SCs depicts a challenge [5], the proposed solution represents a promising approach for industry sectors with a high degree of product customization like the automotive industry or sectors following Industry 4.0 concepts. Further research on this topic is currently being conducted. Furthermore, it is necessary to investigate the scalability of such solutions, since the scalability currently represents a limitation of the blockchain technology.

References

1. Dobie, G., Hubmann, et. al.: Allianz Risk Barometer - Results Appendix 2020. Allianz Global Corporate & Specialty (2020)
2. Dobie, G., Milla, et. al.: Allianz Risk Barometer. Allianz Global Corporate & Specialty (2019)
3. Palm, D., Kales, P.: Efficiency-oriented risk prioritisation method for supply chains in series production. International Conference on Competitive Manufacturing 2016, 417–422
4. Kersten, W., Schröder, M., Indorf, M.: Potenziale der Digitalisierung für das Supply Chain Risikomanagement: Eine empirische Analyse. In: Seiter, M., Grünert, L., Berlin, S. (eds.) Betriebswirtschaftliche Aspekte von Industrie 4.0, 47-74. Springer Fachmedien, Wiesbaden (2017)
5. Ivanov, D., et. al.: The impact of digital technology and Industry 4.0 on the ripple effect and supply chain risk analytics, Int. J. Production Research 57(3), 829-846 (2018)
6. Bosch, R., Penthin, S.: Blockchain als Treiber im modernen Supply Chain Management 4.0. BearingPoint (2018)
7. Iansiti, M., Lakhani, K.R.: The Truth About Blockchain. Harvard Business Review, 118–127 (2017)
8. Buterin, V.: Ethereum White Paper: A Next Generation Smart Contract & Decentralized Application Platform (2013). https://blockchain-lab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf. Accessed 20.03.20
9. Christopher, M., Peck, H.: Building the Resilient Supply Chain. The International Journal of Logistics Management 15(2), 1–14 (2004).
10. Kales, P.: Development of an efficiency-oriented risk prioritisation method for supply chains in series production. Thesis, Reutlingen University (2015)
11. Wasim Layaq, et. al.: Blockchain Technology as a Risk Mitigation Tool in Supply Chain. Int. J. Transport. Engineering and Technology 5(3), 50–59 (2019).
12. Barratt, M., Oke, A.: Antecedents of supply chain visibility in retail supply chains: Journal of Operations Management 25(6), 1217–1233 (2007).

13. Doorey, D.: The Transparent Supply Chain: from Resistance to Implementation at Nike and Levi-Strauss. Journal of Business Ethics (103), 587–603 (2011).
14. Min, H.: Blockchain technology for enhancing supply chain resilience. Business Horizons 62(1), 35–45 (2019).
15. New, S.: The Transparent Supply Chain (2010). https://hbr.org/2010/10/the-transparent-supply-chain. Accessed 20.03.2020
16. Chen, S., et. al.: Impact of Supply Chain Transparency on Sustainability under NGO Scrutiny. Production and Operations Management 63(9) (2018).
17. Lemke, F., Petersen, H.: Managing Reputational Risks in Supply Chains. In: Khojasteh, Y. (ed.) Supply Chain Risk Management, pp. 65–84. Springer, Singapore (2018)
18. Collier, Z.A., et. al.: Supply Chains. In: Kott, A., Linkov, I. (eds.) Cyber Resilience of Systems and Networks, vol. 2, pp. 447–462. Springer, Cham (2019)
19. Pecht, M.: The Counterfeit Electronics Problem. JSS 01(07), 12–16 (2013)
20. DiMase, D., Collier, Z.A., et. al.: Traceability and Risk Analysis Strategies for Addressing Counterfeit Electronics in Supply Chains for Complex Systems. Society for Risk Analysis 36(10), 1834–1843 (2016)
21. Linich, D.: The path to supply chain transparency. Deloitte Uni. Press (2014)
22. Brandon-Jones, E., Squire, B. et. al.: A contingent resource-based perspective of supply chain resilience and robustness. Journal of Supply Chain Management(50), 55–73 (2014)
23. Hackius, N., Petersen, M.: Blockchain in logistics and supply chain: trick or treat? Hamburg Int. Conference of Logistics (HICL) 23, 3–18 (2017)
24. Abeyratne, S.A., Monfared, R.P.: Blockchain ready manufacturing supply chain using distributed ledger. Int. Journal of Research in Engineering and Technology 05(09), 1–10 (2016).
25. Westerkamp, M., et. al.: Tracing manufacturing processes using blockchain-based token compositions. Digital Communications and Networks (2019).
26. Entriken, W., Shirley, et.al.: EIP 721: ERC-721 Non-Fungible Token Standard (2018). https://eips.ethereum.org/EIPS/eip-721. Accessed 2020/03/31
27. Bechini, A., et. al.: Patterns and technologies for enabling supply chain traceability through collaborative e-business. Information and Software Technology 50(4), 342–359 (2008).
28. Grossman, N.: The Blockchain as verified public timestamps (2015). https://www.nickgrossman.is/2015/the-blockchain-as-time/. Accessed 20.03.2020
29. Frantz, C., Nowostawski, M.: From Institutions to Code: Towards Automated Generation of Smart Contracts. International Workshops on Foundations and Applications of Self-Systems 01, 210–215 (2016).
30. Yuan, R., Xia, Y.-B., et. al.: ShadowEth: Private Smart Contract on Public Blockchain. J. Comput. Sci. Technol. 33(3), 542–556 (2018).
31. Lee, H.: Aligning Supply Chain Strategies with Product Uncertainties. California Management Review 44(3), 105–119 (2002).