HOCHSCHULE MITTWEIDA
University of Applied Sciences

Wissenschaftliche Berichte | Scientific reports

Konferenzband zum Scientific Track der Blockchain Autumn School 2022

Nr. 2, 2022

Konferenzband zum Scientific Track der Blockchain Autumn School 2022
Impressum

Herausgeber:
Hochschule Mittweida
University of Applied Sciences
Der Rektor
Prof. Dr. phil. Ludwig Hilmer
Der Prorektor Forschung
Prof. Dr.-Ing. Uwe Mahn

Redaktion dieser Ausgabe:
Hochschule Mittweida |Referat Forschung
University of Applied Sciences

Leitung:
Prof. Dr.-Ing. Andreas Ittner
Dr. Dipl.-[Wi.] Ing. Volker Wannack

Kontakt:
Hochschule Mittweida
University of Applied Sciences
Referat Forschung
Postfach 1457
D-09644 Mittweida

Tel.: +49 (0) 3727 / 58-1264
Fax: +49 (0) 3727 / 58-21264
forschung@hs-mittweida.de
www.forschung.hs-mittweida.de

ISSN 1437-7624

Erscheinungsweise:
Unregelmäßig

Auflage:
Belegexemplare sowie bestellte Druckexemplare

Druck:
Hochschuldruckerei Hochschule Mittweida

Förderung:
Die Hochschule wird mitfinanziert durch Steuermittel auf der Grundlage des vom Sächsischen Landtag beschlossenen Haushaltes.

Bundesministerium für Bildung und Forschung

Projektträger Jülich
Forschungszentrum Jülich

Foto Titelseite: Hochschule Mittweida

Bildnachweise werden direkt am Foto bzw. im jeweiligen Artikel aufgeführt.
Im Scientific Report gelten grammatikalisch maskuline Personenbezeichnungen gleichermaßen für Personen jeglichen Geschlechts.

Die Scientific Reports/Wissenschaftliche Berichte als Wissenschaftliche Zeitschrift der Hochschule Mittweida - University of Applied Sciences lösen die bisherigen Scientific Reports mit allen Volume I-III ab und erscheinen mit Nr.1, 1998 ab November 1998 in neuem Layout und in neuer Zählung.

Für den Inhalt der Beiträge sind die Autoren verantwortlich.

Im laufenden Kalenderjahr sind bereits erschienen:
Nr. 1, 2022
Messtechnische Überwachung von Stauanlagen
XII. Mittweidaer Talsperrentag

SCIENTIFIC REPORTS | WISSENSCHAFTLICHE BERICHTE
The main aspect of the Scientific Reports is to promote the discussion of modern developments in research and production and to stimulate the interdisciplinary cooperation by information about conferences, workshops, promotion of partnerships and statistical information on annual work of the Hochschule Mittweida (FH) University of Applied Sciences. This issue will be published sporadically. Contributors are requested to present results of current research, transfer activities in the field of technology and applied modern techniques to support the discussion among engineers, mathematicians, experts in material science and technology, business and economy and social work.

Die Scientific Reports der Hochschule Mittweida sind online verfügbar unter:
www.forschung.hs-mittweida.de/veroeffentlichungen/scientific-reports

Eine Veröffentlichung einzelner Beiträge erfolgt entsprechend der Open Access Strategie der Hochschule Mittweida auf dem Hochschulschriftenserver: https://monami.hs-mittweida.de

INHALTSVERZEICHNIS

Strategic realignment of medium-sized companies due to distributed ledger technologies in supply chain management

Roman Stammes, Eugen Burov, Thomas Ludwig, Tan Gürpinar
Technische Universität Dortmund, August-Schmidt-Straße 1, 44227 Dortmund
Universität Siegen, Adolf-Reichwein-Straße 2, 57076 Siegen

More than 10 years after the invention of Bitcoin, the underlying blockchain technology is having an increasing effect on today's society. Although one of the most popular application areas of blockchain is still the field of cryptocurrencies, the technological concepts are crossing into further application domains such as international supply chains. Fast-changing markets, high costs of time and risk management as well as biased relationships between the actors pose big challenges to an appropriate supply chain management. Based on a case study about sensor tracking, this paper explores the potential impact of blockchain on small and medium enterprises within an international supply chain. We will show that blockchain technologies offers a high potential to reduce inequalities of power relations between involved actors within supply chains. To achieve this, the requirements for the use of blockchain in supply chain management will be analyzed by means of a conducted case study and an expert survey of the companies concerned.

1. Introduction

Nowadays, global competition, cheap production resources and the rapid availability of materials and products place high demands on an appropriate supply chain management (SCM) within companies. Within such a supply chain, a large number of different actors play a crucial role. Suppliers, manufacturers, customers and service providers all aim to improve its efficiency [1], usually resulting in a low manual effort, i.e., a process chain that is automated as much as possible [2]. To address the challenges of a low manual effort within the supply chain, there are plenty of different SCM systems and technical networks aimed at supporting (semi-)automated internal, but also external cross-company processes [3]. With the advent of inexpensive sensors and devices as well as new possibilities for data exchange, the Internet of Things (IoT) became an effective way to track and authenticate products and shipments using several kinds of data sensors such as GPS or RFID [4]. The IoT devices are further meant to measure environmental aspects and therefore to monitor conditions of products and their quality throughout the entire supply chain.

However, when focusing on small and medium enterprises (SMEs) within supply chains, they usually have large financial constraints, wherefore their high priority is more often placed on inventory management and control [5], instead of an effective SCM. Therefore, the data on the supply chain (including sensor values, environmental parameters, etc.) is held and maintained by the large companies. For this reason, SMEs are forced to trust the data of the large dominant companies within the supply chain, which lead to major differences in power relations and tensions.

Distributed ledger technologies (DLT), such as blockchain, promise a "trustless" transaction system including an unchangeable storage and transparent traceability of data [6]. The multitude of different actors within supply chain networks resulted in first use cases for the application of DLT within the SCM [7]. Distributed ledger technologies store the data transparently for all parties involved and thus create a basis of trust. These technologies thus enable process efficiencies and a uniform information basis to be created.

Such use cases usually consider new forms of sensor-supported hardware which automatically gathers data within the supply chain and stores it in a traceable manner within the distributed ledger. The DLT-based business relationships within the supply chain and the transparent traceability of sensor data are predestined to especially support SMEs to operate in collaborative value networks with shared power relations and grounded negotiations and to enhance the chances for a possible transformation from market imbalance to a rather transparent and fair business. Small and medium enterprises can develop competitive advantage through new implementation strategies [8]. However, in exactly which way SMEs are able to transform or strategically realign their traditional business with regard to their role in a supply chain and thus shifting into DLT-based supply chain management is not obvious. Within this paper, we therefore address the research question which requirements for the use of DLT technologies in SCM must be fulfilled and what are the impacts on power relations between their business partner?

The paper is structured as follows: within related work (section 2), we introduce into the fields of supply chain management and blockchain technologies and present current approaches that focus on applying blockchain technologies within SCM. We will then report on the findings of a product development about tracking IoT data within supply chains and its deployment within an actual

business case (section 3). Based on this product deployment meant as technology probe we were able to discuss with the involved actors blockchain technologies within SCM. Based on the following interview study with the involved actors (section 4), we present the findings about blockchain technologies in supply chain management from the SMEs perspective and its impact on power relations (section 5).

2. Background and state of the art

The research combines two areas of research. The first focuses on IoT-driven supply chain management, the second on blockchain and distributed ledger technologies.

2.1. Supply Chain Management and IoT

A supply chain is a network of companies to supply, produce and distribute a specific product to a final buyer. Nowadays, a supply chain consists of several actors that including legally separated organizations for producing parts or components, providing logistic services and even the customer himself bound by material, information and financial flow [9]. Supply chain management (SCM) encompasses the integration of all core business processes within a supply chain which lead to an increase in value for consumers or actors across organizational boundaries through production data, services or information [10]. Advancing information and communication technologies (ICT) made it possible to process information at different locations within the supply chain, thus enabling advanced planning [9].

As supply chains become increasingly global and complex, companies try to outsource several supply chains services to specialized third-party logistic companies. Although on the one hand a multitude of tasks can be outsourced to specialized companies, on the other hand there are increased requirements for a comprehensive information management and mechanisms to share information within the supply chain. Borade and Bansod (2007) expect that in future all organizations need to adopt partnership information sharing initiatives with suppliers, which requires the establishment of mutual trust within the supply chain to share the vital information [11].

The concept of the Internet of Things (IoT) can be described as a network consisting of numerous “smart” objects, which form an overarching information network to exchange information between interconnected physical objects. The Internet of Things appeared for the first time within the supply chain area in 1990 [12]. Here, the devices are usually equipped with electronic sensors such as RFID making them uniquely addressable [13]. Applying IoT within the supply chain mainly contributes to an improved quality of information and new ways of enabling interactions between goods and machines, but also between humans and machines [14].

The basis for the advantages of applying IoT within the supply chain [15] lies primarily in electronic product coding technology coupled with internet technology [16]. Nowadays, RFID is especially widely used in SCM for efficient data acquisition. RFID tags contain information such as the volume of goods, weight, production date, batch numbers and much more. This technology is often the determining identification for the link from manufacturers, transportation, warehousing, distribution, to the assembler [17]. However, RFID typically requires a reader to query the data at certain stations in the supply chain, which means that there is no continuous tracking, for example on the high seas. To tackle this problem, first developments for tracking devices try to independently send data to relevant actors in the supply chain to get live status of goods and their conditions [18].

Some big ICT companies such as the Telekom AG are currently developing new solutions for IoT which will primarily benefit the manufacturing and logistics industries. The focus is usually on applications that cover the machine and sensor network Narrow-Band IoT (NB IoT). These novel technologies are characterized by the comparatively low costs and lower energy consumption. Using this technology, companies are able to integrate millions of objects and processes inexpensive, fast and integrate securely. Compared to the conventional technologies based on GPS the Low-Cost Tracker has the advantages of lower costs, worldwide 3GPP standard and longer battery life. In addition, these novel trackers also record – besides movement data – additional parameters like vibrations or temperatures. The built-in sensors record and transmit data about harsh environmental conditions or improper handling of the goods through the entire supply chain [19].

Such approaches foster transparency among the involved actors and may affect negotiating power. Transports can be continuing monitored, and due to the integrated movement alarm, theft prevention can be carried out successfully. The sum of these functionalities should pave the way for a large-scale cross-sector use. The Telekom AG reports that due to missing information 30 percent of all deliveries worldwide do not reach their destination in time, and freight theft costs companies billions. Intelligently networked load carriers bring more transparency into the supply chain and the transportation of goods by water, rail and road can be controlled more precisely.

2.2. Blockchain and Supply Chain Management

More than 10 years after the invention of Bitcoin in response to the 2008 global financial crisis [20], the underlying blockchain technology is having an increasing effect on today’s society. A blockchain consists of chronological blocks which represent digital information stored with time stamps in a public database. The individual blocks contain a hash value of the previous block so that verifiability is guaranteed and through referencing the previous block a chain of blocks (blockchain) is created

[21] Usually, the information sent and who sent it is encrypted and only visible to the sender. Each transaction made can be transparently viewed on the blockchain, where the users are usually represented by pseudonyms.

Consensus algorithms are used to achieve agreement between distributed processes and systems within the peer-to-peer network. This peer-to-peer network is designed to achieve reliability in a network with unreliable nodes. Several different consensus mechanisms have already been established in the blockchain area. The most used are the proof-of-work (mining), proof-of-stake or byzantine fault tolerance algorithm [22]. Beside the field of cryptocurrencies, technologies such as Ethereum [23] or Hyperledger [24] allow the creation, administration, and execution of decentralized programs. These decentralized programs (called smart contracts) paved the way for the development of decentralized applications (dApps) that allow the distributed execution of an application within the peer-to-peer networks.

Decentralized applications offer great potentials in the area of trade finance, where a bank processes financing for goods traffic between exporter and importer. The involved actors often do not know each other or simply do not trust each other enough for paying in advance. The exporter wants to receive the payment for the goods before forwarding them to the importer. The importer on the other hand wants to receive the goods before paying the exporter. If blockchain technologies are used, it is possible that the manufacturer can be paid instantly [25].

Letters of credit are a conditional promise of payment by the credit institution, which notifies payment to the payee upon presentation of previously defined documents. The requested documents can be transport documents, such as bills of lading, waybills, unloading confirmations or take-over confirmations, certificates of origin, certificates of quality or insurance certificates. Within the supply chain, parties involved create the documents and pass them on to the other parties involved. Traditionally, most documents are still created and exchanged physically.

Blockchain technology aims to ease these process steps by storing data of IoT sensors transparently within a blockchain and linking those directly to the trade documents. This blockchain-based sensor data serves as evidence for later negotiation. A container, for example, can automatically link temperature and GPS data to the blockchain. Information is picked up by the sensors and saved in the blockchain. After receiving the data, the commands are interpreted, and the system can be executed automatically via the smart contract [25].

There are already several approaches that apply blockchain technologies to SCM. When focusing on rather technical studies, different blockchain frameworks get covered by Samaniego et al. [26] who elaborate on IoT devices which are being used within blockchains to manage device configuration, store sensor data or enable micro-payments. Augusto et al. [27] analyze smart contracts, that are used in the IoT environment of logistics where they highlight the benefits of applying blockchain technologies. However, these approaches mainly focus on rather technical evaluations and lack practical validation.

There is further work focusing on the impact of using blockchain technology in several branches and industries. Casino et al. [28] gives an overview with a systematic literature review about the current status of blockchain applications. Nagamalai et al. [29] deal with the perspective of smart contracts applied for security, privacy and performance issues. Saberi et al. [30] deal with blockchain applications in supply chain risk management, and Korpela et al. [31] perform research on strategic and operational information exchange within a supply chain network via blockchain. All these studies focus on large companies and do not take into account the specifics of SMEs and how blockchain technologies might impact the relationships with other actors within the supply chain.

Wong et al. [32] turned to SMEs and examined the adoption of blockchain in operations and supply chain management among Malaysian SMEs. They revealed the importance and potential of networked ledgers which share real time data to everyone who participate in the network. Within our study, we will extend these perspectives by examining German SMEs and providing substantiate views with an actual use case instead of merely remaining on a rather theoretical level about potential effects.

The literature study shows first investigation of blockchain technologies within supply chain management. However, current approaches focus either mainly on technical investigations or on large companies. Our paper therefore shows the explicitly turn to the role of SMEs and impacts of applying blockchain technologies on the current unequal power relations within supply chains as well as describing the necessary requirements for the implementation of the technology.

3. Case study on managing sensor data in supply chain management

As the literature review revealed, tracking the goods within a supply chain is a major concern for companies. Several problems can arise such as fraud, changes over illegal routes, stealing as well as wrong or unsafe storage under incorrect conditions. As soon as goods are on the way to their destination port, they can no longer be tracked and even if a data platform is used, the company must trust the data points and depends on the data of the shipping a company. This hampers a complete validity and there is no guarantee for the involved companies. Supply chain management is still mainly based on

physical paperwork such as the bill of landing, which secures the right to the goods. Tackling these challenges of modern SCM, the companies involved try to make use of modern ICT to digitalize the paperwork, foster automation, and track the supply chain with different kinds of parameters.

To get insights into which requirements are necessary for the use of blockchain in SCM, we conducted a particular case study together with the companies described below. The aim was to examine the decisive parameters for the implementation of a blockchain solution based on an actual working product instead of rather a theoretical basis. Within the case study, we will report on the findings of an IT project together with a big bank (BANK), an Association for Technical Inspection (TÜV), a logistic enterprise (LOG) as well as a small, but global trading company (TRADE). Thus, beyond a pure literature review or test in a laboratory environment, a live test on the requirements for the use of blockchain in supply chain management was carried out. All names of the companies are anonymized for the review.

The small trading company has its headquarters in Germany and employs three managers, one of whom was responsible for working on the IT project. TRADE procure and sell non-food goods for customer needs, such as small electrical appliances, tools, gifts and decorative items. Their customers are well-known supply chains in Germany and Europe. TRADE offers an own logistics service for GPS data tracking of goods consignments.

The project was carried out by sending a tracker from LOG to the TÜV office in China. The TÜV inspector in turn attached the tracker to the goods and the container was sealed after the goods were loaded. This ensured that nothing could affect the tracker. The imported goods were able to be tracked and traced the entire distance through the tracker. The transport was followed from the production factory in China to the customer in Germany with geofencing. In the IoT tracking project the combination of an API interface with the geofencing contained all the relevant data, such as the time. In particular, at which time the goods arrived at a port on the route.

The implemented “Smart Visibility” service from LOG (Figure 1) made it possible to ensure real-time tracking along the process chain and as it was able to transmit the following environmental data: temperature, air pressure, humidity, vibration and door closing and opening. The IoT-based traceability system enables the company to monitor the quality from production process to delivery to the end customer. Moreover, trust in a cross-sectoral collaboration is enabled, as the data platform and the IoT-tracker share the correct information. This is however problematic, as the owner of the platform has all the power and data available.

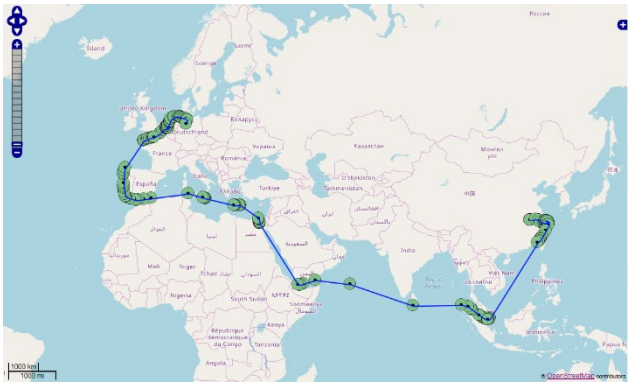

Figure 1 “Smart Visibility" service from LOG Platform

Through the development of procurement and sales activities, the SME wants to establish communication networks with partnership, equality and trust. Due to the pressure of small margins and innovations in SCM, new processes play an increasing role for the involved companies. For this reason, the goal is to process and digitalize the entire value chain so that competitiveness can be maintained.

Furthermore, if a product has left production, no specific information is available. The import companies like TRADE just get a status information, but has no chance of tracking their ordered goods through a reliable platform. To solve the problem, a distributed ledger technology like a blockchain was discussed to strengthen the partnership through trust in an unchangeable system.

In the corporate environment, primarily a consortium technology solution is going to be used to strengthen the negotiation power and equality between the partners. So, TRADE can have a more important role in the supply chain and have more security through the trustworthy data received. Moreover, the complete and reliable traceability in supply chain management can make it reliable and trustworthy, which enables process efficiencies and cost reductions for TRADE.

This project was a first step in using an IoT data tracking platform as a technology probe for discussing SCM platforms using blockchain. To be able to make demands on a functioning blockchain system it is necessary to conduct a live use case and to share these experiences with the participating companies. The case study evaluated to what extent and with which conditions a blockchain-based solution can be used. Furthermore, the imported goods were real goods, where a mistake would be costly and therefore a comparison was made from the results, which requirements had to be fulfilled step by step, so that the blockchain could be connected. Therefore, a classical data platform was taken from the provider LOG and the collected data was evaluated afterwards.

