NutriSafe

Securing of Food Production and Logistics with Distributed Ledger Technology

der Bundeswehr Universität München

Giesecke+Devrient

BOKU

DIEBOLD NIXDORF

TARIS

NutriSafe Toolkit

– DLT Design Principles –

Design of Blockchain-based Information Systems

Design Principles from the NutriSafe Project

Tim Hoiß – Thomas Furtner – Andreas Hermann – Manfred Hofmeier – Yvonne Kummer – Klaus-Dieter Rest – Florian Stocker – Patrick Hirsch – Sascha Oberhellmann – Dennis Lamken – Ulrike Lechner

In:
Trevor Clohessy, Eamon Walsh, Horst Treiblmaier, Theo Stratopoulos (2020): "Blockchain beyond the Horizon". Workshop at the European Conference on Information Systems (ECIS 2020).

Virtual presentation available at
https://www.youtube.com/watch?v=t5UHnlzrn0M

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

Bundesministerium Landwirtschaft, Regionen und Tourismus

SIFO.de

KIRAS Sicherheitsforschung

FFG Forschung wirkt.

This document is part of the **NutriSafe Toolkit**:

nutrisafe.de/toolkit

In a cooperation between Germany and Austria, universities, companies and public authorities are conducting research to make food production and food logistics more resilient by using Distributed Ledger Technology.

On the Austrian side, the project is funded by the Federal Ministry for Agriculture, Regions and Tourism (BMLRT) within the security research funding programme KIRAS. On the German side, the project is funded by the Federal Ministry of Education and Research (BMBF) within the programme Research for Civil Security.

nutrisafe.de | nutrisafe.at

Design of Blockchain-based Information Systems – Design Principles from the NutriSafe Project

Tim Hoiß[1], Thomas Furtner[2], Andreas Hermann[1], Manfred Hofmeier[1], Yvonne Kummer[3], Klaus-Dieter Rest[3], Florian Stocker[1], Patrick Hirsch[3], Sascha Oberhellmann[4], Dennis Lamken[5], Ulrike Lechner[1]

[1]Universität der Bundeswehr München
[2]Giesecke+Devrient Mobile Security GmbH
[3]Universität für Bodenkultur Wien
[4]Diebold Nixdorf Systems GmbH
[5]OTARIS Interactive Services GmbH

This Article was part of the workshop “Blockchain beyond the Horizon” at the ECIS 2020.

Citation:

Tim Hoiß et al (2020): Design of Blockchain-based Information Systems – Design Principles from the NutriSafe Project. In: Trevor Clohessy, Eamon Walsh, Horst Treiblmaier, Theo Stratopoulos (2020): "Blockchain beyond the Horizon". Workshop at the European Conference on Information Systems (ECIS 2020). Available at: https://nutrisafe.de/toolkit.

Design of Blockchain-based Information Systems – Design Principles from the NutriSafe Project

Tim Hoiß, Thomas Furtner, Andreas Hermann, Manfred Hofmeier, Yvonne Kummer, Klaus-Dieter Rest, Florian Stocker, Patrick Hirsch, Sascha Oberhellmann, Dennis Lamken, Ulrike Lechner,
Universität der Bundeswehr München, Giesecke+Devrient Mobile Security GmbH,
Universität für Bodenkultur Wien, Diebold Nixdorf Systems GmbH, OTARIS Interactive Services GmbH

Abstract: *The design of an interorganizational information system based on a distributed ledger infrastructure to share information along a supply chain is the challenge of the project NutriSafe. NutriSafe builds on a blockchain to increase the resilience in food production and food logistics. This workshop contribution presents the design principles that guide the NutriSafe design science approach. We hope for feedback on our approach and would like to share experiences on how to conceptualize, design and implement Blockchain-based information systems.*

The NutriSafe Research Interest

The NutriSafe project (https://nutrisafe.de) explores blockchain technology as the technical infrastructure to increase the resilience of supply chains. The research interest is to design Distributed Ledger Technologies (DLT) for supply chains, design governance structures, innovative business processes and methods and techniques to analyze the level of IT-security and resilience of a supply chain. Part of the NutriSafe project is the design of Business Model Innovations for, e.g. various service providers in data analysis.

