Impact Analysis of Industrial Standards on Blockchains for Food Supply Chains

Themo Voswinckel, Dino Hardjosuwito, Torben Gehring, Ralph Siruet, Andreas Fuessler

Impact Analysis of Industrial Standards on Blockchains for Food Supply Chains

Themo Voswinckel[1], Dino Hardjosuwito[1], Torben Gehring[1], Ralph Siruet[2] and Andreas Fuessler[2]

[1] Institute for Industrial Management (FIR) at RWTH Aachen University, Campus-Boulevard 55, Aachen, Germany
info@fir.rwth-aachen.de
[2] GS1 Germany GmbH, Maarweg 133, Cologne, Germany
service@gs1-germany.de

Abstract. One of the major challenges for the use of the Blockchain technology in industrial applications is the lack of existing standards. They ensure the interoperability of sensors, machines and the data-sharing between stakeholders within a food supply chain. Existing Blockchain-independent implementations of technologies for increasing transparency in supply chains use communication standards whose transferability to Blockchain applications has not yet been analysed sufficiently. This publication analyses the suitability of established standards regarding their use in Blockchains. In this context, the requirements for the distributed database and for the protection of sensitive company data must be considered. Therefore an analysis of eventually necessary changes is executed for the adoption of standards and how they could be implemented.

Keywords: Food chain, supply chain management, Blockchain, standards.

1 Introduction

1.1 The Need for New Solutions in Food Supply Chains

The continuing emergence of scandals within the food industry causes increasing uncertainties among consumers regarding the quality of their daily shopping. One example is the fipronil scandal in Europe in 2017, where an insecticide was discovered in chicken eggs. The total number of the affected eggs only in Germany was estimated to be between 10.7 Million and 35.5 Million [1]. Another example is a meat scandal concerning the German meat producer Wilke in 2019, where Listeria germs were discovered in meat products, which caused three deaths and 37 cases of strong illness [2]. These are only two examples of many in the food industry, which follows as an industry with dynamic company interactions big challenges for the network[3]. Reinforced by several crises, the demand for transparency in supply chains, as a question of risk prevention and consumer protection, has become a general demand for improved access to information in order to regain consumer confidence in food [4]. Through an open-accessible database for value-creating partners, public authorities and end consumers,

the chance to detect problems such as the named ones in a faster way can be realized and all concerned supply chain participants can be informed immediately [5].

The degree of trust directly determines the success potential within company-wide networks. This trust can be provided by secure and independent technologies, which therefore can perceive as a promoter for trust and supporter for the success of collaborative networks. [6] A determining factor is the latency between the steps of detecting an event and initiating countermeasures. By applying the Blockchain technology, it is possible to reduce latencies and the impact of an event on the entire supply chain up until the end consumers [7]. Due to the diverse information system architectures of the interacting parties, sensors, machines and products generally do not speak the same "language" today. [8] What's more, companies use different methods to gather, aggregate and exchange data. By using common dictionaries, models and communication standards, companies can facilitate data sharing and accelerate data aggregation and analysis. Companies or their service providers can define proprietary structures for each data-sharing project or they can select from among widely accepted reference architectures and standards. [8] However, there are currently no standards for the use of Blockchain technology [9].

Several organizations address this problem, aiming to facilitate interoperability in Blockchain solutions. Standardization institutions, such as the International Organization for Standardization (ISO), developed standards to increase transparency and harmonization within Blockchain solutions. The standard ISO 20614, for instance, is a data exchange protocol with a focus on interoperability and preservation. Furthermore the member-driven standard organization Enterprise Ethereum Alliance focusses on open Blockchain specifications, which should lead to interoperability and harmonization within Blockchain solutions. There is also GS1, which is a network of not-for-profit organizations that develops and maintain standards to identify products unambiguously. Using these unique identification numbers, companies are able to connect different Blockchain solutions. [8]

The described problem is analyzed and outlined in the following chapters. The main focus is on the conceptual comparison of existing traceability processes with Blockchain-based processes. By using established GS1 standards, such as Electronic Product Code Information Services (EPCIS) or Core Business Vocabularies (CBV), an analysis of the transferability takes place.