The result of the project was that the different parameters, such as the fact that the IoT tracker does not have access to the network on the world's oceans and cannot retransmit the data packets. It was also revealed that these data that had not been transmitted could be for-

warded afterwards. This is important to adapt the automatic pre-defined contracts to this special feature. Such requirements must be considered, as well as the fact that the sending of the data packets for the different contractual partners may arrive with delays and that there must therefore be no breaches of contract or penalties. The letters of credits to be redefined must also be adapted as well as that the decisions are no longer based on pure trust in the contractual partners rather than the new implemented system.

During the case study and the actual live tracking of the product, a trade finance blockchain solution was announced by the companies as an alternative product to the existing solution. The IoT tracking project therefore served as a helpful component for further development for new solutions in SCM. In addition, BANK has entered a cooperation with 12 other enterprise partners to develop the supply chains of the future. Exactly this endeavor can now be developed with the data collected from the TRADE project.

During the study, the involved actors discussed that the information obtained, such as a trusting structure across the entire delivery network, as well as the transparency and real-time of the delivery information is of crucial importance. Based on the measurement data collected, smart contracts can be attached to a blockchain solution, which can automatically make a payment for predefined events. The manual and paper-based checks of the documents can thus be omitted. However, a transition from the current IT infrastructure to a company-owned blockchain database would require a substantial shift. Indeed, the shift to a blockchain based technology with an IoT traceability system could, through the data immutability, prevent fraud, reduce costs, gain trust and leads to more negotiation power between the participants.

Blockchain technology now enables all banks to store the information on a node and make it accessible to everyone involved. The confirmations are validated by the contractual partners and posted synchronously. Since all data is stored on the permissioned blockchain and cannot be changed, protection against forgery is guaranteed. Interest and principal payments can still be automated via smart contracts. The bank that provides the platform can charge everyone an extra fee, but the platform can make it more transparent, faster and cheaper for everyone. Smart contracts offer the opportunity to agree contracts between business partners without programming via a central office. Breach of contract or legal disputes are thus imposed [33].

In addition to trade finance, the decentralization of the standard credit business also causes many distortions on the financial markets. Through peer-to-peer transactions, the intermediary is no longer involved in the customer's value chain. Blockchain could become a valuable tool for negotiation power, in which SMEs join through a consortium and receive the chance to develop the supply chain process. These processes are usually complex and need a lot of manual execution. The exchange between the enterprises is time-consuming and expensive due to the different IT structure and the exchange of paperwork.

4. Evaluation of the applicability of blockchain-based SCM

To further evaluate the case study findings and first ideas, this section introduces an interview study. The interviews were conducted after the actual product deployment to obtain practical information from the participating companies. Based on the analysis of the companies' feedback, we derive requirements for the use of blockchain in supply chain management.

4.1. Methodology

The interview study was meant to validate, prioritize and enrich the prior case study outcomes with further practice-oriented experiences. We chose semi-structure interviews with multiple experts involved in the same case. We selected five participants according to their position and project involvement within the different companies BANK, TRADE, and LOG [34]. The employees of the companies were also involved in the use case, so that a subsequent evaluation of the results could be carried out. All participants are employed in the trade finance area and would like to see changes in the process in the future In this paper, the importance of having experts give insights into their personal view of the analyzed problem was also considered [20].

The actors were asked about the company's status quo in dealing with supply chain management, assessments of the requirements for blockchain technology and the influence of blockchain technology on SCM in their respective companies Hence, a standardized way to approach the interviewees in three categories to ask general questions, case related questions and questions dealing with a future outlook were used. The interview outcomes then were analyzed according to Mayring's qualitative content analysis [35].

4.2. Interview Results

Our results revealed, that the participants see high potentials in blockchain technology for reducing the administration (costs) of paperwork, and replace the current silo systems by new technology possibilities: "Customers try to digitize and work with us to get off the big paperwork" (interviewee 1). However, there are some major challenges in the current supply chain process. Currently the within the entire process and the forwarder is dependent on the decisions and specifications of the other partners. For instance, the supplier is between the two big power relations of the producer and the retailer. On the one hand, the producer has all the power if the producer has not started the production or acquired the material at his own expense. On the other hand, the retailer can reject the goods as any time: The

retailer can also look at the goods so closely at any time and reject them for no reason (interviewee 2). There is no objective process, if there are contractual defects concerning the goods. Also, the retailer acts as a translator and as a kind of insurance agent between the two parties and becomes the risk taker in the procedure.

Due to the above-mentioned aspects, it is especially interesting for the surveyed companies to test out new technology-based use cases. Basically, there are a handful of companies with which we can work in partnership and further develop projects (interviewee 3). The area of blockchain could be one of the most promising. However, there is just curiosity in blockchain, a real adoption and implementation shall not affect the current supply chain process until advantages are visible. The implemented use case of IoT data tracking was also valuable for the development of the blockchain-based supply chains, because problems arose which could not have been thought of before. The IoT device transmits via the mobile data network and if there is no access to the data network, then no information can be stored in the blockchain-based. In this specific case, the tracker in the Indian ocean was too far away from land and could not transmit the ship's position and other predefined data. In this case, such challenges must be considered for the implementation of trigger events via smart contracts. “Smart Contracts are useful in that an action can be triggered as soon as a shipment arrives in the geofence. The triggering of an automatic payment process would be sufficient, too” (interviewee 3).

According to the interviewees, the following points can be seen as advantageous for the current challenges: no down payments and automatic payments, less paperwork because of the credibility of a distributed ledger, smart contracts in specific defined trigger events, more transparency, less fraud, security data quality IT standards, networks and equality in the drafting of the contract. The challenges must be solved before the new technology revolution can be applied in practice. This also requires the creation of product solutions and easy implementation interfaces. “There is no real product available yet [...] We are not faced with the choice of using either blockchain products or classic products. At the moment it is only interesting, but not practicable. (Interviewee 2)

Finally, the respondents praised that supply chain-based technology solutions are more attractive to them: “We also have a great interest in knowing that our data is stored securely and that we do not fall into the hands of individual large companies, and therefore we would tend to use blockchain solutions” (interviewee 2). Here, the integration of different business networks can help with collaboration of different companies. “It will become decentralized and many business networks will emerge, like Marco Polo [a trade finance initiative]. Many business networks with specific degrees of decentralization will emerge and networks will be established between the entire platforms” (interviewee 1).

After analysis of the survey the decision for distributed ledger networks plays a decisive role in improving cooperation between supply chain partners. Furthermore, analysis showed that the use of objective clearly defined rules, which are observed equally by all contractual partners, leads to a fair and sustainable business relationship.

5. Discussion

The case study has shown the usability of an IoT application in SCM and what requirements or potentials lays in DLT technology, which can create an equilibrium of forces for German SMEs in supply chain management. With the collected data from the use case and the insights gained from the interviews, a blockchain based solution can be developed. By interviewing experts following the use case, the insights could be shared and analyzed to answer the research question about requirements for the use of DLT technologies in supply chain management and its impact on power relations between involved business partners.

The design of the use of such a blockchain-based platform must consider the fact that international transport routes can lead to tracker failures, as it is not always possible to establish a network on the world's oceans. Smart contracts must meet these requirements. Furthermore, the live use case showed that a platform has to meet the requirement that the objectivity of the data can be given to all participating persons at any time and that decisions are no longer based on pure trust in the contractual partners. As the empirical survey revealed, the participating companies are concerned about the data security, applicability, evaluability of the shared information. Furthermore, the evaluation of the existing frameworks should be advanced as well as standardization for rapid adaptation to the market.

Intermediary-free structures enable objective and fair corporate relationships to be established for supply chain management. The inherent transparency of blockchain also means that information is shared equally between all parties and can no longer be manipulated. Equal rights in the supply chain management also means that the SME is no longer subject to uncertainty, but rather to trust. The experts involved also agreed that a distributed database infrastructure like blockchain will come on the market anyway and that early testing has the decisive added value for future implementations. They also list some potential advantages like no down payments and automatic payments, less paperwork because of the credibility of a distributed ledger, smart contracts in specific defined trigger events, more transparency, less fraud, security data quality IT standards, networks and equality in the drafting of the contract

Furthermore, this research indicates that it is essential to conduct live use cases, as this is where the real problems and challenges can be identified. Some points cannot be considered in a theoretical considerations and

tests, such as the issue that the IoT-tracker had no connection to the country and could no longer send data live but had to retransmit it. These uncertainties could be found out with the research approach of accompanying the use case. Currently, most approaches do not focus on already existing (and well-established) ICT which is already used in SCM. This paper could thus provide decisive assistance for future studies that focus on the equality of bargaining power for SMEs in supply chain management under consideration of IoT devices based on blockchain.

6. Conclusion

Since Blockchain is increasingly crossing into various application fields, we provided not only an overview of the current literature in supply chain management with IoT and blockchain, but also a case study with an actual working product together with a German SME. Our case study was conducted to examine the potential impact of blockchain on small and medium enterprises within an international supply chain.

With the help of an empirical study, our case study was able to show that blockchain has the opportunity to reduce inequalities of power relations between the large enterprises and SMEs within supply chains. With the requirements now established for the use of blockchain in SCM a valuable input on the current state of research could be identified. The change of increasing negotiation power in supply chain management for SMEs is based on the new technology blockchain in combination with consortia with other companies. Future studies may be focused on DLT-Use-Cases using IoT-Devises to do automated payments or implementations for a transfer of risk for insurance. There is also a possibility of a more quantified perspective for the blockchain technology.

Moreover, the inherent blockchain characteristics like interoperability, transaction speed, costs, rights and remedies needed to be assessed. Blockchain or distributed ledger technologies could be one of the game changers in future supply chains. However, in order for a fundamental change, cooperation between all participants is required and problems like the limited transaction speed must be solved. Also, the frameworks need an evolution in form of satisfactory IT security, objective standards and equality in the process. The case study of the German SME was presented to uncover necessary requirements for using blockchain in SCM tracing systems as well as current open research areas. Also, the implemented IoT tracking case will be implemented in a subsequent step by the participating companies in a permissioned blockchain solution and the gained insights will be included.

However, further studies are needed to examine the impact of the use of blockchain technologies in SCM in terms of profitability particularly for SME's [36, 37, 38]. The results of this study should therefore not be considered as part of a series of examinations. Only a few studies were focused on the use of blockchain in SCM and no study on the effects of reducing inequalities within power relations has been conducted so far [32]. The small number of studies in this new specific makes it difficult to comparisons our work with other existing and actual tested technologies and use cases. Also, hardly any small and medium sized enterprises have adapted their existing business models in such a way that blockchain can be integrated into SCM [36, 39], which leaves an field of research that can be focused on in future. Following studies can therefore build on our initial work and examine the process chains in the SCM that will change significantly in the future due to distributed ledger systems [32]. Although our work only presents the first steps of applying blockchain technologies in international supply chains, we hope to inspire other designers and developers trying to engage with the issues that may arise from the intersection of SCM, IoT and blockchain.

References

[1] H. Werner, Supply Chain Management: Grundlagen, Strategien, Instrumente und Controlling. Wiesbaden: Gabler Verlag, 2000.

[2] M. Mau, Supply Chain Management: Prozessoptimierung entlang der Wertschöpfungskette: John Wiley & Sons, 2003.

[3] C. Boersch and R. Elschen, Das Summa Summarum des Management: Gabler, 2007.

[4] Fraunhofer Institute for Material Flow and Logistics, “Logistik entdecken,” no. 19, pp. 22–25, 2018.

[5] J. Meehan and L. Muir, “SCM in Merseyside SMEs: benefits and barriers,” TQM Journal, vol. 20, pp. 223–232, 2008, doi: 10.1108/17542730810867245.

[6] P. Rosenberger, Bitcoin und Blockchain: Vom Scheitern einer Ideologie und dem Erfolg einer revolutionären Technik. Berlin, Heidelberg: Springer Vieweg, 2018.

[7] Hurth M. and Knauer C. and Ruf, T., “Digitalisierung in Supply Chains,” BME-Logistikumfrage. Bundesverband Materialwirtschaft, Einkauf und Logistik e.V., 2019.

[8] K. Bär, Z. N. L. Herbert-Hansen, and W. Khalid, “Considering Industry 4.0 aspects in the supply chain for an SME,” Production Engineering, vol. 12, no. 6, pp. 747–758, 2018, doi: 10.1007/s11740-018-0851-y.

[9] H. Stadtler, Ed., Supply Chain Management and Advanced Planning: Concepts, models, software, and case studies, 5th ed. Berlin: Springer, 2015.

[10] D. Lambert, M. Cooper, and J. Pagh, “Supply Chain Management: Implementation Issues and Research Opportunities,” International Journal of Logistics Management, The, vol. 9, pp. 1–20, 1998, doi: 10.1108/09574099810805807.

[11] A. Borade and S. Bansod, ““Domain Of Supply Chain Management - A State Of Art”,” Journal of Technology Management & Innovation, vol. 2, 2007.

[12] M. Ben-Daya, E. Hassini, and Z. Bahroun, "Internet of things and supply chain management: a literature review," International Journal of Production Research, vol. 57, pp. 1–24, 2017, doi: 10.1080/00207543.2017.1402140.
[13] L. Xu, W. He, and S. Li, "Internet of Things in Industries: A Survey," IEEE Transactions on Industrial Informatics, vol. 10, pp. 2233–2243, 2014, doi: 10.1109/TII.2014.2300753.
[14] B. Weimert et al., BLOCKCHAIN AND SMART CONTRACTS - Technologies, research issues and applications, 2018.
[15] A. Dorri, S. Kanhere, R. Jurdak, and P. Gauravaram, Blockchain for IoT Security and Privacy: The Case Study of a Smart Home, 2017.
[16] W. Jiang, "An Intelligent Supply Chain Information Collaboration Model Based on Internet of Things and Big Data," IEEE Access, vol. 7, pp. 58324–58335, 2019.
[17] J. Du, V. Sugumaran, and B. Gao, "RFID and Multi-Agent Based Architecture for Information Sharing in Prefabricated Component Supply Chain," IEEE Access, vol. 5, pp. 4132–4139, 2017.
[18] A. Pundir, J. Devpriya, M. Chakraborty, and L. Ganpathy, Technology Integration for Improved Performance: A Case Study in Digitization of Supply Chain with Integration of Internet of Things and Blockchain Technology, 2019.
[19] A. Pal and K. Kant, "IoT-Based Sensing and Communications Infrastructure for the Fresh Food Supply Chain," Computer, vol. 51, pp. 76–80, 2018, doi: 10.1109/MC.2018.1451665.
[20] H.-G. Ridder, Case study research: Approaches, methods, contribution to theory. München: Rainer Hampp Verlag, 2016.
[21] Burniske, C. and Tatar, J., "Crypto-Assets," 2018.
[22] Drescher D., "Blockchain Grundlagen," 2017.
[23] Bocek T. et. al., "Blockchain Engineering in Ercim News Online," Vol. 110, 2017. [Online]. Available: https://ercim-news.ercim.eu/images/stories/EN110/EN110-web.pdf
[24] S. Abeyratne and R. Monfared, "Blockchain Ready Manufacturing Supply Chain Using Distributed Ledger," International Journal of Research in Engineering and Technology, vol. 05, pp. 1–10, 2016.
[25] S. Kim and G. C. Deka, Advanced Applications of Blockchain Technology. Singapore: Springer Singapore, 2020.
[26] M. Samaniego, U. Jamsrandorj, and R. Deters, "Blockchain as a Service for IoT," in 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2016, pp. 433–436.
[27] Augusto L., Costa R., Ferreira J., and Jardim-Goncalves R., "An Application of Ethereum smart contracts and IoT to logistics," in 2019 International Young Engineers Forum (YEF-ECE), Costa da Caparica, Portugal, May. 2019 - May. 2019, pp. 1–7.
[28] F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues," Telematics and Informatics, vol. 36, pp. 55–81, 2019, doi: 10.1016/j.tele.2018.11.006.
[29] C. Maple, "Security and privacy in the internet of things," Journal of Cyber Policy, vol. 2, no. 2, pp. 155–184, 2017, doi: 10.1080/23738871.2017.1366536.
[30] S. Saberi, M. Kouhizadeh, J. Sarkis, and L. Shen, "Blockchain technology and its relationships to sustainable supply chain management," International Journal of Production Research, pp. 1–19, 2018, doi: 10.1080/00207543.2018.1533261.
[31] K. Korpela, J. Hallikas, and T. Dahlberg, Digital Supply Chain Transformation toward Blockchain Integration, 2017.
[32] L.-W. Wong, L.-Y. Leong, J.-J. Hew, G. Tan, and K.-B. Ooi, "Time to seize the digital evolution: Adoption of blockchain in operations and supply chain management among Malaysian SMEs," International Journal of Information Management, vol. 52, 2019, doi: 10.1016/j.ijinfomgt.2019.08.005.
[33] A. Koenig, BITCOIN - Geld ohne Staat: Die digitale Währung aus Sicht der Wiener Schule der Volkswirtschaft, 3rd ed. München: FBV, 2018.
[34] R. K. Yin, Case study research: Design and methods. 5th ed.
[35] P. Mayring, Qualitative Inhaltsanalyse: Grundlagen und Techniken, 12th ed. Weinheim: Beltz, 2015.
[36] M. Queiroz and S. Fosso Wamba, "International Journal of Information Management Blockchain adoption challenges in supply chain: An empirical investigation of the main drivers in India and the USA," International Journal of Information Management, vol. 46, pp. 70–82, 2018, doi: 10.1016/j.ijinfomgt.2018.11.021.
[37] T. Gürpinar, N. Große, M. Schwarzer, E. Burov, R. Stammes, P. Ioannidis, L. Krämer, R. Ahlbäumer, M. Henke. Blockchain Technology in Supply Chain Management – A Discussion of Current and Future Research Topics. European Alliance of Innovation - Smart City 360, 2022, doi: 10.1007/978-3-031-06371-8_32.
[38] T. Gürpinar, M. Austerjost, J. Kamphues, J. Maaßen, F. Yildirim, M. Henke. Blockchain technology as the backbone of the internet of things - A taxonomy of blockchain devices. Conference on Production Systems and Logistics, 2022, doi: 10.15488/12170.
[39] T. Gürpinar, S. Harre, M. Henke, F. Saleh. Blockchain Technology - Integration in Supply Chain Processes. Hamburg International Conference of Logistics, doi: 10.15480/882.3117.

Supply Chain Automation with Smart Contracts – Assessing Potentials of Blockchain Technology in the Logistics Sector

Beat Weichsler
Westfälische Wilhelms-Universität Münster, Schlossplatz 2, 48149 Münster

As economies are getting more and more interconnected, the importance of the global logistics sector grew accordingly. However, both structural challenges and current events lead to recent supply chain disruptions, exposing the vulnerabilities of the sector. Simultaneously, blockchain has emerged as a key innovative technology with use cases going far beyond the exchange of virtual currencies. This paper aims to analyze how the technology is transforming global logistics and its challenges. Therefore, six use cases, are presented to give an overview of the technological possibilities of blockchain and smart contracts. The analysis combines theoretical approaches from scientific journals and combines them with findings from real-world implementations. The paper finds that the technology can change supply chain design fundamentally, with processes and decisions being automated and power within supply chain structures changing. However, implementations also face technological, environmental, and organizational challenges that need to be solved for wide-spread adoption.

1. Introduction

This paper is going to analyze the possible applications of DLT in the supply chain context. The main question to be answered is whether and how the technology can be used to overcome existing problems in Supply Chain Management (SCM) and how to create additional value to supply chain stakeholders. Therefore, 4 key questions are to be answered:

1. How do distributed ledgers work from a technical perspective? What are the currently available options available for real-world implementation?
2. What use cases using DLT have already been theoretically developed? Have they seen successful real-world implementation?
3. What are major problems related to the implementation? Are they a thread for the future success of DLT in Supply Chain Management?
4. Taking everything into consideration; how impactful is the technology going to be for the future of supply chains?