The approach of NutriSafe is guided by the Design Science paradigm. Design is done in three iterations and the design is guided by three scenarios of food supply chains. Consulting these scenarios, we identify four use cases that are supported by the blockchain as technical infrastructure: (1) urban consumers that demand information about not only nutrition value but also transparency over the whole supply chain, (2) a crisis situation as, e.g., a cyberattack to the infrastructure, and (3) recalls and traceability of food products, and (4) a major crisis in which public authorities need to step in.

The NutriSafe Design Principles for blockchain based business information systems

After roughly one year of the project, we have designed parts of the technology and collected our experiences in form of design principles. An initial set of design principles has been developed by the NutriSafe team and the consortium has been asked for revision and validation.

Design Principle	Explanation
(Technology Stack) A blockchain-based infrastructure is a sophisticated technology. It takes more effort than expected to design and implement a blockchain.	This is more an observation than a design principle. The technology stack of Distributed Ledger Technologies (as, e.g., Hyperledger) is quite complicated when one designs and implements information systems that are based on a blockchain backbone. At the same time, examples and documentation are not readily available for all blockchain technologies and all design issues.
Blockchain Design	
(Blockchain Growth) Think of how to handle growth of the network	Designing blockchains (especially private blockchains) one should consider how to manage maintenance, performance and onboarding of participants when growing.
(Transparency vs. Confidentiality) The DLT design needs to resolve the conflict between transparency and confidentiality for the application domain. Moreover, blockchain design needs to reconsider transparency and confidentiality to obtain the maximum advantage from DLT.	The conventional blockchain is - at least in theory - fully transparent, located at a set of nodes, and stored for eternity. In our scenario and use cases, we learned about concerns of actors: competitors or malicious actors may use open information in the blockchain to either blackmail an organization or obtain strategic information about competitors´ supply chain. There are concepts and technologies as, e.g., channels, private data collections, access control lists, idemix (features in Hyperledger Fabric), for fine grained confidentiality in the blockchain. Rethinking confidentiality and transparency is necessary for innovation of blockchain-based business models and maximizing benefits from DLTs for ecosystems.
(**This is a blockchain - not a database! This is a blockchain - not an ERP System!**) Keep the data and transactions minimal.	A general blockchain stores all the transactions until every part of the blockchain stops its service. Furthermore, in the case of smart contracts or chaincode, the software is executed at least on a set of nodes in public chains, sometimes even on every node. Only store the needed data on the blockchain, try to run reports or analyses outside the blockchain by only using the data. Always keep in mind the blockchain is no database and no ERP-system.
(Onchain vs. Offchain) Consider whether all data is stored inside the blockchain or are data parts stored outside the chain.	When designing a blockchain one must decide which data needs to be stored and handled on the blockchain and which data can be or needs to be handled offchain (e.g. to provide high levels of confidentiality or to limit the amount of data).
(Interfaces and integration) Blockchain-based information systems need interfaces and integration with other information systems.	Look at the ecosystem of existing information systems in the domain and provide interfaces for them. In the NutriSafe case, a lot of SMEs handle data in procurement and fulfillment in the traditional way: On paper or in Excel. To be compatible, a blockchain-based information system for SMEs needs an Excel interface. Interfaces should be standardized to enable integration of systems using different technologies.
(Ease of use) Clients have to be easy to be used.	This is easy, as this is the job of a client designer (not a DLT designer). DLT design (IT and smart contracts) will remain complicated. But this is not visible outside to end users (e.g. farmers in the NutriSafe case), who will just use the client.