1.2 The Research Project "SiLKe" addresses the Needs of new Data Exchange Solutions

The project with the name "SiLKe", which is funded by the German Federal Office for Education and Research (BMBF), takes up the possibility of using the Blockchain technology in supply chain management and investigates a possible implementation of such a solution for food supply chains. The project addresses the requirements on a technical solution from the perspective of the different supply chain stakeholders, transfers these requirements as challenges for the use of a Blockchain and develops a practicable application. One of these challenges, which will be addressed within this paper, is the lack

of industry standards for applying a Blockchain solution within an industrial supply chain under consideration of the existing individual IT-infrastructure of each integrated company [9].

2 Applying Standards for Data Management in Blockchain Applications

As the base for a qualified evaluation regarding the implication of applying a Blockchain on the compatibility of industrial cross-company process standards, the first step is to understand the high number of necessary standards which are required for different business processes. The following Figure 1 gives an overview about the industrial standards established by GS1, which will we considered as a reference within the following analysis.

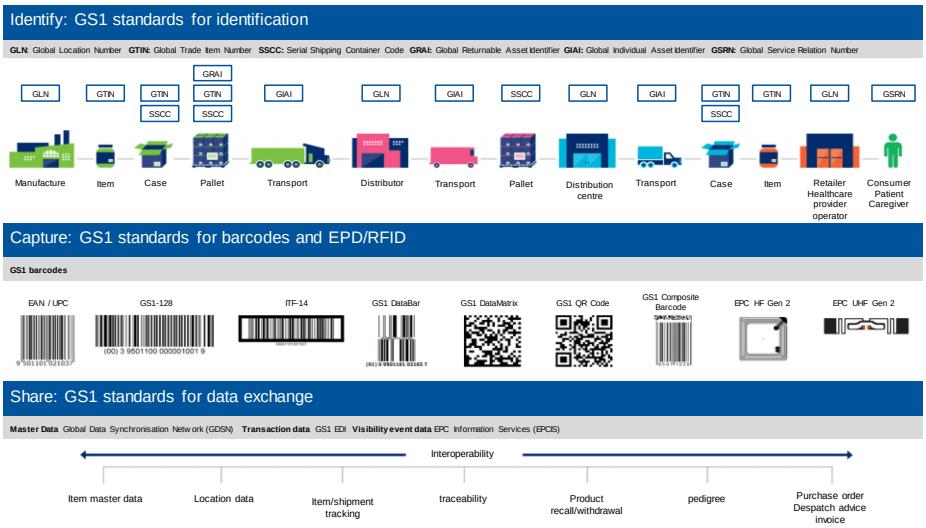

Fig. 1. Overview of industrial standards of GS1

In the following, especially the data management is considered as one of the main aspects to be addressed in the context of Blockchain applications. The focus here is on looking at the different types of data, how this data is generated, stored, backed up and exchanged. These topics are enriched, ensuring appropriate data quality and compliance with data protection. By describing the relevant aspects as they are handled today without the use of Blockchain technology, a comparison is thus made between three different technological approaches (traditional, i.e. without Blockchain, with a Permissioned Blockchain and with a Public Blockchain).

2.1 Data Type

In the context of production networks, the three different kinds of data types, master data, transaction data and event data exist for tracking and tracing information along a supply chain [10]. In the following, they will be presented and evaluated with regard to their usability in a Blockchain solution.

Master Data. Master data is the source of common business data that is used for all systems, applications and processes of an entire company. A further distinction is made between static master data, which is largely unchangeable over time, and relationship master data, which represents data of customers and suppliers. Hereby the identification of a unique designation of e.g. companies, products and locations is necessary. [10]

Both kinds of master data can also be exchanged or retrieved via a Blockchain since there is no technical difference between the data and both can be recorded in a Blockchain. Therefore no adjustments are necessary on the technical side. In the case that not all master data is available in the same format for each ecosystem stakeholder, general regulations for the exchange of master data must first be formulated.