To answer that question, first, a short analysis of both the global logistics sector and the status quo of blockchain technology is being given. Afterwards, a detailed analysis of how Distributed Ledger Technologies (DLT) can bring innovation to the logistics sector is being given. Therefore, a deep dive into six use cases is conducted, including both economic and technological perspectives. Finally, these findings are being discussed regarding challenges and overall future implications for the industry.

2. Theoretical Foundations

This chapter is going to give an overview of important basics and notations for this paper. First, the current state of the logistics sector is being outlined. Afterwards, important foundations of DLT are being introduced.

2.1. Status Quo of the Global Logistics Sector

With the trend of globalization in the last decades and the establishment of more and more interconnected supply chains, logistics have emerged to become a central part of the global economy. According to the World Bank, the global GDP peaked in 2019 at $84.6 trillion [1]. 11% of this GDP, $9.3 trillion, are thereby trade-related costs [2]. This is up from 2010, were trade-related costs made up 10.53% of the global GDP at that time. the global logistics sector can be divided into several subcategories. It is notable that over 55% of the market can be contributed to the two largest categories, with “Road Freight Transport” being the largest with 32.43%, followed up by “Warehouse and Distribution” with 26.67%. After that, a large gap occurs, and the following categories “Domestic Parcel Delivery” and “Contract Logistics” can consequently only contribute to less than 5% of the entire market.

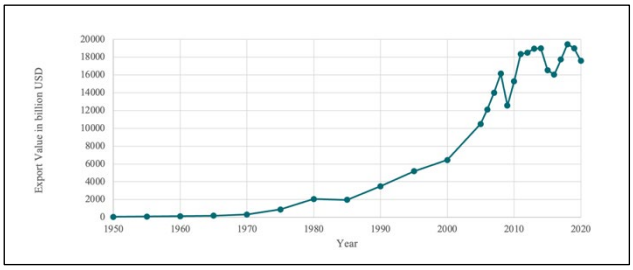

Figure 1: Trade Export Value in billion US dollars [3]

However, while enabling modern globalization, the logistics sector also faces challenges. Looking at the data of Global Trade Export Value in figure 1, we can see that from 1950 to 2008, the growth of the global trade export value was only accelerating. However, since 2008, we can analyze both a general slowdown in year-to-year growth as well as 3 major pushbacks in the years 2008, 2014 and 2019.

This can be traced back to two structural problems of the sector as well as current geopolitical events. First, the

high uncertainty among supply chains leads to an increasing amount of disruption. In 1996, Richard Wilding introduced the "Supply Chain Complexity Triangle", combining all major sources of supply chain uncertainty into one framework [4]. The three dimensions thereby are "Amplification of Demand", "Deterministic Chaos" and "Parallel Interactions". Second, the increased use of Just-in-Time Manufacturing in the recent years furthers stresses global trade. While the "strategic implementation of the JIT approach significantly improces manufacturing performance" [5], it also leads to less resistant supply chains that do not tolerate a large amount of disruption because of low reserves and high interdependencies.

Additional to the structural challenges, current geopolitical events further strained the interconnected logistics sector. The most notable event was thereby the Covid-19 pandemic. The measurements against the spread of the virus caused a wide range of new challenges and problems to the global economy and supply chains. Even after the introduction of vaccines in 2021, local outbreaks in producing countries like China and Vietnam regularly lead to lockdowns and disruptions along the entire supply chain [6]. On 23 March 2021, one of the most used shipping routes in the world, the Suez Canal, was blocked by the container ship Ever Given. Over 400 vessels were directly affected by the event, leading to an economic damage in the billions [7].

2.2. Technological Foundations of Distributed Ledgers

To analyze use cases in chapter 3 and the overall impact on the industry in chapter 4, it is important to firstly understand the theoretical foundations of the technology. Therefore, important concepts and their technological boundaries of DLT are being introduced.

First, it is important to understand the difference between centralized, decentralized, and distributed data processing. Centralized Computing refers to a data set controlled and operated by one entity. This entity has the entire power to decide upon changes in the data set. Decentralized Computing means that data and/or computing is shared across at least two entities. These entities can however have different roles, for example one is allowed to only access the file, while another is allowed to change the data set. Distributed computing is a subset of Decentralized Computing. All data and decision power are shared across multiple servers in the system, also called nodes, with each node having the same rights [8].

Blockchain is one implementation of a distributed ledger. As its name suggests, its data is stored in a chain of blocks. The data structure of a block contains the hash of the respective block, the hash of the previous block, and finally the data itself. A hash of a block is generated by an algorithmic function transforming the blocks' data into a shorter key. It is often referred to as a "Digital Signature" of the data. Having the hash of the previous block also integrated ensures that a change of data in the previous block could directly be detected when comparing the hashes [9]. Because of its design, blockchain has far-reaching characteristics centralized data storage cannot match. Information that is stored within a block is immutable to changes, as this would require all following blocks to also adopt the changes. Additionally, the decentralization increases safety concerning failure of single nodes. As the data is spread across multiple entities, one failure is not going to have an impact on the entire system. Finally, blockchain is transparent and its data visible to all participating nodes.

To ensure all participating entities agree to the same data set within the ledger at any given point of time, a consensus mechanism is required. At the moment of writing, two mechanisms are relevant when comparing different blockchains. The first one, Proof-of-Work (PoW), requires miners. Miners are network nodes that take part in the approval process, exchanging computational power against assets. Therefore, different nodes compete against each other. The "winner" can verify the block and add it to the chain – therefore it receives a fee [10]. The second, Proof-of-Stake (PoS), also requires nodes willing to participate in the approval process. Instead of mining, nodes are required to deposit a certain amount of assets. Whenever a new block is proposed, a lottery system chooses one of the nodes with a deposit. This node can now approve the block and receive the transactional fee. As the deposit always needs to be higher than the transactional fees, there is no incentive to manipulate the system [11].

3. Analysis of Supply Chain Use Cases Using Blockchain Technology

This chapter is going to explore the application of DLT within Supply Chain Management. Therefore, a literature review has been conducted to find relevant theoretical approaches, of which six have been found. Additionally, a look at practical implementations of these approaches has been done to evaluate real-life status of the ideas. The six uses cases have been categorized in three fields of implementation, which are going to be presented now.

3.1. Increasing Supply Chain Visibility and Data Transferring

This category includes two use cases that create value by generating and using information about the supply chain and making this visible in a trusted, non-changeable way.

3.1.1. Status Quo and Problems Today

Data sharing across the supply chain is an important part of modern SCM as different stakeholder possess important information being relevant for all entities. For example, downstream retailers have better information about the final customers and overall market trends, while upstream retailers have an information advantage

regarding product quality and preliminary product availability. Therefore, a lack of data sharing leads to lost sales, double marginalization, and overall customer dissatisfaction [12].

However, and according to the article "Building a transparent Supply Chain", published in 2020 by the Harvard Business Review, current technologies are often not sufficient for data collection. This can be illustrated by the example of a simple scenario where a retailer buys a product from a supplier with a bank providing the necessary capital. For that transaction, information flows, inventory flows and financial flows are generated. However, not all flows are being saved in all the Entity-Resource-Planning (ERP) systems. Therefore, drawing the connection between all three flows and entities is, especially in a real-world complexity, ex-post not possible [13]. Using technologies like blockchain might be a solution to this problem, creating transparency and value along the entire supply chain.

3.1.2. Use Case 1: "Increasing Supply Chain Transparency"

In many industries, this need for supply chain transparency is especially important. One of those industries is the agri-food sector, where information is not only used to create additional value but is also necessary to validate the origin and quality of the products. Today, this additional information is not only requested by the retailers, but also by the final customer, who generally demands more transparency [14].

To solve that issue, different papers suggest an implementation of blockchain technology to enhance transparency. The paper "Blockchain-based Traceability in Agri-Food Supply Chain Management: A Practical Implementation" aims to design and evaluate the impact of a communication system that is based on decentralized blockchain technology [15]. Therefore, a system called "AgriBlockIoT" is presented, that combines the use of modern sensor technology and Internet of things (IoT) devices like radio-frequency identification (RFID) systems and wireless sensors as well as a blockchain network to connect them. AgriBlockIoT can then store all relevant information of the entire food supply chain and make this visible to all stakeholders. The concrete implementation varies from industry to industry, but it is necessary to list all participating supply chain stakeholders and decide-upon which information is supposed to be added to the blockchain. Additionally, for each stakeholder, IoT devices can support the data capturing and uploading. For example, the packaging company can gear up its machinery with smart weights for automatic detection and uploading of weight information.

This leads to a completely new way of interaction between supply chain stakeholder, shifting away from linear communication flows to a multi-dimensional communication model, as shown in figure 2.

Additional to the process documentation, smart contracts can be implemented to trigger certain actions when anomalies are being detected. Overall, the implementation of the process clearly holds advantages to all participating parties. Firstly, all stakeholders have all information available at any time. Second, the manual documentation and communication effort can be reduced, as shown in figure 2.

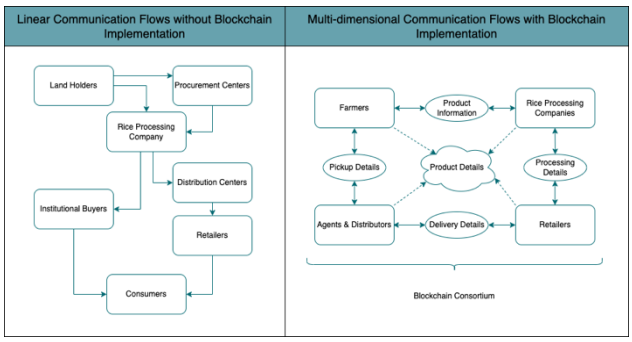

Figure 2: Communication Flows in Use Case 1 with and without Blockchain [16].

Looking at the real-life implementation of this use case, we find many companies, both established and start-ups, having tried out different approaches in that regard. One of the leading companies in that area is London-based start-up "Provenance" [17]. The company focusing on delivering transparency and value for the final customer, with their product including a proof of certificate for final customers, a digital map with all supply chain stakeholders, and integrated third-party certifications. Provence has a total funding of $6.6m, having finished the latest round worth $5.3M in March 2022 [17].

3.1.2. Use Case 2: "Enhancing Supply Chain Risk Identification"

Supply Chain Risk Management (SCRM) refers to "the implementation of strategies and plans to manage supply chain networks through constant risk assessment and reduce vulnerabilities to ensure resilience in supply chain" [18]. It is an important part of SCM. Risks can thereby be classified into two categories, endogenous risks, which includes moral risks, information delivery risks, and procurement risks, and exogenous risks, which refers to market demand risks as well as policy and legal risks [19].

An exemplary SCRM process can follow these steps in the respective order: "Identify Risks", "Asses & Prioritize", "Develop a Treatment Plan", "Reduce Risk Exposure", "Reduce Impact ex post", "Review and Learn" [20]. It makes sense to apply the findings of use case 1 with a focus on potential risks for a more effective SCRM. The additional and verifiable information gained by blockchain implementation throughout the supply chain can result in various findings. For example, it might help to identify geographic concentration of production resources, logistical dependency on certain companies, or other risks not visible earlier.

The paper "Big Production Enterprise Supply Chain Endogenous Risk Management Based on Blockchain" investigates this approach in industrial supply chains. It concludes that while blockchain adoption might be not helpful to discover exogenous risks, it states that endogenous risk detection can be improved and implementation of DLT is reasonable and feasible [21].

As of March 2022, we can also see first real-world adoptions of blockchain technology in SCRM, especially in the agri-food sector. For example, IBM FoodTrust is one implementation of that use case. It enables retailers to connect their whole supply chain to a private blockchain. If a food safety issue is reported, it is immediately clear who caused the problem and what products are affected.

3.2. Process and Decision Automation

As the use cases focusing on better data visibility from chapter 3.2 have been presented previously, this chapter is going to give an overview of cases that interact deeper with the supply chain functionality.

3.2.1. Status Quo and Problems Today

Many processes along the supply chain are still often very manual, having only a low level of automation. This low level of automation can be traced back to two main reasons. Firstly, as analyzed earlier, supply chains' complexity increased over the last years, with many steps and stakeholders added. Secondly, regulatory authorities often still require a large amount of manual documentation.

The low level of automation does not only result in high opportunity cost. Another big problem is false information or inaccurate data. Research suggests that 10% of freight invoices contain inaccurate data which ultimately lead to disputes and further process inefficiencies along the supply chain [22]. Therefore, automating processes along the entire supply chain is an interesting category of use cases, of which two examples are going to be presented in the following.

3.2.2. Use Case 3: "Automatic Creation of Documents"

The first presented use case refers to the automatic creation of documents. Trade in general, but especially international shipping requires a lot of documentation. The most important document is thereby the Bill of Lading (B/L). This document can be seen as the main contract between the exporter and importer. Also, it states all relevant terms and conditions agreed-upon. In modern shipping, it also acts as trigger for payment cycles and has further information based on legal requirements. In most cases, B/L are still print-out papers that require wet signatures for relevant milestones. The administrative costs of this B/L creation and updating is estimated to make up 37% of the total freight forwarder fees [24].

The paper "Addressing some of bill of lading issues using the Internet of Things and blockchain technologies: a digitalized conceptual framework" introduces one way to completely automate all B/L-related processes. Therefore, containers and shipping gates are being outfitted with IoT technology, especially sensors and internet connectivity, so that devices can communicate directly with each other and without an intermediary.

Afterwards, a blockchain with five key components is being implemented. First, a privacy protocol cryptographically hashes all relevant data submitted through the supply chain. Second, a transaction ledger creates transaction when pre-defined milestones (e.g., arrival of a container in the harbor) are achieved. Third, a consensus mechanism verifies the authenticity of the suggested transaction. If approved, the transaction is being added into a block. Fourth, smart contracts are being triggered by the transactions and enforce agreed-upon terms, like the payment in cryptocurrency from wallet A to wallet B. Finally, whenever a transaction is completed, blocks are being added to the blockchain.

Regarding real-life implementation it is notable that this is not only a theoretical approach but has already been implemented by many different companies. Besides in-house solutions of large shipping companies, some start-ups around the world have emerged to offer an electronic bill of lading on a blockchain basis as-a-service, one of them being Slovenia-based start-up CargoX. Its product is built-upon Ethereum and offers the digitization of various types of freight documents, a full-text search across all documents, validation of the original source and prove of ownership, as well as a customizable interface [24]. CargoX raised $7m via an Initial Coin Offering (ICO) in 2018, however newer financial data is not available [25].

3.2.3. Use Case 4 "Automatic Coordination and Revenue Sharing"

Instead of only focusing on automating certain process elements to increase visibility and reduce operational costs, blockchain implementation can also be used to automate decisions across the entire SCM. The paper "Intelligent Smart Contracts for Innovative Supply Chain Management" suggests an approach that automates both, supply chain coordination in terms of supplier selection, as well as a fair ex-post revenue sharing. The goal is to create a framework that pre-defines all necessary criteria. Decisions are then being shifted away from the supply chain coordinator and are being made by the respective smart contracts.

To share revenue in a transparent way, a smart contract is being set up including a revenue sharing algorithm, following five steps. First, it calculates the average unit cost c_{sme} each member must bear within the supply chain. Second, for each resource, a minimum possible cost of competing suppliers ck_{min} is identified. As soon as the smart contract gets triggered, the algorithm distrib-

utes ck_{min} to all suppliers. Then, alignment costs are being distributed. These refer to expenses that occur for a single supplier to align with the greater interest of all supply chain members. Finally, the remainder is being shared as profit among all participants by a pre-defined clearing key.

The second part introduced by the paper is the automated supply chain coordination. Therefore, the originator firstly initializes the process by predefining all criteria on the blockchain. These include the product criteria, such as required parts, quantity, quality, delivery methods, and deadlines, as well as the overall profit and clearing keys for all parts, and finally the deadline for bids from suppliers. When all information is published on the network, suppliers can start to place bids. Finally, when the deadline has passed, a smart contract gets triggered that formally places all orders at the suppliers.

Overall, the blockchain-based network automates the manual process of finding the best supply chain partners. It offers clear advantages to the currently obscure bidding processes for all participating parties. This part was now investigated with a focus on the originator. If we imagine a system where the bidding process is also being automized, e.g., by smart contracts that bid automatically when certain conditions are met from supplier side, we can imagine how this network creates completely new supply chain designs that manually were not to be emerged.

3.2. Sustainability & Governance

This chapter is going to give an overview of how DLT can be used to create improvements regarding sustainability goals. Therefore, a short overview of the current situation is given as well as deep dives into two use cases.

3.3.1. Status Quo and Problems Today

Companies nowadays are facing the pressure from multiple stakeholders to ensure their business operations are meeting modern Environment, Social & Governance (ESG) standards. On the one hand, consumers are paying more and more attention regarding sustainability when choosing products to buy [26]. On the other hand, investors are looking closely on the ESG performance of their assets and are willing to pay a premium for socially responsible investments [27].

One major problem when looking at ESG performances is however information availability and trust. As Goldman Sachs points out in an article, a significant amount of ESG data on companies are self-reported making it difficult to objectively compare the information [28]. Additionally, more and more concerns are rising regarding Greenwashing. Therefore, it seems logical that companies should investigate whether new technologies can help to make their ESG data better comparable and more meaningful. In this chapter, two use cases are presented that do increase ESG performance by applying DLT to their operations.

3.3.2. Use Case 5: "Real-time Emission Reduction in Supply Chains"

As described in the previous use cases, blockchain is a suitable technology to increase visibility and transparency along the supply chain. This use case applies data from the blockchain to feed an algorithm to reduce carbon emissions.

This blockchain-based system was presented in the paper "A blockchain-based approach for a multi-echelon sustainable supply chain" and later-on tested by a simulation. Therefore, an exemplary supply chain having suppliers, manufacturers, distributors as well as a central manager controlling the entire chain was designed. Within that framework, an algorithm was developed to include all relevant data inputs, such as inventory, labor, and transport costs. Additionally, carbon emissions were converted to a monitorial value to conduct optimization with one variable only. The system then follows a 3-step approach.

1. In the "Initializing Phase", a first optimization is being done by inserting all available data points as input for the algorithm. The outputs, including Economic Order Quantity (EOQ) for each outlet and inventory storages, are being uploaded to the blockchain. Additionally, carbon threshold limits are being determined, quantifying the maximum allowed carbon emission per product.
2. The "Intervening Phase" is the part where blockchain technology is especially needed. Real-time data is being uploaded to the blockchain and emissions per product piece are being constantly calculated. If a limit of a certain outlet is being reached, a smart contract triggers the main system to start the "Optimization Phase".
3. In this third phase, all new data points are being downloaded from the blockchain and the algorithm is being executed with the updated information. As soon as a new optimum is being found, the instructions are being updated in the blockchain and the "Intervening Phase" starts again.

To give an example how this system might reduce CO2 emissions, imagine a factory in Malaysia having higher energy costs than expected because the weather is warmer than the annual average. If emissions are exceeding the pre-defined limits, the algorithm is going to investigate whether using another factory in China for the next batch has a lower emission cost, thus lowering overall carbon emission and creating an overall more environmentally friendly supply chain.