(Network vs. Chaincode vs. Client). A DLT consists of 3 different parts, which requires different experts and knowledge	DLT design requires 3 different skill sets (network, chaincode, client). Setting up the network has to be done by IT trained staff (no need to know about the business logic of the chaincode). The chaincode has to be developed according a lengthy investigation into what data has to be where under which circumstances. Chaincode developers always have to be accompanied by testers to ensure integrity of code. And the client SW as the frontend to the user requires specific knowledge regarding usability.
(**A DLT design needs to take security into account).** A permissioned blockchain is not secure-by-design.	A permissionless DLT has several measures build in to ensure security, as the central point (administrator) taking care about security is missing. A permissioned DLT (Hyperledger Fabric) has just some of those built-in security measures and therefore is more sensitive against regular IT hacks. A Permissioned DLT is as (un)secure as your IT system is. This can be overcome by using conventional IT security as you would use for your data base system to close the gaps.
Governance	
(Design Governance) Find a suitable governance model for the blockchain.	The decision about policies and consensus needs to be done in the beginning since changing them could be a significant task. Democratic processes fit into the blockchain paradigm but would also enable consensus attacks (cf. BSI Blockchain Report). For a particular use case such as the NutriSafe Blockchain, a purely democratic model is not an option, as a small blockchain can be taken over too easy and since the interest and stakes in participation vary between smaller and more active actors. In permissioned blockchains some instance(s) need(s) to handle the rights to participate. It is needed to maintain participation rights and even to be able to revoke rights.
(Accountability) Putting data in the blockchain does not release from responsibility.	GDPR demands accountability for information, and this includes information stored in a blockchain. GDPR also requires personal information to be deleted upon request - and the typical blockchain design does not allow information to be deleted. Thus, think about the data to be shared, accountability for this data, and whether it is necessary to store and share personal data in the blockchain and how to delete personal information upon request. In the NutriSafe case, supply chains are transnational: within the EU GDPR and other regulations are quite uniform, it becomes really challenging in international settings.
Ecosystem	
(Specific vs. Global) Both small, use-case specific, and global blockchains are useful in practice.	At the beginning of our research, there has been the idea of a single big, global blockchain for food production and logistics. Nevertheless, in some use cases, it makes sense to design and develop small-scale, specific blockchains for disjunct use cases. Also concepts of, e.g. channels and ordering services (in Hyperledger) allow for a separation of concerns within a blockchain. In the NutriSafe project, in case of food safety use cases, small blockchains make sense, e.g. that farmers indicate their quality levels. In case of food security, larger blockchain consortia are needed, e.g. to find alternatives for suppliers in food shortages or to manage food distribution in case of shortages.
(**Participation**) Include also actors from the wider ecosystem, as e.g. public authorities, laboratories, veterinarians.	Actors who participate in the physical production and -logistics supply chain might participate in a blockchain-based ecosystem. Think about veterinaries, certification authorities or labs that provide data. In these cases, data ownership needs to be taken into account. For integration purposes, think about IT-service providers, the study "NutriSafe Monitor - Resilienz und Blockchain Technologie in Lebensmittelproduktion und -logistik" found that more than 66 % of SMEs do not host their IT themselves. Therefore, any blockchain ecosystem needs to take also the IT service providers on board.
(Incentives) Make sure there is an incentive for participation in a blockchain ecosystem.	There are many reasons why actors participate in blockchains: legal reasons, process improvements or business models - beyond mere transparency. In NutriSafe, we address information sharing along the supply chain: producers may inform their customers, customers may request information about all steps in the supply chain. NutriSafe provides functionality for traceability and recalls and allows public authorities to obtain information and act upon in cases of major crisis events. We anticipate that the blockchain infrastructure provides incentives for all eco-system participants in all events and that it does not make sense to have a blockchain-backbone only for crisis events.
(Competences) Do not expect that everyone is capable of maintaining blockchain nodes.	To maintain blockchain nodes, it requires knowledge about the blockchain, e. g. to operate or configure it as well as resources. Not every organization (especially SMEs) has the capabilities to run a node - they may "only" access blockchain as a service, provide data or get information from the blockchain. In the design of the blockchain-based infrastructure, an easy to use solution is necessary - an interface that facilitates the use of the blockchain without any user interaction for entering data in the blockchain and with standard interfaces, e.g., Excel spreadsheets. For querying, develop an easy to use solution, e.g., with pre-generated report templates.
(Standardization) Blockchain-based information systems need standards.	Standards for data models and processes facilitate inter-organizational information sharing in a blockchain. This is an important aspect. When setting up a DLT as a backbone to various business information systems, the IT implementation is only one aspect. The business logic you want to run on DLT incl. their interfaces, data formats, rules,… is the big work and needs standardization.

Acknowledgements: We thank the German Federal Ministry of Education and Research (BMBF) for the funding of NutriSafe (FKZ: 13N15070) as well as the safety research funding program KIRAS, financed by the Austrian Federal Ministry of Agriculture, Regions and Tourism (project number: 867015). In addition, we thank the interview partners who guided the development of the NutriSafe design principles.