Transaction Data. Transaction data is recorded as a result of business transactions, e.g. at the conclusion of a transfer of ownership (e.g. purchase orders, invoices) or the transfer of custody of goods (e.g. transport advice, proof of delivery) [10]. Hereby the identification system serves as an access key to more detailed information as used in the exchange of transaction data [11]. All relevant event data related to business processes from ordering to invoicing can be exchanged via standardized electronic message types. Transaction data can also be exchanged or accessed via a Blockchain. The question arises whether the transaction data itself should be stored in the Blockchain or whether the visible events that triggered transaction data transmission (e.g. a shipping notification) should be recorded in the Blockchain and should be made retrievable.
In the first case, the existing processes for transaction data have to be transferred to the Blockchain. To do this, generally valid regulations and recommendations for the exchange of transaction data by Blockchain would have to be developed first, since these do not exist today with regard to the Blockchain technology. This requires corresponding standardization efforts. A sender and a recipient of a shipping notification, for example, have an essential interest in not giving third parties (such as competitors) any insight into the flows of goods and quantities that can be read from shipping notification data. This goes beyond pure data content and also includes access rights and encryption issues. The development of a proprietary solution for this would be an obstacle to scalability. [11] In the latter case, new event data would be added to the Blockchain, which would be redundant to conventional process data. It is the same process as if the sender and recipient apply the classic EDI message (such as a shipping notification) and get automatically informed of an event. [11]

Event Data. Event data are records of the completion of business process steps in which physical or digital entities are handled. Each event records which objects participated

in the process, when the process took place, where the objects were and will be located afterwards and in what business context the process took place. [10]

Event data represents the category of data types that receives most attention within a Blockchain application for supply chain use cases. One of the core aspects of the SiLKe-project is to exchange this data between the partners by means of a Blockchain. Visible event data does not initially have any influence on the process comparison (with or without Blockchain). [11]

2.2 Data Generation

Before storing data in a Blockchain it is necessary to generate the data. For the first step of data generation, the identification of the respective objects requires special identification keys that enable the differentiation between the different types of objects which are shown in figure 1. These are for instance identities for products, for companies and locations, for logistic units and for returnable assets such as vehicles or transport equipment [10]. For the next step, the capture of the data, standardized data carriers are required. Examples are Barcodes as well as RFID-Transponders [10]. With these data carriers it is possible to identify objects by their specific product identification number.

The data generation is one of the upstream processes of the Blockchain and can be realized identically as without a Blockchain. By standardizing the codes and the data carrier, it is possible for each member of the supply chain to read and generate the data for tracking information. The same technology can be used for generating data in a Blockchain solution because the generation is independent of the storage of the data. Here it is important that the data carrier is readable. Nevertheless, a change from bilateral to multilateral data exchange within a Blockchain may change the situation of data access (scope) and the way the generated data is presented (e.g. data encryption or provision of references where data can be found). [11]

2.3 Data Storage

Another important aspect in the context of data management is the storage of data. In currently existing standardization systems, the storage of data is managed depending on the data type. In the case of GS1, the company issuing these Global Location Numbers (GLN) is responsible for keeping business partners informed of all GLNs related to their trading relationship. In contrast, the visible event data is stored in a decentralized way. The companies have their own repository where they save their generated data. Such a repository has an acquisition interface for storing and a query interface for requesting event data. Each entity stores the event data relevant to them and exchanges relevant entries with business partners [12].

In the case of applying a Blockchain, it should represent the repositories and act as a distributed storage network with all the typical technological benefits of a Blockchain. As a consequence, the individual repositories must back up much more extensive data, as they back up the replicated content holistically, which means that scaling problems must be taken into account. In Fig. ***2*** a possible realization of an integration of a Blockchain in the supply chain is shown. Every company generates its data on its own and

represents a node in the Blockchain network. Regarding the requirements of the different types of data, a related storage strategy is applied and only the event data is stored in the Blockchain.