In a simulation using so-called MATLAB software, this system was compared to a standard supply chain optimization using a NSGA-II algorithm [29]. Different CO2 prices were tried out, and the blockchain approach could outperform the industry standard by reducing emission cost on average by 2.58%. Additionally, overall opera-

tional costs were lower in all cases independently of order demand. It is however important to note that this simulation cannot reflect real-world complexity. Therefore, the results should be seen rather as a proof-of-concept than a real validation of the superiority of the blockchain-based system [30].

3.3.2. Use Case 6: "Creating Traceable Circularity in Supply Chains"

As the concept of Circular Economy (CE) is a growing trend, current research is investigating the necessity for Circular Supply Chain Management (CSCM). Even though the terminology and the boundaries of CSCM are not clearly defined yet it becomes evident that the sector is driven by two main visions: firstly, the goal of a zero-waste economy, and secondly the generation of restorative and regenerative production cycles [31].

The basis of this chapter is an approach presented in the paper "E-waste Management Using Blockchain based Smart Contracts". However, certain adjustments have been undertaken. Firstly, the system is being generalized from a focus on the Indian recycling eco-system to fit for a global implementation. Secondly, a credit system is introduced that creates financial incentive for recycling, thus eliminating the need for penalties from governmental agencies as proposed in the paper. Thirdly, the conclusion to circularity of the entire supply chain is being conducted and presented. Lastly, an overall score was created to give consumers further insights about the level of circularity of a respective product.

The first step in this adopted approach is to bring all stakeholder on the same blockchain network, including the implementation of smart sensors to track activities and interfaces for users. The stakeholder in this process are the producers, the retailers, the consumers, the collection centers as well as recycling units. The second step is that smart contracts are being developed that allow the assignment of a unique ID to every product in the supply chain. Additionally, a credit score is being calculated. This score is being generated by the value of the raw materials within the product, multiplied by a certain factor larger 1. The larger this factor is, the higher the incentive for all supply chain stakeholders to participate in the entire recycling process. However, a higher factor also leads to a higher purchasing price for the final customer, potentially lowering the attractiveness of the offer. The third step happens through the entire product-lifecycle. To ensure the product does not only make it to the customer, a credit score has to be paid whenever the product changes its owner. Therefore, the retailer pays the producer, and the consumer pays the retailer (step 1 and 2 in figure 3). As the product is not used anymore, the user can give it back to the retailer, thus receiving back his money. The retailer can afterwards return the product to the producer, who is responsible for the follow-up recycling process. All payment processes are automated with smart contracts, giving all parties the certainty that credits are going to be paid back. The exact process is modelled in figure 3, showing all physical and financial transactions.

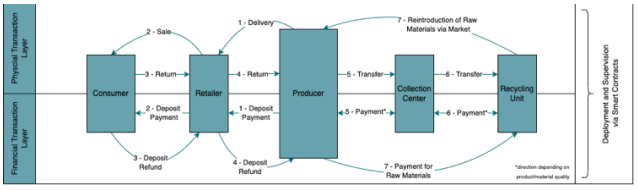

Figure 3: Proposed Circularity of Use Case 6. Own Representation.

Additionally, as all product transactions can be non-alterably traced ex-post, a score can be calculated in real-time, showing the degree of recycling every product has. For example, a shoe designed in a way that a lot of resources could be recycled in the past receives a good score that could be used for marketing purposes.

While this exact approach has never been implemented, also because it was partly modified in this paper, similar approaches have been conducted already. The US-based specialty chemicals manufacturer Eastman Chemical has developed a blockchain network together with German software company SAP that can certify products with an exact percentage of recycled materials used in production as well as a tracking of that process over time. According to Eastman Chemical, this project has the potential to "be a turning point for the circular economy" [32].

4. Discussion of the Findings

4.1. Blockchain Implementation in Supply Chains Today

According to the analysis conducted in chapter 3, two main categories of blockchain penetration depths could be found. First, low-level use cases, focusing on increased visibility and low-level process automation can be seen. This category includes use case 1 and 3 of this paper. The technology of blockchain in these cases are seen as a tool to enable an evolutionary progress. However, the technology does not really change the way supply chains are designed or decisions are being made. Therefore, it cannot be seen as a revolution within Supply Chain Management.

The second category however refers to higher-level use cases, such as cases 2, 4, 5, and 6. Here, the increased visibility and transparency enabled by DLT is used to create deeper interference with the management of supply chains. Therefore, decisions, like the process of choosing the best manufacturer, are being shifted away from single supply chain stakeholders and are instead exercised by pre-defined conditions within smart contracts. This category is indeed to be seen as revolutionary, as it transforms supply chain design and shifts power from stakeholders to the technology.

Looking at real-world implementations, it is noticeable that many companies did already implement pilots of the lower-level use cases. By just increasing visibility and

automating low-level processes, companies can try out the possibilities of the technology and build up internal blockchain competences, without risking a falsely implemented smart contract to result in the malfunction of a supply chain. The higher-level use cases however only start to emerge in the real world. Scientific papers are already proposing specific instructions of how the technology might be implemented and simulations being conducted to understand the implications, and it is to be expected that more and more real-world implementations of these ideas are to be seen in the next years.

4.2. Identified Problems & Concerns regarding Blockchain Implementation

The reason why real-world implementation, especially of higher-level use cases, are however slow to emerge is because even though possibilities are promising, companies are also facing a lot of challenges. To better understand the barriers of real-world adoption, the TOE-framework, developed by Tornatzky and Fleischer in 1990 is going to be used.

Firstly, technological problems occur within blockchain implementation. A big challenge are thereby security challenges, such as 51% attacks on smaller networks and endpoint vulnerabilities from user interfaces and APIs. Additionally, the immutability of blockchain does also create challenges. It is difficult to impossible to change data within blocks, even though if false information has been uploaded. Thirdly, according to a representative study by the World Trade Organization, Standardization, Interoperability and Integration to back-office systems are a big hurdle for real-world implementation [33].

The second dimension of the framework refers to all environmental problems. Firstly, legal and governmental uncertainties are a huge problem. While different countries indicate different approaches regarding future legislation of crypto projects [34], also current laws are partly in conflict with DLT. Article 17 of Europe's GDPR states the so-called "Right-to-Forget", meaning companies must delete user data on request. It is however unsure how this can be done for date stored in blockchains.

The last dimension investigated are organizational problem. Thereby, a lack of management expertise and commitment can be observed [35]. This means that decision makers are not fully aware of the possible implications DLT might offer. Adding to that, the high implementation costs of blockchain developments lead to a lower motivation to implement DLT projects.

4.3. Possible Implications for the Future of Supply Chains

While it is difficult to predict and quantify the exact degree of innovation DLT is going to bring to the logistics sector, it is safe to say that some parts of it are going to be evolutionary or revolutionary influenced by the technology. All presented use cases that conducted a simulation or real-world comparison of the proposed implementations could see efficiency gains and therefore value creation compared to the Status Quo. Also, the rising number of crypto-startups and their successful financing rounds show that various parties believe in the financial success of DLT. Based on the analysis of this paper, three assumptions can be made regarding possible implication on Supply Chain Management:

1. DLT can digitize, automate, and enhance processes in a way earlier technologies were not able to. As analyzed earlier, the complexity of supply chains leads to a situation where white spots regarding automatization can still be found in many places, for example the wide use of paper and wet signatures for the B/L process. The analysis suggests that these white spots will be automated by the implementation of DLT soon.
2. DLT has the possibility to solve basic and structural challenges that have been around in Supply Chain Management for decades. For example, the well-researched bullwhip effect could be significantly reduced. By automating order and prediction processes with smart contracts, the amplification of highs and lows can be reduced. Looking at the contract theory, we can explore a second example. The Grossmann- Hart-Moore model of contract incompleteness states that at the time of contract signing, not all future events can be predicted, thus leading to a deviation from the original agreement at some point of time [36]. With the introduction of smart contracts, that are being pre-defined and are non-changeable afterwards, the degree of contract completeness could be increased.
3. It is to be expected that legislation is going to follow innovation. Theoretical research and practical pilots are already showing today the effectiveness of the technology, therefore putting pressure on governmental bodies to create an environment this innovation can thrive. In the blockchain world, this could be seen already in a financial context. The German authority for financial supervision, Bafin, created a legal environment for crypto-based security token offerings (STO) to enable innovative corporate financing models with a safe legal frame [37].

5. Summary and Take-Aways

To assess the potentials of blockchain technology, this paper first gives an overview of important concepts and currently available implementation options. Thus, the differences between centralized, decentralized, and distributed computing as well as blockchain technology are explained. Afterwards, in chapter 3, a deep dive into six use cases is undertaken. The paper finds that these cases can be categorized regarding their implementation depth into low-level and high-level use cases, that differ in implications for the supply chain design. Afterwards, technological, environmental, and organizational problems are presented that explain why blockchain technology is only starting to emerge. Many concerns

and questions remain unanswered today, thus, creating a need for further research as well as entrepreneurial action, additionally underlining the importance of combing theoretical and practical approaches for this young technology.

The main question to be answered with this paper is whether and how DLT can be used to overcome existing problems in Supply Chain Management and to create additional value for its stakeholders. The main advantage blockchain is enabling is the increased visibility, trust, and certainty for all supply chain members. However, the implications of using these advantages go far beyond that. The analysis shows that the implementation of distributed technologies can increase supply chain resilience and improve their design. Additionally, different approaches are presented that proved in simulations and pilots that value creation through blockchain implementation does work. However, while promising, the technology cannot be expected to solve all supply chain-related problems. More and more interconnected economies, the effects of JIT manufacturing, and the consequences of geopolitical events are not going to be solved only by automating certain processes with DLT. Thus, to create sustainable, secure, and efficient supply chains that meet the economic and political goals of the next decades, blockchain and DLT can only be seen as one piece that needs to be set and seen in the bigger context.

References

[1] GDP (constant 2015 US$), Retrieved March 8, 2022 from: https://data.worldbank.org/indicator/NY.GDP.MKTP.KD.

[2] Logistics Global Industry Costs 2020, Retrieved March 8, 2022 from: https://www.statista.com/statistics/943500/logistics-industry-costs-worldwide/

[3] Worldwide export trade value 1950-2020, Retrieved March 9, 2022 from: https://www.statista.com/statistics/264682/worldwide-export-volume-in-the-trade-since-1950/.

[4] R. Wilding, The supply chain complexity triangle Uncertainty generation in the supply chain (1996).

[5] J. Singh, H. Singh, Strategic implementation of just-in-time practices for enhancing the performance of manufacturing industry - an empirical investigation. International Journal of Manufacturing Technology and Management, 35 (2021), 369.

[6] A. Swansan, Ukrainian Invasion Adds to Chaos for Global Supply Chains - The New York Times (2022).

[7] J.M. Lee, E.Y. Wong, Suez Canal blockage: an analysis of legal impact, risks and liabilities to the global supply chain, MATEC Web of Conferences, 339 (2021), 1019.

[8] D. Lindsay, S.S. Gill, D. Smirnova, P. Garraghan, The evolution of distributed computing systems: from fundamental to new frontiers. Computing, 103 (2021), 1859–1878.

[9] A. Meier, H. Stormer, Blockchain = Distributed Ledger + Consensus, HMD Praxis der Wirtschaftsinformatik, 55 (2018), 1139-1154.

[10] O. Vashchuk, R. Shuwar, Pros and Cons of Consensus Algorithm Proof of Stake. Difference in the Network Safety in Proof of Work and Proof of Stake, 9 (2018), 106–112.

[11] F. Saleh, Blockchain Without Waste: Proof-of-Stake (2019)

[12] D. Waters, Supply Chain Risk Management: Vulnerability and Resilience in Logistics (2011).

[13] V. Gaur, A. Gaiha, Building a Transparent Supply Chain (2020).

[14] C.N. Verdouw, H. Sundmaeker, F. Meyer, J. Wolfert, J. Verhoosel, Smart Agri-Food Logistics: Requirements for the Future Internet. Lecture Notes in Logistics (2013), 247–257.

[15] M.P. Caro, M.S. Ali, M. Vecchio, R, Giaffreda, Blockchain-based Traceability in Agri-Food Supply Chain Management: A Practical Implementation (2018).

[16] F. Antonucci, S. Figorilli, C. Costa, F. Pallottino, L. Raso, P. Menesatti, A review on blockchain applications in the agri-food sector. Journal of the Science of Food and Agriculture, 99 (2019), 6129–6138.

[17] Provenance - Crunchbase Company Profile & Funding. Retrieved March 16, 2022 from: https://www.crunchbase.com/organization/provenance.

[18] A. Gurtu, J. Johny, Supply chain risk management: Literature review. Risks, 9 (2021), 1–16.

[19] Y. Fu, J. Zhu, Big Production Enterprise Supply Chain Endogenous Risk Management Based on Blockchain. IEEE Access, 7 (2019), 15310–15319.

[20] D. Waters, Supply Chain Risk Management: Vulnerability and Resilience in Logistics (2011).

[21] Y. Fu, J. Zhu, Big Production Enterprise Supply Chain Endogenous Risk Management Based on Blockchain. IEEE Access, 7 (2019), 15310–15319.

[22] M. Kückelhaus, Perspectives on the upcoming impact of blockchain technology and use cases for the logistics industry. DHL Trend Research, Accenture (2018).

[23] E. Irannezhad, H. Faroqi, Addressing some of bill of lading issues using the Internet of Things and blockchain technologies: a digitalized conceptual framework. Maritime Policy and Management (2021).

[24] CargoX, Retrieved March 16, 2022 from https://cargox.io/solutions/for-transport-and-logistics/.

[25] CargoX Crunchbase Company Profile & Funding., Retrieved March 16, 2022 from https://www.crunchbase.com/organization/cargox.

[26] Netherlands: Share of Customers paying attention to sustainability, Retrieved March 18, 2022 from: https://www.statista.com/statistics/656337/share-of-customers-paying-attention-to-sustainability-of-products-in-the-netherlands/.

[27] B.R. Auer, F. Schuhmacher, Do socially (ir)responsible investments pay? New evidence from international ESG data. The Quarterly Review of Economics and Finance, 59 (2016), 51–62.
[28] Measuring the Immeasurable: Scoring ESG Factors, Retrieved March 18, 2022 from: https://www.gsam.com/content/gsam/global/en/market-insights/gsam-insights/gsam-perspectives/2015/esg/qis-article.html.
[29] K. Deb, A. Pratap, S. Agarwal, T. Meyarivan, A Fast and Elitist Multiobjective Genetic Algorithm: NSGA-II. IEEE Transactions on Evolutionary Computation, 6 (2002).
[30] V.K. Manupati, T. Schoenherr, M. Ramkumar, S.M. Wagner, S.K. Pabba, R. Singh, A blockchain-based approach for a multi-echelon sustainable supply chain. International Journal of Product, 58 (2019), 2222–2241.
[31] M. Farooque, A. Zhang, M. Thürer, T. Qu, D. Huisingh, Circular supply chain management: A definition and structured literature review. Journal of Cleaner Production, 228 (2019), p. 882–900.
[32] Eastman collaborating with SAP on GreenToken to track recycled content, Retrieved March 18, 2022 from: https://www.eastman.com/Company/News_Center/2021/Pages/Eastman-collaborating-with-SAP-on-GreenToken.aspx.
[33] P. Deepesh, E. Ganne, Blockchain & DLT in Trade: A Reality Check (2019).
[34] China declares all crypto-currency transactions illegal, Retrieved March 19, 2022 from: https://www.bbc.com/news/technology-58678907.
[35] S. Saberi, M. Kouhizadeh, J. Sarkis, L. Shen, Blockchain technology and its relationships to sustainable supply chain management. International Journal of Production Research, 57 (2019), p. 2117–2135.
[36] S.J. Grossman, O.D. Hart, The Costs and Benefits of Ownership: A Theory of Vertical and Lateral Integration. Journal of Political Economy, 94 (1968), p. 691–719.
[37] Bafin: Merkblatt zur Ausgabe sogenannter Krypto-Token (2021).

The future of soulbound tokens and their blockchain accounts

Felix Hildebrandt
LUKSO Blockchain GmbH, Köpenicker Chaussee 3a, 10317 Berlin

The topic of soulbound, non-transferable tokens is getting lots of interest within the blockchain space lately as decentralized societies become more tangible with Web3 social media applications and DAOs. In this article, I want to outline how such tokens function, their problems for adoption and standardization, and how they differ from verifiable credentials in the SSI field. As such soulbound assets will likely rely on extended recovery and asset management schemes to become viable identities that safely gain reputation and trust, features like social recovery and contract-based accounting are incorporated. By combining those new technologies and the theoretical crypto-native identity construct, the paper will give an impression of the future user-centric data economy.

1. Current NFT Landscape

NFTs are non-fungible, tradable tokens primarily used to represent something of monetary value, but use cases for documenting attendance, skills, and accomplishments have become more prevalent. These tokens are attestations to specific individuals and hold value similar to diplomas, certificates of achievement, or even reputations gained through interpersonal interactions. This use case reveals an issue with current NFT standards: they are transferable and cannot be bound to a specific individual. As Vitalik Buterin discussed [1], today's NFTs are tradable items that can gain value and inevitably become a signal of wealth, even when it is not the original intent.

2. Soulbound Token Functionality

Unlike regular NFTs, soulbound tokens (SBTs) are a concept of non-transferable assets. Once issued, they belong to a specific identity. They cannot move to a new address (without social recovery) and cannot be traded for a different asset. However, they can represent specific values. Soulbound tokens mimic special certificates, accomplishments, accurate proof of attendance, or social interaction graphs that cannot stem from another identity. Issuers of these tokens "are not interested in whether or not you paid someone who attended some event. They are interested in whether or not you personally attended that event." [1]

Bound tokens could be issued by the same account, acting as a post or information about themselves, but also attested or shared by other individuals or institutions. A Web3 attestation flow [2] would enable self-sovereign acting users with attesters and verify instances around them. Handing out such soulbound tokens from others to user accounts would enable bound airdrops from communities or a DAO controlled by accounts with certain SBTs instead of votes that could just be traded, building much stronger bonds within communities.

2.1 Issues with non-transferability

The decision POAP [3] made when creating their attendance token ecosystem breaks down the problems faced with developing bound tokens.

1. Users might have good reasons to migrate their assets to a different wallet for security concerns. Externally Owned Accounts (EOAs), the most prevalent blockchain wallets currently used, are bound to one single recovery phrase that cannot be changed if compromised. That's due to their minimal key-based [4] nature. Users would face the loss of their non-transferable tokens if these accounts became inaccessible or compromised.

2. Users could create a custom smart contract with a transfer or ownership function to hold the bound NFT. With such wrapper contracts, users could sell or trade the asset's "shell" instead of the non-transferable NFT if transfer functions are limited to one or static within an NFT's constructor.

Transferability has led to exploiting tokens that are not meant to be transferred, like secret drops or whitelist spots. One could argue that services that rely on those NFTs can verify ownership by checking if the asset has been moved, but there are further issues:

3. SBTs on EOAs could not exist without external proof and reissuing services. Imagine a user who wants to update their address. They would need to verify that they are the original identity of both the current and the new address, denying that the SBT has not been sold. It would require a dependency/process to authenticate. Such a service is provided by the Proof-of-Humanity attestation service [5] but might get complicated against non-human identities. However, even more cumbersome, every attestation service would have to implement an interface to either burn/reissue or transfer the SBTs, which will cause a tremendous number of transactions for rich histories of interactions.

4. What if only the owner of the anonymous smart contract wrapper has changed without transferring the NFT that it holds? Depending on the management of the roles of such a smart contract, the traceability of SBTs can become unmanageable, as people may just set up a non-standardized and non-bound shell around them.

The conclusion: Soulbound tokens are not easy to implement because they must be issued to specific identities that have met a particular prerequisite, which requires customer verification (KYC) or an established social construct. Once the framework is more tangible, prototypes will likely test different attestation aspects and protocols.

Here, modular standards [6] (LSPs) mainly developed by LUKSO for now, can solve some issues by replacing traditional EOAs with smart contract-based accounts built around the ERC725 Proxy Account [7] standard. Such can contain metadata for storing verifiable information or claims of identities and only use EOAs as their controllers. An example would be Universal Profiles [8], which can have descriptions, pictures, assets, and more data attached. Through a key manager, the account can be controlled by multiple keys with individual permissions, safely allowing numerous devices and services to restrict control of the identity. Unlike key-based accounts, contract-based ones can update security without losing tokens or relying on third parties to reissue assets. Services could only hand out non-transferable tokens directly to Universal Profiles if they prove their ownership through controller keys. Especially such an interface detection for universal contract standards further limits the use of wrapping up assets.

In theory, the only edge case remaining is setting up an abstract identity from an anonymous profile when buying an asset that starts gaining an honest reputation after the first (and final) SBT trade. For example, a Universal Profile that stays anonymous to get some SBTs. Since it cannot secretly sell the SBTs, it sells the whole anonymous account to someone instead. The buyer could change the keys, fill his profile with correct information, and act truthfully. The only remedy would be attesters introducing precautions.

2.2 Hybrid types for extended management

SBTs could also implement a revoke function for issuers or communities, where tokens are initially revocable and transferable before transitioning into a strict non-transferability. To ensure tokens are not financialized and sold to a different party, or if keys are lost or stolen, the issuer could burn and reissue (or transfer) the token to a new wallet. Such hybrid forms could also bring lots of value when proving if the user has authentic community membership or is new to Web3 and does not have his final account set up. Tokens or memberships could be easily revoked within a probationary period or after a duration of unexplained inactivity.

The more SBTs the account has, the easier it would be to prove the identity belongs to that address, thereby confirming the legitimacy of reputation-based NFTs and SBTs held within the account. These systems serve social media purposes, similar to a resume for job applicants. Instead of proving work experience and the completion of assessments, SBTs allow for the growth of online reputation as a means for being recognized and taken seriously. If there is only one SBT and an account with few interactions, it will become difficult to distinguish between honest members and blenders. Uncertainty may lead to actual engagement counters or metrics, as an SBT is only as good as its strict hand-out process and trusted issuer.

2.3 Cutting dependencies

Even if there is no standardization for SBTs yet, the concepts are slowly becoming tangible. Web2 was never built around sovereign identities; instead, machines with their device address connected to central servers and having their data managed and held by external services. [2] Even if Web3 could solve such dependencies in the future, it currently still lacks primitives to represent social identities in the first place. Most blockchain projects have become fundamentally dependent on Web2 or are using Web2-like structures in the backend. Some examples of the dependencies we face:

1. Since EOAs cannot represent profiles independently, NFT artists rely on centralized platforms like OpenSea and Twitter to commit to scarcity and initial provenance and act as authenticated projects. EOAs do not have data attached; they only serve as an address to hold assets and sign data with a private key so that outsourcing appears justified.

2. DAOs that try to move beyond sellable coins for voting often rely on Web2 profiles to authenticate and ensure Sybil resistance. Faucets or quota systems face the same issue. Using the Ethereum Name Service (ENS) as a Web3 equivalent mainly depends on a paid subscription [4], but also just acts as a sellable NFT held by an address.

3. Many Web3 participants rely on custodial wallets managed by centralized entities like Coinbase or Binance. Decentralized key management systems are not user-friendly and lack the functionality to act on happened transfers for tokens or NFTs, making it super hard to manage assets even before building more complex data economies like social media applications.

4. Most services gathering asset information about an account rely on centralized projects like Etherscan since services cannot easily read data directly from the network or smart contracts.

The common sense of criticism directs to the conclusion that there need to be multiple standards between the token and its account to enable convenient and decentralized societies, leading to the next question.

3. What is a soulbound token without a Soul?

Souls as token enclosures in outlined decentralized societies could represent humans, machines, organizations, or anonymous or fictional personalities- anything that requires an identity and a reputation bound to them specifically. An identity has little value without external attestations of abilities, qualities, and character- the building blocks of reputation and trust. SBTs can represent these attestations for Web3 identities, but unlike most tokens today, they hold no value without this bond to an identity instance, e.g., "Soul."

It is crucial not to restrict what a Soul is and what it could become. Through Proof of Humanity [5], a human Soul might be able to expand the field of decentralized finance (DeFi) services into undercollateralized lending. SBTs could represent "digital twins" of real-world assets or other requirements from the DeFi world. But one might also gain a reputation in other communities by having a fictitious identity, as seen by the movement of Web3 communities where NFTs act as entry points to gated communities. SBTs could enable new horizons within public or private communities for both sides.

Still, Souls as regular EOAs make it hard to enable the full capability of SBTs in a decentralized society:

1. There is no standardized way of attaching data directly to the account other than by holding or owning an external contract that might be transferable.

2. There is only one backup seed for each account, and people could quickly lose their Souls and assets. This lack of security is especially problematic for individuals with valuable assets and cross-app reputations stored on one account. Users should not hold their whole identity or Soul on one single, static backup.

3. There is no structure to owning multiple social graphs or tokens with one identity. Every NFT is just thrown onto one address, which can be chaotic without Souls for every service.

4. They lack convenience. EOAs need funds before interacting with anything on-chain, cannot accept or reject transactions, cannot store data themselves, and do not store their set of owned assets in a decentralized, automated way.

In conclusion, SBTs do not directly bring more people into the blockchain ecosystem; it is the framework that surrounds them. Extended account functionalities and convenience are needed for new use cases and mass adoption. Souls must function as a user-centered identity manager, not just a simple token enclosure.

4. Mainstreaming contract-based accounts

As mentioned before, LSPs could be seen as a game changer for decentralized societies. Since 2020 the LUKSO project has been actively building standards to simplify and improve the blockchain experience. It could become the perfect framework for Souls, even without initially considering SBTs. In detail, the combination of an EC725 Proxy Account [7] and LSP2 Storage Schema [9] lets a basic EOA evolve into a contract-based identity that features attaching rich information to it in a unified list scheme that is easily parsable and expandable. This could become useful for direct claims or attached assets on the ERC725 Account. [6] LSP3 [10] further transforms the account into a Universal Profile, adding public data like images, names, tags, and descriptions. With the LSP6 Key Manager [11], a Soul could easily update and upgrade the security to swap out or manage multiple keys and define specific permissions. By having a Storage Schema, the frame of the SBT could already have its metadata before attaching anything to it. It would enable identities to start gaining some initial reputation and interact with each other in an easily accessible way, which is especially needed to go beyond the current Web3 adoption.

In combination, the ecosystem of LSPs [4] will remove numerous dependencies and bring more convenience. For instance, The LSP1 Universal Receiver [12] is a standard for transaction handling that could be used to reject or approve tokens. The feature is not only convenient, but it also allows for the safe listing of specific accounts. The ability to deny specific soulbound tokens and social interactions is vital in the context of Souls, as SBTs are ideally forever connected to an address.

4.1 Social Media adoption for Web3

LENS [13], a popular blockchain social media protocol, can serve as an example that further outlines the burdens of EOA-Souls. The project uses EOAs to receive an NFT that mimics account profiles. Using NFTs as profiles has considerable disadvantages. The social media identity is not only attached to a static EOA key but also uses regular transferable NFTs, which means Souls purely rely on data from held assets instead of data being directly attached to the account. Not just profiles, but also interactions (posts, follows, comments, or reposts) are represented by an NFT. Since there is no functionality to accept or deny incoming assets, bot accounts could register handles, follow spam channels and send NFTs representing a follow to other accounts, which would propagate the unapproved content within their feed. This spamming could get even worse if spam attesters handed out SBTs. Therefore, prompt or discard by default should be common sense when introducing future SBTs. By using the NFT method, multiple profiles could also be sent to one EOA, making them unusable with any social graphs, as their interactions are not linked directly. Uncontrollability of asset transfers may be why Aave, initiator of the protocol, is hesitant to issue handles.

Even for the organization of assets and attached services, LSP9 offers Vaults [14] that mimic profile subfolders or separated wallets, keeping NFTs well organized and enabling services to read and write contents from or to certain sub-contracts. This categorization might

become essential long-term when things like social media posts fill up accounts with thousands of NFTs. For SBTs, it has to be said that such Vaults would also need to be bound. Without proper organization, searching for a token from the past becomes unwieldy. This chaos can already be seen on some OpenSea profiles of larger LENS accounts: it quickly happens to lose sight, which will only get messier for future social graphs. Like subdomains on ENS [15], Vaults could be the best solution for these organizational issues. The read access to Vault contracts would further allow users to focus on enjoying social applications. In contrast, the applications manage their transactions but always keep data and rights on the user's side.

4.2 Convenience is essential

LUKSO standards can provide users unprecedented convenience and reduce dependencies on centralized entities [16] with standards for tracking received assets and a tool to subsidize transaction fees. Currently, most blockchains rely on centralized instances like Etherscan's block explorer to query a profile's current and previously owned assets and transaction history. For future decentralized societies, frequent tokenized rights or interaction checks will result in heavy demand for these queries. LSP5 [17] and LSP10 [18] keep track of every owned asset or Vault by default. This information can always be read directly from the contract, removing the need for block explorer APIs and making room for truly decentralized frontends.

Developing a novel blockchain ecosystem goes beyond the creation of smart contract standards. A standardized off-chain relay tool [19] built by LUKSO also allows services to pay for transactions and execute them on the user's behalf. Users are alleviated from directly paying fees, so they no longer have to get coins from crypto exchanges to start interacting with the blockchain. Projects and companies can develop new business models, such as advertising or subscription-based financing, network quotas allowances, or subsidized onboarding. These features provide a more familiar experience for the user, significantly lowering the entry barrier for newcomers who expect a Web2 user experience. For services like LENS, users would not have to get MATIC tokens before claiming a handle or publishing a post. Instead, EVM-based projects could run their funded off-chain relay service to create better onboarding.

Using extended complexity like smart contracts as accounts requires more gas per transaction and therefore comes with a higher cost. The team at LUKSO spent years developing those fundamental building blocks and making them as modular and lightweight as possible. However, it won't be the best experience on occupied networks, which are struggling with fees already. If most of the network still uses EOAs, they further heavily lack the feature set while interacting with contract-based accounts. Blockchain standards can only achieve long-lasting and proper convenience if the entire ecosystem relies on them. That's why LUKSO focuses on a standalone ecosystem. However, standards and tools are compatible with all EVM chains and developed for various economies.

5. The need for community recovery

The last chapter explained the significant impact contract-based accounts bundled with a key manager could offer for Soul recovery. For security concerns, services could implement varying burn-and-reassign methods for SBTs. One example would be using social recovery schemes [20], where trusted relationships are relied upon to back up a Soul instead of just creating more self-recovery options for the user. But defining the right set of Souls to restore an identity might be difficult. The user must balance choosing a significant enough number of friends to avoid both power positions and collusion. Group size can have a substantial effect on interpersonal relationships within a group. Collective thinking dominates in large groups, as opposed to small groups, where each voice carries more weight and has a high impact in the event of discrepancies.

For social recovery decision-making, large groups may succumb to a collective opinion more than the individual's wishes. In contrast, smaller groups with closer interpersonal relationships can more accurately manage a Soul's wishes but have less collective accountability, making them more prone to collusion. Here, death, disputes, or falling out of touch would require frequent updates to maintain a successful recovery.

A more robust solution, is tying Soul recovery to its memberships across communities or services, drawing on a broad set of real-time relationships for security. [21] People a user currently and frequently interacts with could attest that an old account is no longer accessible or under that user's control. After a certain number of attestations, the previous SBT can be removed, and a new token reissued to a new address. Such a community recovery model would require consent from a member belonging to a qualified majority of a random subset of Soul communities.

By "embedding security in sociality," [21] users can constantly regenerate the keys to access their accounts through community recovery, deterring Soul theft or sale. If someone wants to sell a Soul, he would also have to bribe all his recovery relationships, annihilating its or his social circle's credibility.

Social recovery does not provide a solution for recovering compromised EOA private keys from an attacker. Once known, the attacker can always act as the compromised identity, since the backup is static. Again, a set of smart contract-based accounts could likely bring SBTs forward. Mainstream adopters could secure their identity with multiple private keys for different devices. Since the smart contract address will stay the same, SBTs would not need to be burned and reissued from old

addresses. Only the keys and security will require updating through recovery, reducing the overhead issuers would deal with. LSPs, as sophisticated building blocks coming out of the ERC725 Alliance [22] work field, are a giant leap forward in developing security options for the ecosystem. With changeable keys with different permissions, hackers will likely be limited in functionality by default. If set up correctly, the scheme efficiently prevents unauthorized users from accessing the higher permission keys of the Soul. Proper backups, like community recovery, could be added in the future to act as the final option for regenerating keys to control a lost Soul.

6. Caution when binding Souls

Although possibilities may sound promising, people must use Souls with caution and anonymity. SBTs have great potential to "compensate for in-group dynamics and achieve cooperation across differences." [21] Still, they risk being "used to automate red-lining of disfavored social groups or even target them for cyber or physical attack, or enforce restrictive migration policies." [21] Initially, individuals might only carry SBTs that they are comfortable sharing publicly. Still, as most of society grows into such ways of interaction, some will not question the consequences of sharing. An excess of SBTs may reveal too much, making the Soul transparent and vulnerable to social control. Blockchain-based systems used for social media are likely public by default, and so are the profile and NFT data written into contracts. "Any relationship recorded on-chain is immediately visible not just to the participants, but also to anyone in the entire world." [21] If improperly managed, having multiple anonymous Souls and pseudonyms for various social corners and SBTs could make it very easy to correlate different Souls to each other.

Services could use zero-knowledge proofs for linked off-chain data that can only be seen by certain other Souls if revealed. However, when examining the other extreme, having too many private SBTs may lead to hidden communication channels that eschew correlation discounting for governance and social coordination, forming dangerous manipulative bubbles that undermine healthy social systems.

Cheating can also be an uncomfortable subject. "Souls may misrepresent their social solidarity, while coordinating through private or side channels." [21] For example, if SBTs were issued to prove attendance to a required conference, unscrupulous conferences could offer such SBTs in exchange for bribes. With an adequate number of bribed people, Souls and bots could generate fake social graphs that make the account look authentic.

Managing faked social bubbles could become cumbersome for DAOs and their voting power. "Conversely, if SBTs are used to discount coordination, Souls may avoid SBTs to maximize their influence." [21] Coordination is a game theoretical problem on its own. Solutions include creating highly frequented community channels with strong social ties and repeated interactions, similar to school classes or working environments. Services could also require SBTs or strong bonds to others to participate in discussions to detect superficial, collusive groups. Regarding the backend, protocols could implement incentives and punishment systems to encourage honest behavior. Fortunately, there is already research on social media behavior from the recent decade that can be drawn upon.

7. Connection to Verifiable Credentials

For self-sovereign identity (SSI), the W3C [23] has been setting up new standards for years with Decentralized Identifiers [24] (DIDs) and Verifiable Credentials [25] (VCs) to issue certificates. These standards use a Web3-like Identity Flow [2] similar to SBTs, where data is managed in a user-centric way. Issued certificates are shareable depending on the user's location. Still, they often include personal, sensitive items such as driver's licenses or passports and mainly focus on institutional, centralized issuers like universities, governments, etc. VCs also differ since they do not specifically need to operate on a public blockchain. Hadrien Charlanes, founder of the SSI attestation project Sismo [26], mentioned: "VCs fit well with systems requiring off-chain operators, databases, and traditional actors." [27] They are perfect for use cases like "KYC, off-chain certificates and to bridge from Web2 to a blockchain native environment." [27] Instead, SBTs are crypto-native, fully operating as a data layer on the blockchain.

SBT standards can become new members of the already actively developing SSI tech stack. SBTs and VCs complement each other because of the data protection terminology. [21] SBTs are initially public, making them unsuitable for private data. On the contrary, VCs are used to sharing information unilaterally, making them unsuitable for joint social applications since they rely on some level of publicity and community. When sharing VCs, Souls cannot know that another one owns an SBT until that information is shared. Invisibility makes establishing a reputation, credible commitments, and visibly verifiable governance impossible. Secondly, it is almost impossible for an identity in a multiparty social relationship to have the unilateral right to disclose the relationship without the consent of the others. When two parties co-own an asset and choose to represent their relationship through a VC, such a credential does not enable mutual consent and permissions. This problem carries over to more complex cases in managing ownership and complex organizational forms such as DAOs and permissions, a feature of decentralized societies. [21]

The DID and VCs standards built on top of the current economy that deals with restrictions on private data are slowly seeing adoption. Ideas that take an approach by focusing on public data push development forward rapidly. [2] Here, SBTs and LSPs have the significant advantage of developing on a blue ocean for a data economy

that is yet to come. Various businesses outside the creative economy could adapt, expand or dock onto standards to make mainstream decentralized services a reality for the younger generation, whose most crucial skill is the exchange and finding of interests among each other that SBTs could soon enable.

9. Outlook

The path from the current web3 ecosystem to augmented sociality mediated by SBTs faces a classic adoption dilemma: SBTs encourage non-transferability and identity-specific approvals, but today's EOA wallets do not have proper backup schemes and risk losing their digital Soul. As the paper about decentralized societies stated, “In order for community recovery wallets to work, they need a wide variety of SBTs across discrete communities to be secure. What comes first: SBTs or strong social recovery?” [21]

This question of the SBT’s birth is the perfect starting point for contract-based accounts and the first set of LSPs [28] built beyond the ERC725 Proxy Account [7] standard. Here, communities can develop various key and backup schemes beyond a key manager without reissuing SBTs, as their Soul will only update its controller keys. Such contract-based Souls can also deliver much more convenience like permission handling, relayed transactions, or transfer approvals. Extended functionality would allow accounts to exist with solid onboarding, directly added claims, and recovery before more significant amounts of SBTs are handed out. Due to their integrated data storage, proper enclosures will further give more weight to who users are and less about what they have acquired. All this leads to safeguarding people and their assets without relying on 3rd parties.

Hybrid versions of SBTs could be another good starting point by giving communities time to build proper recovery before tokens are locked, further strengthening SBT issuing. But it has to be said that such management schemes still would have to be laid out and tested in the wild. For now, ideas are novel, and there is no commonly adopted flow regarding social media solutions.

Judging by all the community building happening in Web3, proper Soul frames and related SBTs could move the crypto scene from a generally money-oriented mindset into a more social space, giving people back not only power over their data and interactions but also placing focus on what truly matters: individuals and their genuine, unique relationships.

Acknowledgements

A sincere thank you to Rob Golden who assisted me in polishing this article and giving early feedback.