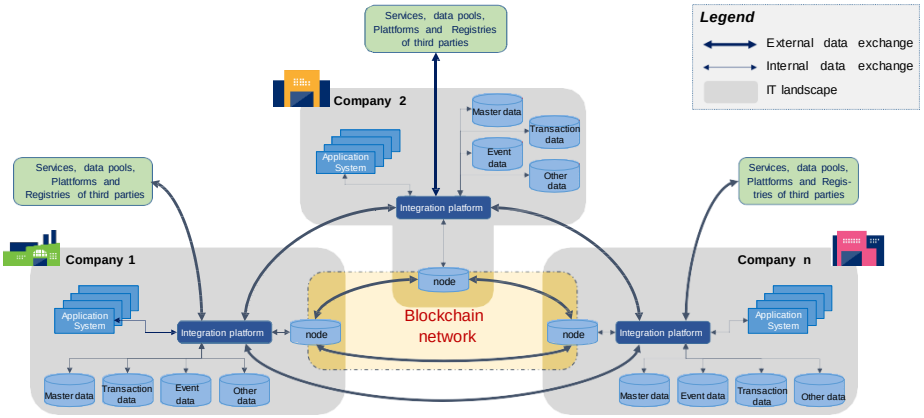

Fig. 2. Transfer of existing traceability processes into a Blockchain application [11]

Due to the fact, that the Blockchain is transparent and every node has access to the data, the question arises how the event data is stored in the Blockchain. There are several ways to store the data. First, the data can be stored completely unencrypted and is only signed cryptographically. The second option is to store only the cryptographic hash value of the data and link the address of the unencrypted data's storage location, which would not be stored in the Blockchain itself. Another option is a combination of these two ways to store the data. In this case, it should be evaluated which option is the most suitable for a food supply chain due to companies' business secrets and the Blockchain scalability. [11] Within the framework of the research project a combination of unencrypted and encrypted data will be used. This is because business secrets are important for companies and not every event data has to be shared with every network member.

2.4 Data Quality

In addition to the generation and storage of the data, the data quality plays a significant role in the context of industrial standards and depends on several factors. In the context of data quality, the aspects of data responsibility, conformity with relevant data as well as the checking of data for completeness, correctness and consistency are dealt with below.

Responsibilities. An important element to be taken into account with regard to the requirements for a traceability system are regulations on the responsibilities for data management. In dependence of the kind of asset to be managed, different roles are accountable for the generation of those assets. The right for the allocation of item identifiers is in the case of GS1 managed by the manufacturers themselves. The interacting parties are responsible for their personal representation. The pallet identification number is either created by the logistics company or to be conveyed by the manufacturer of the

goods [10]. Each participant involved in one of the business processes is responsible for the collection, recording and distribution of event data. An important use case in the context of responsibilities is the case of product recalls. Within the GS1 framework, the notification of the product recall has to be made by the originator of the product recall. After that, the responsible authority has to be identified before the affected partners can be informed. The concerned person regarding the product recall is responsible for confirming that the products have been removed. In the end, the initiator of the product recall is responsible for the final report of the product recall. The responsibility for the created events lies entirely with the creator of the event, who also secures the event. [13] The use of a Blockchain as a means of data exchange does not change the responsibility for the origin of the data. In this regard, the structure above needs to be considered analogously when applying a Blockchain.

Review of the Data. The generated and transferred data must meet defined quality requirements regarding completeness, correctness and consistency. To guarantee these requirements, various verification mechanisms need to be provided. The completeness of the data can be ensured by the predefined length of identification numbers (for those with fixed lengths). Since they are composed of different contextual elements, all of them have to be filled with information. [11] More challenging is the review of data regarding correctness. The use of automated data collection technologies increases the safety of reading data correctly. Especially the dimensions “what”, “where” and “when” can benefit from that. In this case, the "what", i.e. the object of detection, is usually recorded automatically. This happens by using standardized identifiers on the object and by using a corresponding reader for the identifiers. The “where” can be captured in the same way by scanning a barcode or transponder of the corresponding location. In case of a predefined location such as a warehouse gate, the dimension “where” can be registered in the system, whereby every scanned product can be allocated with the ID of this location. The "when" can be automatically tracked in the moment of the query. [11]