References

[1] Soulbound. (2022, January 26). Vitalik Buterin. Retrieved August 10, 2022, from https://vitalik.ca/general/2022/01/26/soulbound.html

[2] Hildebrandt, F. (2022, February 19). Identity Solutions for the Internet: Part 2 | KEEZdao. Medium. Retrieved August 10, 2022, from https://medium.com/keezdao/identity-solutions-for-the-internet-part-2-44aa1111b435

[3] Introduction. (n.d.). POAP. Retrieved August 10, 2022, from https://documentation.poap.tech/docs

[4] Hildebrandt, F. (2022b, March 5). LUKSO Ecosystem: Part 1 by Felix Hildebrandt | LUKSO. Medium. Retrieved August 10, 2022, from https://medium.com/lukso/lukso-ecosystem-part-1-4c3f5d67b081

[5] Proof Of Humanity. (n.d.). Proof Of Humanity. Retrieved August 10, 2022, from https://www.proofofhumanity.id/

[6] Hildebrandt, F. (2022c, March 5). LUKSO Ecosystem: Part 2 by Felix Hildebrandt | LUKSO. Medium. Retrieved August 10, 2022, from https://medium.com/lukso/lukso-ecosystem-part-2-fdc6abedf9dc

[7] Fabian Vogelsteller (n.d.). ERC: Proxy Account · Issue #725 · ethereum/EIPs. GitHub. https://github.com/ethereum/EIPs/issues/725

[8] Universal Profiles. (n.d.). LUKSO Universal Profile Explorer. Retrieved August 10, 2022, from https://universalprofile.cloud/

[9] LSP2 - ERC725Y JSON Schema | LUKSO Tech Documentation. (2022, June 15). LUKSO Tech Docs. Retrieved August 10, 2022, from https://docs.lukso.tech/standards/generic-standards/lsp2-json-schema/

[10] LSP3 - Universal Profile Metadata | LUKSO Tech Documentation. (2022, August 6). LUKSO Tech Docs. Retrieved August 10, 2022, from https://docs.lukso.tech/standards/universal-profile/lsp3-universal-profile-metadata/

[11] LSP6 - Key Manager | LUKSO Tech Documentation. (2022, August 2). LUKSO Tech Docs. Retrieved August 10, 2022, from https://docs.lukso.tech/standards/universal-profile/lsp6-key-manager/

[12] LSP1 - Universal Receiver | LUKSO Tech Documentation. (2022, April 28). LUKSO Tech Docs. Retrieved August 10, 2022, from https://docs.lukso.tech/standards/generic-standards/lsp1-universal-receiver/

[13] Lens Protocol. (n.d.). LENS Protocol. Retrieved August 10, 2022, from https://lens.xyz/

[14] LSP9Vault | LUKSO Tech Documentation. (2022, June 10). LUKSO Tech Docs. Retrieved August 10, 2022, from https://docs.lukso.tech/standards/smart-contracts/lsp9-vault/

[15] Adams, R. S. (n.d.). How to maximize your ENS domain. Ryan Sean Adams. Retrieved August 10,

2022, from https://newsletter.banklesshq.com/p/how-to-maximize-your-ens-domain?s=r
[16] Hildebrandt, F. (2022e, May 10). LUKSO Ecosystem: Part 3 by Felix Hildebrandt | LUKSO. Medium. Retrieved August 10, 2022, from https://medium.com/lukso/lukso-ecosystem-part-3-9af6bbcc24da
[17] LSP5 - Received Assets | LUKSO Tech Documentation. (2022, July 8). LUKSO Tech Docs. Retrieved August 10, 2022, from https://docs.lukso.tech/standards/universal-profile/lsp5-received-assets/
[18] LSP10 - Received Vaults | LUKSO Tech Documentation. (2022, July 8). LUKSO Tech Docs. Retrieved August 10, 2022, from https://docs.lukso.tech/standards/universal-profile/lsp10-received-vaults/
[19] Execute Transaction | LUKSO Tech Documentation. (2022, July 15). LUKSO Tech Docs. Retrieved August 10, 2022, from https://docs.lukso.tech/tools/relayer-api/execute-transaction/
[20] Why we need wide adoption of social recovery wallets. (2021, January 11). Vitalik Buterin. Retrieved August 10, 2022, from https://vitalik.ca/general/2021/01/11/recovery.html
[21] Weyl, G. E. (2022, May 10). Decentralized Society: Finding Web3's Soul. SSRN. Retrieved August 10, 2022, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4105763

[22] ERC725 Alliance. (n.d.). ERC725 Alliance. Retrieved August 10, 2022, from https://erc725alliance.org/
[23] Oskoboiny, G., Ran, R., & Jaffe, J. (n.d.). World Wide Web Consortium (W3C). W3C. Retrieved August 10, 2022, from https://www.w3.org/
[24] Decentralized Identifiers (DIDs) v1.0. (2022b, July 19). W3C. Retrieved August 10, 2022, from https://www.w3.org/TR/did-core/
[25] Verifiable Credentials Data Model v1.1. (2022, March 3). W3C. Retrieved August 10, 2022, from https://www.w3.org/TR/vc-data-model/
[26] Sismo - Curate your identities with privacy. (n.d.). Sismo. Retrieved August 10, 2022, from https://www.sismo.io/
[27] dhadrien.sismo.eth. (2022, May 27). Twitter. Retrieved August 10, 2022, from https://twitter.com/dhadrien_/status/1530171210121846787?t=Ly4yvOSI6pg30ng5CUskSw&s=19
[28] Introduction | LUKSO Tech Documentation. (2022, July 21). LUKSO Tech Docs. Retrieved August 10, 2022, from https://docs.lukso.tech/standards/introduction/

Digital Power of Attorney catalyzed by Software Requirements for Blockchain-based Applications

Arno Pfefferling, Theo Weigel
Hochschule Mittweida, Technikumplatz 17, 09648 Mittweida

Blockchain Technology (BT) with so-called web3 is at an inflection point between new sub-theme hypes and world-wide industrialization over last three years thanks to large companies like MicroStrategy [1], Facebook [2] and several Venture-Capital formations [3] who are already fighting over market share and community growth. Our work represents insights from Literature-based Software Requirement (SR) elicitation for a specific Blockchain-based Application, which is creation, managing and control of digital Power of Attorney (POA). The context of POA is not only a financial driven use-case it is by far a heavy weight universal legal transaction. We use a morphological box and reduced PRIMS-P to synthesis a generic specification for further Blockchain-based Application development. Formulated SRs in POA context are reflected on our core actors which are Grantor and authorized, trusted, external Entities. Proposed characteristics for relationship and effects are visualized in a reference model originally used in digital platform ecosystems [4]. This design and modelling approach facilitated closing discussion of BT and its future eCommerce perspective.

1. Introduction

Blockchain Technology (BT) and its applications are since 2016 more or less a hyped topic and described by several peer-reviewed technical as well as theoretical research contributions [5]. Financial applications are by far not the only solutions today, but they are according to Guo & Liang (2016) the ones with the greatest impact in terms of value streams and usage levels which makes BT interesting for sharing economy too, whereby the "innovative distributed ledger technologies such as for example the blockchain could support this with transparent recording and value exchange mechanisms among the involved actors" [7]. This quote is for our work the starting point to investigate how BT needs to be specified and which Software Requirements (SR) are consequences out of the involved real-world actors.

The chosen application scenario for value exchange is the topic of digital legacies, specifically digital services for the implementation and use of Powers of Attorney (POA). Digital value lays in the representation of various unilateral legal transactions and the scope of their actual release. Caruso (2018) points out that "modern unilateral contracts can expand the range of private autonomy and enable agreements that will generate net welfare gains". Generally, POA is within innovative firms already partly automated by so called Enterprise Legal Management (ELM) Software where arrangements of contracts and accounts for example in the event of death can be processed. ELM is "just as Enterprise Resource Planning has overhauled the finance function, so too there is promise that a foundational and integrated system of record can improve in-house legal operations and workflows" [9]. But POA is particularly helpful for private relatives, as important documents like living wills, bank statements and insurance documents are available and processed digitally. So, if the worst comes to the worst, the surviving dependents are relieved of stressful administrative tasks. Besides those promises processes in this context are very sensitive, since "involving incapable, isolated, institutionalized persons in research tries to prevent possible, albeit unintentional, exploitation of them as members of a vulnerable population." [10]. A machine or technical system can emotion-free transact this sensitive data, so that we anker BT with the described application context and want to catalyze technological benefits in real-world use-cases.

We follow the Research for Application-oriented contributions to uncover veritable properties of BT. According to the "Blockchain Research Framework" from Spohrer and Risius (2017) our approach can be seen as crucial prove for multidisciplinary statements. Furthermore, their prospective paradigmatic research questions:

"How do blockchain platforms differ regarding features and designs?

How can different blockchain systems complement each other to overcome individual constraints?

What are the technological interdependencies between different blockchain features (e.g., levels of permission and consensus mechanisms)?

How can the technical strengths of multiple public?"

are guiding our here proposed systematic literature review and conceptual design-oriented methodology in totality. After the introduction, this paper is explaining two core elements: 1) Smart Contract (SC) which is program code stored, processed, and used over BT – in other words SCs are acting as automated logic for the transactions on data; 2) Characteristics of BT under the context of POA – including a generic mapping of possible semantic objects. Followed by a detailed description of our applied Methodology and convicted Findings completed at

a discussion of our proposed SR. Those SR are elicited from explained source items and align with the goal to enhance the digital handling of POA, especially for Grantors, which are manifestation of our user-centric view.

2. Background and Foundations

The mystical emergence of Bitcoin has seen light over the recent years, so that the development steps and preconditions as well as the circumstances around Satoshi Nakamoto are more and more acknowledged [12]. Also, the Limitations in Bitcoin were addressed by a group led by avowed Viatlik Buterin [13] and resulted in founding the Ethereum Blockchain. The first practical applications have been implemented on the Ethereum Blockchain, starting in 2016, with the "Ethereum Request for Comments" (ERC) 20 and the standardized SC structure including the functionality to implement so-called Initial Coin Offerings, which allowed to access a global capital market direct in the creation step [14]. The combination of a distributed programmable logic on a ledger with the omnipresent need of market fit in an open innovative environment and the wide unregulated experimental setup have created application areas beyond cryptocurrencies. Academic literature defined features of distributed ledger technology are trust-free, transparent, and highly secure nature by decentralization [15]–[17].

Today, two applications are significantly present in the Ethereum eco-system. Firstly, the so-called Non-Fungible Tokens based on ERC 721, which are used to map ownership of digital or digitized values and goods, currently mainly for digital art and collectibles, as well as the entire complex of topics of so-called Decentralized Finance, which deals with the exchange and trade of decentralized values in the form of e.g., security or utility tokens [18]. SC-based decentralized exchanges such as: MDEX or Uniswap recorded a tremendous growth in sales in the process. Currently, the top 10 decentralized exchanges on Ethereum are turning over values of approximately $3 billion daily [19]. The examples of ERC 20 and ERC 721 token shows that Blockchain-based SC works and have entered a mainstream in regards of eCommerce, so that already new disruptive markets with enormous growth potential are realized [20].

In addition to these pioneering standardizations, new topics and industries are constantly being investigated regarding the use of BT by a crowd as audience and pilot applications aiming for new use-cases in being under dynamical development [21]. In supply chain management (proof of origin, tracking) and, most recently, in digital identities based on the principle of self-governance (self-sovereign identity) are particularly worth mentioning. Finally, we want to highlight that at Mittweida University of Applied Sciences other prototypes in use of BC are being investigated, such as: decentralized electronic voting, SC-automated insurance cases as well as authorization and signing of digital exam certificates. Following the archetype taxonomy from Weking et al. (2020) we have research steps in any application fields and this paper can be seen as practitioner contribution within Blockchain-based supply chains for data traceability, verification, reduction of redundancy on physical assets as a user-centric shared database for all members of the whole value chain. Involved actors in the value chain of POA are defined as the following: a) authorized Entity (in German "Bevollmächtigte"): has the right given by the Grantor to carry out a specified power for something in the real-world. This something can be a need of various actions or even state confirmations covered by a scope and underlying initial goal of the Grantor. Legal difficulty for interpretation of giving meaning to normative standards for SC is already addressed and noted [23]. To solve this interpretation, issue the authorized Entity must interact with an external Entity to achieve the execution of a specific point from a POA record. b) external Entity (in German "externe Dritte"): person or institution which validates the execution of the given POA scope and notifies all participants of a state change (e.g. "done"). c) The Grantor (in German "Vollmachtgeber"): person that creates and initially defines from himself goals for the POA. d) The Power of Attorney (in German "Vollmacht"): POA is a document or record that authorizes the holder to carry out specified power given by the Grantor. Holder in respect to digital objects means a state which is linked to one identified actor. e) trusted Entity (in German "Treuhänder"): person or institution which observes a POA dataset and knows about its validity by ensuring legal custody of a POA record. The single POA record itself is manifested by at least containing a signatory signature [24]. The core actor is the Grantor who need to have an initial goal and could name all involved actors or at least the trusted Entity to avoid fraud. Conflicts are disputed via Governance transactions as Trust building ankers within the BT system itself and reach a central design aspect as it is empirical suggested by Lewis et al. (2021).

For mapping the domain of POA with BC we defined characteristics in a morphological box, which is a creativity method for the systematic analysis of complex processes. According to [26] morphological analysis "is best suited for problems/systems of interest which cannot be adequately expressed using quantitative models and thus methods and software for mathematical optimization or simulation are nonapplicable (e.g. objective function and mathematical programming)". The domain under consideration of BT is broken down in a structured way to identify system components for which possible variants as Levels are defined (see Table 1).

The following tasks were conducted: 1) definition of characteristics (or attributes in case of physical objects) of existing components which have independence of each other, then 2) listing all cross-brainstormed expressions of respective characteristics to create a matrix in which every combination of theoretically possible values is aligned and 3) selected expression of the characteristics are chosen in each row, resulting in a minimized combination by intuitively consideration of holistically as solutions at a specific time. To get a systematic this

selection process was carried out several times and 4) new rows were iterated overall in four brainstorm sessions.

Characteristic	Level 1	Level 2	Level 3	Level 4	Level 5
Blockchain ecosystem [new - old]	Solana	IOTA	Hyperledger	Ethereum	Bitcoin
Blockchain privacy [low - high]	public	cloaked transactions	semi-permissioned	permissioned	
Blockchain dynamics [beneficial - mandatory]	popularity	lifetime	Quality of Service		
Jurisdiction [wide - narrow]	global	EU	Germany		
POA components [exact - fuzzy]	record	document	metadata	interfaces	participants
POA participants [sovereign - contractual]	Grantor	trusted Entity	authorized Entity	external Entity	
POA events [immediate – undefined]	create	validate	execute	unknown	
record storage [physical - unbound]	analog	digital local	network storage	cloud storage	distributed storage
record management [direct - undefined]	local	offline	online	distributed	gapped
record interaction [physical - unbound]	paper	in person	remote	automated	machine

Table 1: Morphological box to evaluate and classify selected source items during Screening phase.

The Level is a description of the variants for determined characteristic features. The benefit for our work by applying this creativity method was to limit the amount of source items of the SLR and leave focus for the synthesis of the SR specification. Relationship of uncertainty, vulnerability and trust are seen in the context of business processes [27]. Furthermore Müller et al. (2020) mentioned importance of reputation systems with Claims are defined as part of our core value-creation mechanism within eCommerce perspective.

3. Research Methodology

Fundamental starting point for our findings is a Systematic Literature Review (SLR) under applying the PRIMS-P flow. Terminology and scoping elements of PRIMS-P are not described in detail, since the content is repetitive to our paper structure and this work is not aimed to be fully compliant with PRISMA-P. No drawback is expected since our work is not intended to be health research [28], [29]. Between Mid of January to End of May 2022, data collection and a three staged analysis were completed (see Figure 1). To align the study and research direction, selected keywords were chosen the following "Blockchain" AND/OR "Power of Attorney". Search for data was done via google.scholar.com, aisel.aisnet.org, link.springer.com and ieeexplore.ieee.org. Data by identification of other online sources like blog, media, marketing posts are included as well. A manual forward/backward search based on identified source items was added [30]. Because BT in combination with POA is a completely new subject within Information Systems, only strong healthcare related items were strictly excluded to focus on the use of POA not the circumstances under those are triggered. For avoiding within-study bias [31] two persons from different backgrounds had to do the coding followed up by bi-weekly alignment meetings. We want to point out that the finding of a SR specification is the synthesized output of the SLR, which is adopting within the software engineering domain more and more [32].

3.1. Rationale and Objectives

Central object for rationale and derived objectives is the investigation of POA itself. Legally binding POA are informal in Germany, but they must fulfil certain requirements to be valid for a specific unilateral legal transaction. The already existing legal characteristics of POA are precisely defined and thus documented in the form of laws [33]. Classic POA in this sense are often notarized or certified, thus ensuring the integrity and validity of a POA. What is not clear, however, are the procedures and the application of these properties to a POA that is created, validated, and executed in a digital form only.

The legal and, in this context, technical BT interactions between the Entities involved are insufficiently explored. Since in ELM systems digital workflows and electronic documents are kind of used our research is trying to stay agile according to points of evidence-based decision making [34] – immutable and transparent BT can catalyze this due to its core functionality. Also the particular importance is the safeguarding of the interests of the participants in a POA [8], where in-built privacy from newer BT can strengthen the objective of POA. Based on

the legal properties of a POA, it can be assumed that it represents a series of conditional events (specified in the scope) that are triggered, validated and executed by different real-world Entities.

In conclusion the applied Jurisdiction defines the boundary conditions for the POA object itself and the SR frame must align with it. Transactions in relation to POA can be defined as legal services for challenging digital transformation of all spheres of life [35].

For BT as an object, we draw rationale mainly out of the funding source, because especially private funding-sources maybe profit-orientated for their own products [14], in that case, a source item is less legible.

Even if DAO and Community-oriented value streams were visible our objectives are on technical design and how software as a tool is used and finally realized. Business perspectives or consequences for technological decisions are subordinated. Argumentation is that we focus on goals and refinement process [36].

3.2. Eligibility Criteria and Evidence Collection

The Parameter during Identification and Screening steps are the following: Age of the source 2012 and above, Keywords evaluated with use of morphologic box Levels (see Table 1), type of source (academic paper/media post). We tried to stay in a general approach over specialized drilling. Meaning if there is a concept presented in a source item which works in more general context, that source will be preferred over specialized concepts. This was important so that specialized approaches do not influence the later implementation and avoid a foam of bias. The number of citations on source items just indicated relevant sources but did not make them standout for us.

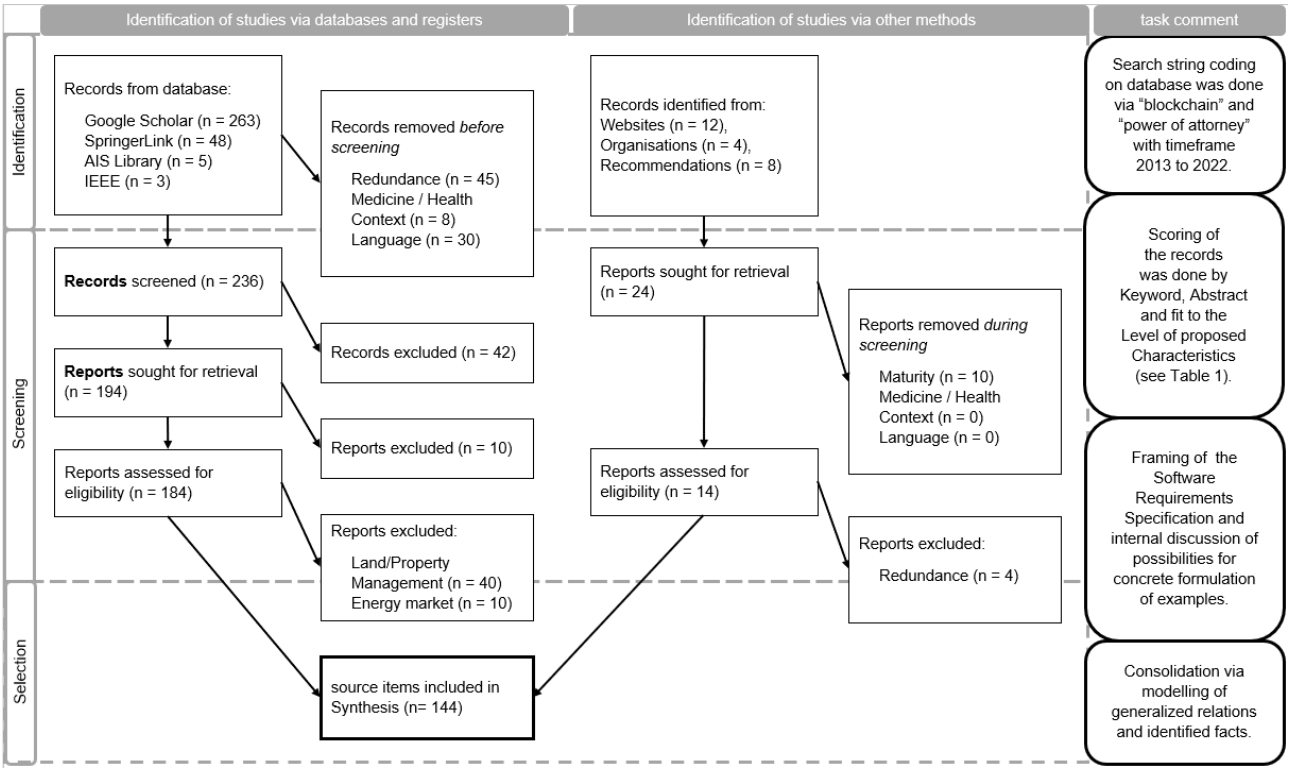

Figure 1: Three phase analysis of our SLR to synthesis SR for the Blockchain-based POA [37].

4. Results and Discussion

Our profound Findings are represented with the use of a SR specification template based on IEEE 830, ISO/IEC/IEEE 29148:{2011,2017} in combination with a goal-oriented requirements engineering [38] to build the best structure of fulfilling a widely usable specification within BT and the domain of POA. The underlying process model for the requirements engineering is adopted from [39] and starts with the application domain where system artifacts and source material represent the domain analysis – in our work completely gathered from the SLR. Developed prototypes and models were finally refined to the SR specification (see Figure 2).

Requirements itself are seen as a relation between form and context inside a system independent from the type of use like decision-support or knowledge systems are representing [40]. This independency from the type of use is in our view positive since also activities associated with requirements engineering vary widely depending on established practices of public as well as private organizations. These are sometimes presented as chronological phases considerable intertwining of real-world practical activities [41].

4.1. Synthesis of Requirements

Scope for handling digital POA were to allow users: A) Creation, validation and management of POA datasets consisting of POA records and its metadata; B) Write integrity information of POA datasets anchored per BT; C) user management with role-based privileges; D) interactions with POA records can be backtracked. Based on scope A-D we aligned the system goals and defined raw technical requirements to map those to building blocks in the reference model (see Figure 2). In addition to Hein et al. (2020) proposed value-co creation and the boundary resources of well- and ill-structured characteristic – we modified and added from the core value-creation mechanism outwards BT as catalyzer for more general representation of eCommerce platforms, were Consumer stays, but context is given by POA objects and Jurisdiction is the main inward directed effect for Boundaries.

As in between overview we want to establish a service architecture with persistence, storage, blockchain and notification layer all combined in a gateway on top of a central web user interface [42]. On this interface three pages (application root, stakeholder view of existing records and specific validated datasets) are defined as SR. A more detailed list of our defined SR is given under https://aizr1.github.io/spoa/ whereby the actual definition can vary according to the use-case. Example is the relation of a technical backend structure to end-devices for signing on the distributed ledger and a necessary onboarding procedures with focus on identification [43]

4.2. Product Overview Perspective, Functions and Constraints

The value stream is the interaction of POA with BT going through value-creating mechanism triggered by Innovation which comes from the Consumers itself since each POA scope and reasoning comes from Grantors itself. This loop-in-loop relation is a core functional SR like user management with account and resource assignment, storage management with record access and validation management with integrity mapping for POA datasets. Outcome is the major goal 1) to secure the Grantor's interests of a POA by enabling Entities to validate its integrity, contents and history of interaction fully digitally. 2) enforced default that Entities use disclosed context and avoid green-washing policies [44].

In detail, a user can create or interact with a POA dataset and enter metadata (e.g., names of participants, execution, or termination dates). This dataset will be cryptographically signed and stored securely in a versioned object storage. The system will take the cryptographic data and store it on BT using on-chain transactions. A trusted or external Entity is now enabled to validate the POAs integrity, contents, and history of interaction digitally. This brings us to goal 2) where processes that require POA need to be more secure, by providing a purpose-built system using the auditing capabilities and tamper-proof properties like BT but realized in an Event-driven architecture since the system achieves to handle various heterogenies legal content, such as POA record information with private user data, local data or other content which falls under privacy protection laws.

Another feature or required constraints is the integrable of an existing cloud environment to maximize scalability of the whole system [45]. If a feature requires non-standard protocols or software, it might constrain the overall system and should be excluded.

4.3. User Characteristics, Assumptions and Dependencies

Central objects are POA datasets, which are digital representation of documents or records that authorizes the holder to carry out a specified power given by the Grantor. The digital representation is allowing and enforcing "smart regulation by conditions to nudge individuals" [46] so that object-based value-creating mechanism is depending on a user-centric view. Integrity of information about the power and scope are cryptographically verifiable data of POA record, which is created automatically to every active dataset. A dataset in short is a collection of POA records, metadata, and additional information. According to Hegadekatti (2017) main task is a Proof for the existence of documents. We tackle this by POA records which can be linked to any file (e.g. PDF, Video, Audio), containing the actual POA legacy as created and initial scoped by the Grantor. Such a record has defined and maybe changing participants by a SC without negotiation [48]. A user is a representation of a real-world person and can assume various roles based on the type of interaction with a POA record. Assumption in the synthesis is the dependency of specific BT implementations since very different maturity degrees and characteristics were noticed. Furthermore, the many different BT on the market show lack of evidence-based realization of use-cases. Most fitting source items use SC in production usage.

4.4. Quality of Service

The Quality of Service (QoS) refers to the quality of a communication service from the user point of view. Since our users are the Consumer itself we set security general as goal 3) and resulting SR that central parts of the system will be written in Rust, which was developed to eliminate classes of critical bugs, while being performant [49]. For traffic definition any connection between services must be encrypted, regardless of the underlying network architecture as well as a reverse-proxy which should take care of SSL Termination instead of the backend itself. For storage in general any data stored or buffered must be encrypted. Regarding authentication no personal identifiable information is stored on any browser persistence [50], [51].

For reliability, the SR of automated testing in critical part and shall ensure basic functionality as well as integration of coded services added by manual testing of all user actions shall ensure correct end-functionality. Specifically

SC have a need by inter-SC communication operation that can pave the way for several coding irregularities like reentrancy, denial of service, mishandled exception [52]. Additional we see auditing of the system design, which aims to trace every interaction of POA datasets. Audit logs shall be written to a tamper-proof, historically verifiable system (e.g. again Event-based architecture or BT).

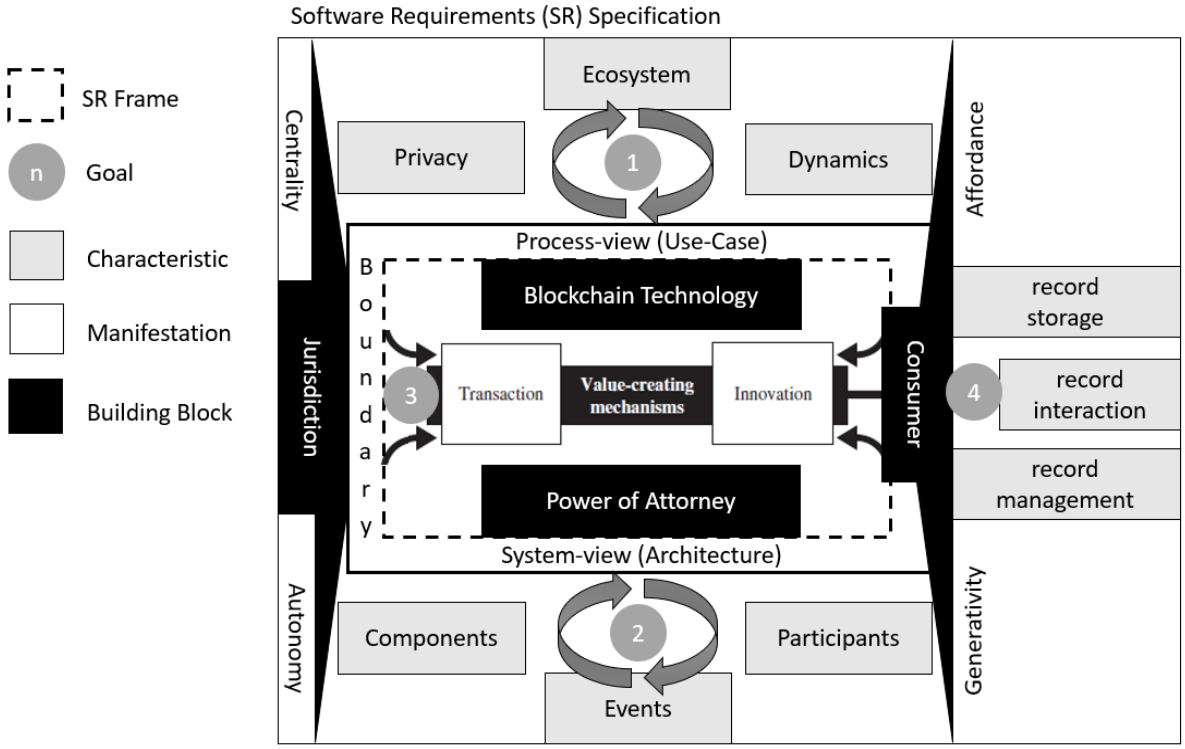

Figure 2: Visualization of our proposed SR specification with core element adapted by Hein et al. [53].

This means our resulting design is not excluding a combination of two or more Blockchain solutions, which can be declared as a strength [11]. Paik et al. (2019) analysis shows a "unique design of the ledger structure, network, consensus protocol and cryptographic mechanisms it uses", so that single Blockchain solutions definitely have benefits against their competitors and a combination of those is a win-win for eCommerce position. System as well as user configuration is externalized in files to ensure full modularity. For the user aka Consumer we propose goal 4) by end-device flexibility and inbuild authentication over SC. These are confirmed suggestions in practical studies [14], [55].

5. Conclusion and Outlook

In summary our work presents a design and model for software engineering domain in building Blockchain-based Application on the context of digital POA. The design and model are a SR specification which uses a SLR and morphological box to synthesis a structure of relations by Process- and System-view. The generosity of our SR specification was one modeling aspect so that our approach can be adjusted for other use-cases. This is important since SC security shows domain specific invoking methods [52]. SC Security stretches over the whole BT system since SC have vulnerabilities in the process of development, deployment as well as interaction [56].

Affordance represents a high market need like an industry must-have versus Generativity a market portability as easy to use system to work with from Consumer view. On the contrary Centrality stands for the degree of decentralization versus Autonomy as gauge for self-sovereign POA from Jurisdiction view. Characteristics of Building Blocks are unordered triad for the goals and development stage independent orientation of agile sprint planning. Future research could be done in building a framework to define SR dynamically within the triad.

5.1. Limitations

Our current work and research project future are oriented mainly for German Jurisdiction so that some thoughts might not fit to other more restriction-less regions and we lose the benefit of "develop suitable legal frameworks to cope with the upsurge and hefty volume of online transactions" [57]. Still, if we look at the electronic transactions it can be noted that we are very close to the eIDAS regulations [58] and a shift for our SR specification to European Jurisdiction is very well possible. For more comprehensive formulation of SR our work can be extended by other research methods like semi-structured interviews to e.g. reveal more details of accounting practice [59]. Also, the SLR is not trying to propose new research questions neither an unknown gap, but it is at least in our understanding a practical tool to define a specification systematic by use-case depending

on SR. As soon as the research community has more increments of technical Blockchain-based Applications further understanding of the "trade-off between system usability and values" can be investigated [60]. Our work is in this view tightened to more practical research than theory.

Acknowledgements

Special thanks to the German Research Foundation who supplied financial the WIR! showcase region Mittweida and us as the smartPOA sub-project (FKZ: 03WIR1317B). Furthermore, we are grateful for our industry partner Memoresa GmbH and their practical experienced software engineers who always had a sympathetic ear.

References

[1] N. Kessler, "MicroStrategy kauft den Dip – so viele Bitcoins waren es diesmal," Apr. 22, 2022. https://www.deraktionaer.de/artikel/aktien/microstrategy-kauft-den-dip-so-viele-bitcoins-waren-es-diesmal-20248591.html (accessed May 08, 2022).

[2] E. Kühl, "Facebook-Kryptowährung: Kapp den Diem!," *Die Zeit*, Hamburg, Jan. 28, 2022. Accessed: May 08, 2022. [Online]. Available: https://www.zeit.de/digital/internet/2022-01/facebook-kryptowaehrung-diem-libra-aus

[3] R. Rai, "An Overview Of Web3 Venture Capital Activity In 2021," Jan. 02, 2022. https://www.forbes.com/sites/rahulrai/2022/01/02/an-overview-of-web3-venture-capital-activity-in-2021/ (accessed May 08, 2022).

[4] A. Hein *et al.*, "Digital platform ecosystems," *Electron Markets*, vol. 30, no. 1, pp. 87–98, Mar. 2020, doi: 10.1007/s12525-019-00377-4.

[5] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where Is Current Research on Blockchain Technology?—A Systematic Review," *PLoS ONE*, vol. 11, no. 10, p. e0163477, Oct. 2016, doi: 10.1371/journal.pone.0163477.

[6] Y. Guo and C. Liang, "Blockchain application and outlook in the banking industry," *Financ Innov*, vol. 2, no. 1, p. 24, Dec. 2016, doi: 10.1186/s40854-016-0034-9.

[7] T. Puschmann and R. Alt, "Sharing Economy," *Bus Inf Syst Eng*, vol. 58, no. 1, pp. 93–99, Feb. 2016, doi: 10.1007/s12599-015-0420-2.

[8] D. Caruso, "Then and Now: Mark Pettit's Modern Unilateral Contracts in the 1980s and in the Age of Blockchains," *B.U. L. Rev.*, vol. 98, p. 1789, 2018.

[9] R. van der Meulen, "Gartner Insights," *4 Key Trends in the Gartner Hype Cycle for Legal and Compliance Technologies, 2020*, Sep. 21, 2020. https://www.gartner.com/smarterwithgartner/4-key-trends-in-the-gartner-hype-cycle-for-legal-and-compliance-technologies-2020 (accessed Apr. 15, 2022).

[10] A. M. Heesters, D. Z. Buchman, K. W. Anstey, J. A. H. Bell, B. J. Russell, and L. Wright, "Power of Attorney for Research: The Need for a Clear Legal Mechanism," *Public Health Ethics*, vol. 10, no. 1, pp. 100–104, 2017.

[11] M. Risius and K. Spohrer, "A Blockchain Research Framework: What We (don't) Know, Where We Go from Here, and How We Will Get There," *Bus Inf Syst Eng*, vol. 59, no. 6, pp. 385–409, Dec. 2017, doi: 10.1007/s12599-017-0506-0.

[12] U. W. Chohan, "A History of Bitcoin," *SSRN Journal*, Feb. 2022, doi: 10.2139/ssrn.3047875.

[13] V. Buterin, "A NEXT GENERATION SMART CONTRACT & DECENTRALIZED APPLICATION PLATFORM," Ethereum Foundation, 2015. [Online]. Available: https://blockchain-lab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf

[14] K. Lauslahti, J. Mattila, T. Hukkinen, and T. Seppälä, "Expanding the Platform: Smart Contracts as Boundary Resources," in *Collaborative Value Co-creation in the Platform Economy*, A. Smedlund, A. Lindblom, and L. Mitronen, Eds. Singapore: Springer, 2018, pp. 65–90. doi: 10.1007/978-981-10-8956-5_4.

[15] R. Beck, J. S. Czepluch, N. Lollike, and S. Malone, "BLOCKCHAIN – THE GATEWAY TO TRUST-FREE CRYPTOGRAPHIC TRANSACTIONS," *Research Papers*, May 2016, [Online]. Available: https://aisel.aisnet.org/ecis2016_rp/153

[16] M. Marchesi, L. Marchesi, and R. Tonelli, "An Agile Software Engineering Method to Design Blockchain Applications," *CEE-SECR '18*, 2018, doi: 10.1145/3290621.3290627.

[17] T. Rathee and P. Singh, "A systematic literature mapping on secure identity management using blockchain technology," *Journal of King Saud University - Computer and Information Sciences*, p. S1319157821000690, Mar. 2021, doi: 10.1016/j.jksuci.2021.03.005.

[18] A. Miglo, "STO vs. ICO: A Theory of Token Issues under Moral Hazard and Demand Uncertainty," *Journal of Risk and Financial Management*, vol. 14, no. 6, Art. no. 6, Jun. 2021, doi: 10.3390/jrfm14060232.

[19] Binance Capital, "CoinMarketCap," *Die Rangliste der besten dezentralen Kryptowährungsbörsen*, May 01, 2022. https://coinmarketcap.com/de/rankings/exchanges/dex/ (accessed May 01, 2022).

[20] K. P. Jørgensen and R. Beck, "Universal Wallets," *Bus Inf Syst Eng*, vol. 64, no. 1, pp. 115–125, Feb. 2022, doi: 10.1007/s12599-021-00736-6.

[21] J. Weking, M. Stöcker, M. Kowalkiewicz, M. Böhm, and H. Krcmar, "Archetypes for Industry 4.0 Business Model Innovations," presented at the StrategicIT, Hyatt Regency New Orleans, Aug. 16, 2018. Accessed: May 25, 2022. [Online]. Available: https://aisel.aisnet.org/amcis2018/StrategicIT/Presentations/3/

[22] J. Weking, M. Mandalenakis, A. Hein, S. Hermes, M.

Böhm, and H. Krcmar, "The impact of blockchain technology on business models – a taxonomy and archetypal patterns," *Electron Markets*, vol. 30, no. 2, pp. 285–305, Jun. 2020, doi: 10.1007/s12525-019-00386-3.

[23] M. Giancaspro, "Is a 'smart contract' really a smart idea? Insights from a legal perspective," *Computer Law & Security Review*, vol. 33, no. 6, pp. 825–835, Dec. 2017, doi: 10.1016/j.clsr.2017.05.007.

[24] S. Vattaparambil Sudarsan, O. Schelén, and U. Bodin, "A Model for Signatories in Cyber-Physical Systems," in *2020 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, Sep. 2020, vol. 1, pp. 15–21. doi: 10.1109/ETFA46521.2020.9212081.

[25] S. Leewis, K. Smit, and J. van Meerten, "An Explorative Dive into Decision Rights and Governance of Blockchain: A Literature Review and Empirical Study," *Pacific Asia Journal of the Association for Information Systems*, vol. 13, no. 3, Sep. 2021, doi: 10.17705/1pais.13302.