This standardized data checking procedure can also be transferred to a Blockchain application. Event data can be checked regarding completeness in the same way and data can be captured automatically with the reading standards and technology. Due to the opportunities offered by the Blockchain technology, Smart Contracts can be used for automated reviewing processes. In addition, they offer further opportunities for the automation of data acquisition. Human sources of error can mostly be eliminated by this automation. In this context, it must be examined which existing verification mechanisms are better (more effective, simpler, less expensive) for Smart Contracts and which verification mechanisms should be replaced by them. [11]

Updating and Correction of Data. The last topic in the context of data quality focusses on the aspect of updating or correcting data which has already been saved and shared within a company ecosystem. Due to the tracing of all events during the value creation of an object, it is possible to reconstruct the whole supply chain history. Status updates from objects are generated by creating a new event. It would work in the same way in

a Blockchain solution. New events would be stored in the Blockchain and the tracing of all events successively builds up a production history. [11]

However, it cannot be ensured that faulty data doesn't get into the Blockchain. In such a case, the data cannot be simply deleted or overwritten. Within the GS1 standard, a subsequent correction event is generated, that corrects a wrong event. [12] The application of a Blockchain and the previously described approach have in common that no faulty block can be simply deleted or replaced. Instead, a new block entry must be entered into the Blockchain containing the corrected information. The correction event could most likely be adopted in a Blockchain solution. Within a consensus method, it is mandatory, that the participants decide if the corrective transaction should be added. This raises the question of whether other participants even have the knowledge to decide on the correctness of other participants' data. At this point, Smart Contracts could again play a supporting role. [11]

2.5 Data Exchange

Another aspect which has to be considered is the data exchange, which needs to get realized with different interfaces. Within the GS1 standard, three different interfaces exist [14]. The first interface is the data acquisition interface, which offers the possibility to share data via a website and to send conforming messages to the company IT infrastructure. [11] The second interface is a query control interface, which has two different modes. In the on-demand mode the service-requesting device makes a request and receives an immediate response. In the standing-request mode, the service-requesting device subscribes to a periodically recurring query [14]. The third interface is a query callback interface. Whenever a query service is executed, its results are passed on at the same time. [14]

The data exchange itself can be structured architecturally in various ways. In the simplest case, the centralized repository is shared with all value-adding partners [12]. In the case of distributed push choreography, each entity in the supply chain keeps the collected data in its own EPCIS repository. If necessary, each partner can receive and forward it to every partner in the supply chain. No EPCIS queries are involved since the exchange of all events is triggered directly [12]. In the third case of the distributed query choreography, each party in the value chain keeps the collected data in its own local repository. Any party that needs data from another party has to request it [12].

In principle, all three described architectures can also be theoretically realized using Blockchain technology. In an independent architecture, none of the participants would represent a data-holding node and the Blockchain would be the data-providing system. This would mean a complete externalization of the data holding. With the distributed push choreography, the data would be cumulated in the Blockchain, so that the result would be a significant amount of redundant data in the Blockchain. Of the three choreographies, the distributed query choreography has the greatest proximity to a Blockchain, in which the query is regulated via rights management. So this rights management can be used as a guideline for a Blockchain solution. [11]

2.6 Privacy

With regard to data protection, the question of how personal data can be protected against misuse must be investigated. With applying non-speaking identities as randomized events and article numbers, conclusions about the underlying products or identities are excluded. A conclusion on the context is only revealed with the respective access rights. Identities should have the aim to identify objects in an economic context and not the involved individuals. The tracked "who" entity within an event is always a company or a company section but never the acting person behind it. In addition, each application should have a reliable system of rights indicating which subscriber can view which information. [11]

The described approach above can also be applied to a Blockchain. To ensure that only permitted entities get access, a clear role and right management is necessary. It has to be clearly defined who may read what kind of data from which network partner. Therefore, it is necessary to make use of appropriate encryption methods. At the same time, it must be ensured on the process side that, even with a high level of transparency, no conclusions can be drawn about the persons who are connected with the data. [11]

3 Conclusion and Outlook

The assurance of standards for the system-wide exchange of information in business relationships is an essential cornerstone for a functioning supply chain. As we have seen there are a lot of existing company-wide process standards that can be projected onto a Blockchain solution, which was validated within the reseach project consortium. The unique identification through the identities enables the non-overlapping recording of object-related data. The storage of the data in the form of events can also be used in a Blockchain solution. In this case, it is necessary to define what data and what information should be captured and stored. A standardized data carrier for an automatic and fast identification of objects plays an important role in the data generation. Updating or adding information as the production progresses can be carried out seamlessly by applying a Blockchain.

The use of Smart Contracts offers the opportunity to automate specific processes and to check data regarding its completeness and correctness. For this, it is necessary to map the relevant business logic in the corresponding Smart Contracts. Within the framework of the research project SiLKe a Smart Contracts library will therefore be defined and evaluated. Another important point is the management of roles and rights. It has to be clearly defined which member of the network is allowed to write and read transactions. It must be taken into account that even with absolute transparency within the entire supply chain, no business secrets must be derivable from that. This has to be already considered during the development of a Blockchain solution for food supply chains. In this case, sensitive data of companies must be protected. The big challenge is to find a practicable solution for ensuring a safe, unchangeable and transparent food supply chain while guaranteeing a high level of safety of personal and sensitive company data. This is also an important part of the current development in the SiLKe project

and will continue to be one of the key issues in the future when industry standards need to be implemented into a Blockchain solution.

References

1. European Comission: Fipronil in eggs. Factsheet. http://publications.jrc.ec.europa.eu/repository/bitstream/JRC110632/jrc110632_final.pdf
2. Hellner, C.: Verkeimt, verkauft, versagt, https://www.zeit.de/wissen/2019-11/rueckrufe-lebensmittel-wurst-milch-verbraucherschutz-qualitaet
3. Camarinha-Matos, L.M., Afsarmanesh, H.: Collaborative Networks in Industry and Services: Research scope and challenges, pp. 33–42. IFAC Proceedings Volumes 40, Nantes (2007)
4. Frentrup, M., Theuvsen, L.: Transparency in Supply Chains: Is Trust a Limiting Factor? In: European Association of Agricultural Economists (ed.) 99th EAAE Seminar 'Trust and Risk in Business Networks, pp. 64–74. EAAE (2006)
5. Abeyratne, S.A., Monfared, R.P.: Blockchain ready Manufacturing Supply Chain using Distributed Ledger. International Journal of Research in Engineering and Technology 5, 1–10 (2016)
6. Camarinha-Matos, L.M. (ed.): Adaptation and value creating collaborative networks. Proceedings. Springer, [Berlin, Heidelberg] (2011)
7. G. Schuh, R. Anderl, R. Dumitrescu, A. Krüger, M. ten Hompel: Industrie 4.0 Maturity Index. Managing the Digital Transformation of Companies. Update 2020 (2020)
8. Betti, F., Bezamat, F., Fendri, M., Fernandez, B., Küpper, D., Okur, A.: Share to Gain: Unlocking Data Value in Manufacturing (2020)
9. Herweijer, C., Waghray, D., Warren, S.: Building Block(chain)s for a Better Planet (2018)
10. Janssen, C., Kim, S., Klaeser, S., Lee, C., Migliori, D., O'Brien, D., Simske, S., Traub, K., Troeger, R., Waldorf, E.: GS1 Global Traceability Standard. GS1's framework for the design of interoperable traceability systems for supply chains (2017)
11. Füßler, A., Siruet, R.: Konzeptionelle Übertragung bestehender Traceability-Prozesse auf Distributed-Ledger-basierte Anwendungsumgebungen. Entscheidungshilfe für die Umsetzung im Forschungsprojekt SiLKe (2020)
12. Kennedy, A., Troeger, R., Morgan, G., Traub, K., Allgaier, P., Arguin, P.: EPCIS and CBV Implementation Guideline. Using EPCIS and CBV standards to gain visibility of business processes (2017)
13. Dabydeen, A., Laur, R.: Product Recall in Multiple Recall Jurisdictions Implementation Guideline (2012)
14. Kennedy, A., Troeger, R., Morgan, G., Traub, K., Allgaier, P., Arguin, P., Biggs-Gregory, K.: EPC Information Services (EPCIS) Standard (2016)