[26] M. Zec, A. Schneider, and F. Matthes, "Towards a Process Model for Computer-Supported Collaborative Morphological Analysis," *AMCIS 2015 Proceedings*, Jun. 2015, [Online]. Available: https://aisel.aisnet.org/amcis2015/SystemsAnalysis/GeneralPresentations/9

[27] M. Müller, N. Ostern, and M. Rosemann, "Silver Bullet for All Trust Issues? Blockchain-Based Trust Patterns for Collaborative Business Processes," in *Business Process Management: Blockchain and Robotic Process Automation Forum*, vol. 393, A. Asatiani, J. M. García, N. Helander, A. Jiménez-Ramírez, A. Koschmider, J. Mendling, G. Meroni, and H. A. Reijers, Eds. Cham: Springer International Publishing, 2020, pp. 3–18. doi: 10.1007/978-3-030-58779-6_1.

[28] PRISMA-P Group *et al.*, "Preferred reporting items for systematic review and meta-analysis protocols (PRISMA-P) 2015 statement," *Syst Rev*, vol. 4, no. 1, p. 1, Dec. 2015, doi: 10.1186/2046-4053-4-1.

[29] L. Shamseer *et al.*, "Preferred reporting items for systematic review and meta-analysis protocols (PRISMA-P) 2015: elaboration and explanation," *BMJ*, vol. 349, no. jan02 1, pp. g7647–g7647, Jan. 2015, doi: 10.1136/bmj.g7647.

[30] J. Webster and R. T. Watson, "Analyzing the Past to Prepare for the Future: Writing a Literature Review," *MIS Quarterly*, vol. 26, no. 2, pp. xiii–xxiii, 2002.

[31] C. F. Durach, J. Kembro, and A. Wieland, "A New Paradigm for Systematic Literature Reviews in Supply Chain Management," *J Supply Chain Manag*, vol. 53, no. 4, pp. 67–85, Oct. 2017, doi: 10.1111/jscm.12145.

[32] P. Brereton, B. A. Kitchenham, D. Budgen, M. Turner, and M. Khalil, "Lessons from applying the systematic literature review process within the software engineering domain," *Journal of Systems and Software*, vol. 80, no. 4, pp. 571–583, Apr. 2007, doi: 10.1016/j.jss.2006.07.009.

[33] M. J. Pettit, "Modern Unilateral Contracts," *B.U. L. Rev.*, vol. 63, p. 551, 1983.

[34] M. Milkovich, J. A. Nicholson, and D. B. Nicholson, "Applied Learning of Emerging Technology: Using Business-Relevant Examples of Blockchain," *Journal of Information Systems Education*, vol. 31, no. 3, p. 187, Sep. 2020.

[35] Y. A. Tymchuk and A. V. Shkalenko, "Analysis of the Impact of Robotic Legal Services on the Changing Institutional Environment of Economy and Law," in *"Smart Technologies" for Society, State and Economy*, Cham, 2021, pp. 1146–1158. doi: 10.1007/978-3-030-59126-7_125.

[36] D. Alrajeh, A. Cailliau, and A. van Lamsweerde, "Adapting Requirements Models to Varying Environments," in *2020 IEEE/ACM 42nd International Conference on Software Engineering (ICSE)*, Oct. 2020, pp. 50–61. doi: 10.1145/3377811.3380927.

[37] M. J. Page *et al.*, "The PRISMA 2020 statement: an updated guideline for reporting systematic reviews," *BMJ*, p. n71, Mar. 2021, doi: 10.1136/bmj.n71.

[38] A. van Lamsweerde, "Goal-oriented requirements engineering: a guided tour," in *Proceedings Fifth IEEE International Symposium on Requirements Engineering*, Aug. 2001, pp. 249–262. doi: 10.1109/ISRE.2001.948567.

[39] H. F. Hofmann and F. Lehner, "Requirements engineering as a success factor in software projects," *IEEE Software*, vol. 18, no. 4, pp. 58–66, Jul. 2001, doi: 10.1109/MS.2001.936219.

[40] H. F. Hofmann, *Requirements Engineering: A Situated Discovery Process*. Springer-Verlag, 2013.

[41] Jay, "The Hardest thing about Engineering is Requirements," Mar. 03, 2022. https://jaybs.medium.com/the-hardest-thing-about-engineering-is-requirements-28a6a70c4db4 (accessed Mar. 14, 2022).

[42] J. Lockl, V. Schlatt, A. Schweizer, N. Urbach, and N. Harth, "Toward Trust in Internet of Things Ecosystems: Design Principles for Blockchain-Based IoT Applications," *IEEE Trans. Eng. Manage.*, vol. 67, no. 4, pp. 1256–1270, Nov. 2020, doi: 10.1109/TEM.2020.2978014.

[43] C. Klikovits, P. Abraham, and R. Rambacher, "A Framework to identify People, Devices and Services in Cyber-physical system of systems," in *2021 IFIP/IEEE International Symposium on Integrated Network Management (IM)*, May 2021, pp. 914–919.

[44] M. Bellucci, D. C. Bianchi, and G. Manetti, "Blockchain in accounting practice and research: systematic literature review," *Meditari Accountancy Research*, 2022, doi: 10.1108/medar-10-2021-1477.

[45] D. Li, L. Deng, Z. Cai, and A. Souri, "Blockchain as a service models in the Internet of Things management: Systematic review," *Transactions on Emerging Telecommunications Technologies*, vol. 33, no. 4, p. e4139, 2022, doi: 10.1002/ett.4139.

[46] M. Yu. Kozlova, "Accessibility of Register Information as an Element of Smart Regulation of Entrepreneurial Relations in the Digital Society," in *Towards an Increased Security: Green Innovations, Intellectual Property Protection and Information Security*, Cham, 2022, pp. 387–396. doi: 10.1007/978-3-030-93155-1_43.

[47] K. Hegadekatti, "Legal Systems and Blockchain Interactions," Social Science Research Network, Rochester, NY, SSRN Scholarly Paper 2893128, Feb. 2017. doi: 10.2139/ssrn.2893128.

[48] S. Williams, "Smart Contracts don't negate Power of Attorney or the need for one.," Apr. 11, 2019. https://www.linkedin.com/pulse/smart-contracts-dont-negate-power-attorney-need-one-samson-williams (accessed May 08, 2022).

[49] J. Goulding, "What is Rust and why is it so popular?," *Stack Overflow*, Jan. 20, 2020. https://stackoverflow.blog/2020/01/20/what-is-rust-and-why-is-it-so-popular/ (accessed Mar. 16, 2022).

[50] A. Hindle, "Impact of GDPR on Identity and Access Management," *IDPro Body of Knowledge*, vol. 1, no. 1, Art. no. 1, Mar. 2020, doi: 10.55621/idpro.24.

[51] S. Schwerin, "Blockchain and Privacy Protection in the Case of the European General Data Protection Regulation (GDPR): A Delphi Study," *The JBBA*, vol. 1, no. 1, pp. 1–77, Jul. 2018, doi: 10.31585/jbba-1-1-(4)2018.

[52] Z. A. Khan and A. S. Namin, "A Survey on Vulnerabilities of Ethereum Smart Contracts," arXiv, arXiv:2012.14481, Dec. 2020. doi: 10.48550/arXiv.2012.14481.

[53] A. Hein, J. Weking, M. Schreieck, M. Wiesche, M. Böhm, and H. Krcmar, "Value co-creation practices in business-to-business platform ecosystems," *Electron Markets*, vol. 29, no. 3, pp. 503–518, Sep. 2019, doi: 10.1007/s12525-019-00337-y.

[54] H.-Y. Paik, X. Xu, H. M. N. D. Bandara, S. U. Lee, and S. K. Lo, "Analysis of Data Management in Blockchain-Based Systems: From Architecture to Governance," *IEEE Access*, vol. 7, pp. 186091–186107, 2019, doi: 10.1109/ACCESS.2019.2961404.

[55] A. Bogner, M. Chanson, and A. Meeuw, "A Decentralised Sharing App running a Smart Contract on the Ethereum Blockchain," in *Proceedings of the 6th International Conference on the Internet of Things*, New York, NY, USA, Nov. 2016, pp. 177–178. doi: 10.1145/2991561.2998465.

[56] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," *Future Generation Computer Systems*, vol. 107, pp. 841–853, Jun. 2020, doi: 10.1016/j.future.2017.08.020.

[57] W. C. Iheme, "A Comparative Assessment of the Legal Frameworks on Cross-Border Consumer Disputes," in *The Indian Yearbook of Comparative Law 2019*, M. John, V. H. Devaiah, P. Baruah, M. Tundawala, and N. Kumar, Eds. Singapore: Springer, 2021, pp. 61–93. doi: 10.1007/978-981-16-2175-8_4.

[58] T. Vogt, "Die neue eIDAS-Verordnung – Chance und Herausforderung für die öffentliche Verwaltung in Deutschland," *Information - Wissenschaft & Praxis*, vol. 67, no. 1, pp. 61–68, Feb. 2016, doi: 10.1515/iwp-2016-0011.

[59] R. Esmander, P. Lafourcade, M. Lombard-Platet, and C. Negri-Ribalta, "A silver bullet?: a comparison of accountants and developers mental models in the raise of blockchain," in *Proceedings of the 15th International Conference on Availability, Reliability and Security*, Virtual Event Ireland, Aug. 2020, pp. 1–10. doi: 10.1145/3407023.3409193.

[60] K. Cousins, H. Subramanian, and P. Esmaeilzadeh, "A Value-sensitive Design Perspective of Cryptocurrencies: A Research Agenda," *CAIS*, pp. 511–547, 2019, doi: 10.17705/1CAIS.04527.

Vergleichende Analyse von dezentralen Börsen und dem traditionellen Wertpapierhandel

Maximilian Heimbrock

Anhand von verschiedenen Vergleichskriterien werden in diesem Beitrag dezentrale Börsen mit dem traditionellen Wertpapierhandel verglichen. Der Text basiert auf der Bachelorarbeit des Autors, die im Wintersemester 2022/23 an der Heinrich-Heine-Universität Düsseldorf geschrieben wurde.
Im Laufe des hier vorgelegten Beitrags werden die Funktionsweisen der Börsen erläutert. Daraufhin werden die Vergleichskriterien in einer verkürzten Schlagwort-Tabelle aufgelistet. Abschließend werden die Chancen und Risiken dezentraler Börsen gegenüber traditionellen Börsen herausgestellt.

1. Einleitung

Zur Einordnung des Themas werden im Folgenden die für diesen Beitrag maßgebenden Definitionen von „Dezentrale Börse" und „traditioneller Wertpapierhandel" genannt. Zum heutigen Stand gibt es keine einheitliche Definition einer Dex.

Dezentrale Börse

In diesem Beitrag wird unter einer Dezentralen Börse (Dex) ein digitaler Handelsplatz für Vermögenswerte auf Basis der Blockchain-Technologie verstanden, der den Handel von Vermögenswerten ohne Zwischenhändler ermöglicht.

Traditioneller Wertpapierhandel

Als traditioneller Wertpapierhandel wird in diesem Beitrag der Handel mit Vermögenswerten verstanden, bei dem sich der Handelsteilnehmer eines oder mehrerer Zwischenhändler bedient.

Organisationsstruktur

Eine Dex ist ein Computerprogramm auf einer Blockchain[1], eine Anwendung im DeFi-Sektor und ist als eine Dezentrale Autonome Organisation (engl.: Decentralized Autonomous Organization, kurz DAO) konstruiert.

Eine DAO existiert digital und mit Hilfe von Smart Contracts[2] auf einer Blockchain. [31] Sie wird nicht von einer oder ein paar wenigen einzelnen Entitäten gesteuert, sondern agiert automatisiert auf Basis ihres Programmcodes. Änderungen an dem Programmcode können von jedem Stakeholder vorgeschlagen werden. [28] Über die Änderungsvorschläge wird anschließend auf der Blockchain (im Folgenden auch als On-Chain bezeichnet) mithilfe des Gouvernance-Tokens[3] der DAO abgestimmt. [31]

Der Handelsteilnehmer interagiert direkt über die Blockchain mit der Dex, ohne Zwischenhändler zu nutzen. [37] Als grafische Benutzeroberfläche kann dafür ein Webinterface genutzt werden. [50] Die Verwahrung der Vermögenswerte erfolgt auf der privaten Wallet (deutsch: Geldbörse)[4] des Handelsteilnehmer. [37]

Beim traditionellen Wertpapierhandel bedient sich der Nutzer eines oder mehrerer Zwischenhändler(s) (auch als Intermediäre bezeichnet), um eine Transaktion durchzuführen. Dabei erteilt der Kunde einem Intermediär den Auftrag, in seinem Namen einen Vermögenswert zu erwerben bzw. zu verkaufen. Für die Transaktion dient eine Börse als Marktplatz. Anschließend werden weitere Intermediäre beauftragt, die Transaktion abzuwickeln.

Die Intermediäre übernehmen dabei verschiedene Aufgaben wie z. B. die Verwahrung der Vermögenswerte. [45] Bspw. verwahrt die blocknox GmbH die Vermögenswerte der Kunden, die über die Bison-App oder die Digital Exchange der Börse Stuttgart handeln. [9] Bei dem Handel mit Kryptowährungen kann der Nutzer ei-

1 Eine Blockchain ist eine fälschungssichere, verteilte Datenstruktur, in der Transaktionen in der Zeitfolge protokolliert, öffentlich nachvollziehbar, unveränderlich und ohne zentrale Instanz abgebildet werden. Für eine weitergehende Erläuterung siehe Klitzsch (2019), S. 159–163.

2 Ein Smart Contract ist ein Computerprogramm auf Basis der Blockchain-Technologie. Das Programm folgt einer WENN-DANN-Logik, sodass, sobald ein zuvor festgelegter Auslöser eintritt, eine ebenfalls zuvor festgelegte Folgereaktion ausgelöst wird. Die Folgereaktion ist genauso wie der Auslöser im Programmcode des Smart Contracts mit Hilfe der Blockchain-Technologie transparent und fälschungssicher hinterlegt. Für eine weitergehende Erläuterung siehe Popescu (2020), S. 42–43.

3 Ein Gouvernance-Token ist ein Token, der ein Stimmrecht repräsentiert. Aus Gründen des Umfangs wird nicht weiter auf den Gouvernance-Token eingegangen. Für weitere Informationen dazu siehe z. B. Hsieh et al. (2018), S. 8.

4 Eine Wallet dient der Aufbewahrung der Private Keys für Kryptowährung. Auch wenn in der Wallet nur der Zugriff auf die Vermögenswerte und nicht die Vermögenswerte selbst aufbewahrt werden, wird im Folgenden aus Vereinfachungsgründen davon ausgegangen, dass die Vermögenswerte in der Wallet aufbewahrt werden. Für weitere Informationen dazu siehe z. B. Antonopoulos (2018), S. 95–118.

ner traditionellen Börse entscheiden, ob er die Vermögenswerte einem Intermediär zur Verwahrung überträgt oder nach dem Handel auf seine private Wallet überträgt. Wenn er sich dafür entscheidet, die Vermögenswerte vom Intermediär verwahren zu lassen, besitzt der Intermediär die Private Keys (deutsch: Private Schlüssel)[5] für die Vermögenswerte. [14]

Market-Making

Im folgenden Abschnitt werden die beiden Mechanismen, die von Börsen für das Market-Making verwendet werden, [2] grundlegend erläutert. Eine Börse bedient sich entweder eines Automated Market Maker (kurz: AMM) oder eines Orderbuchs.

AMM:

Bei einem AMM handelt es sich um einen Smart Contract, der den Tausch von zwei Vermögenswerten ermöglicht.[6] Im Gegensatz zum Orderbuch, handelt der Nutzer eines solchen AMM nicht mit einem anderen Handelsteilnehmer der Börse, sondern mit einem Liquidity Pool (siehe Abbildung 2). [26]

Ein Liquidity Pool ist der Liquiditätsvorrat einer Dex. Für jedes Tauschpaar an Vermögenswerten, die an der Dex gehandelt werden, existiert ein Liquidity Pool, in dem Liquidität der beiden jeweiligen Vermögenswerte vorhanden ist. [54] Wenn ein Nutzer Token einer Kryptowährung erhalten möchte, muss er im Gegenzug Token der anderen Kryptowährung dem Pool hinzufügen.

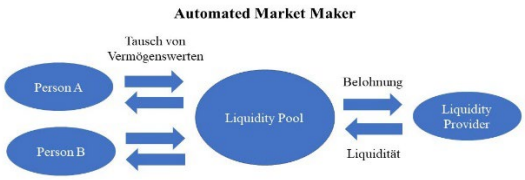

Abbildung 1: Funktionsweise eines Automated Market Makers (AMM)

Quelle: eigene Darstellung

Um den Preis der gewünschten Kryptowährung, und damit der Anzahl an Token, die der Nutzer von der anderen Kryptowährung dem Pool hinzufügen muss, zu bestimmen, nutzt der AMM einen sog. Constant Product Market Maker.[7] Dieser basiert auf der Formel: x * y = k. Dabei stehen x und y für die Preise der beiden Vermögenswerte im Pool. Die Variable k bleibt konstant und verändert sich nicht. Daraus ergibt sich, dass wenn der Preis eines Vermögenswerts durch eine erhöhte Nachfrage steigt, gleichzeitig der Preis des anderen Werts exponentiell fällt. Als Ergebnis muss der Handelsteilnehmer umso mehr von einem Vermögenswert eintauschen, desto weniger von dem anderen Vermögenswert im Pool vorhanden ist (siehe Abbildung 3).[8]

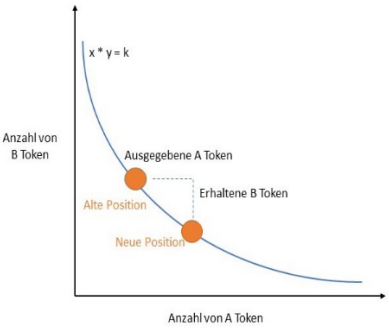

Abbildung 2: Darstellung eines Constant Product Market Maker

Quelle: eigene Darstellung, in Anlehnung an z. B. Mohan (2020) S. 19

Ein Preisunterschied zu anderen Börsen, unabhängig davon, ob es sich dabei um Dex's oder traditionelle Börsen handelt, löst Arbitragegeschäfte aus, durch die die Preise wieder angeglichen werden. [43] Dabei verändern die Arbitragegeschäfte das Mengenverhältnis der Vermögenswerte in dem Liquidity Pool der Dex, sodass der Preis an der Dex mit dem Preis an den anderen Börsen übereinstimmt. [35]; [33]

Orderbuch:

In einem Orderbuch tragen die Käufer und Verkäufer den Preis ein, zu dem sie bereit sind, eine gewünschte Menge des Wertpapiers zu handeln, während die Börse als Intermediär zwischen den beiden Handelsteilnehmern vermittelt. (Siehe Abbildung 4) Dafür führt die Börse für jedes Wertpapier ein eigenes Orderbuch. [8] Wenn das Angebot eines Verkäufers mit dem eines Käufers übereinstimmt, wird die Transaktion ausgeführt und die beiden Positionen aus dem Orderbuch entfernt.

5 Die Private Keys ermöglichen den Zugriff auf die Vermögenswerte, indem sie für die Signierung einer Transaktion verwendet werden und dadurch verifizieren, dass der Besitzer der Private Keys auch der Besitzer der Vermögenswerte ist. Für weitere Informationen dazu siehe z. B. Antonopoulos (2018), S. 57–79.

6 Der Vollständigkeit halber sei angemerkt, dass ein AMM-Algorithmus auch bei anderen DeFi-Protokollen als Dex's Anwendung finden kann. Für weitere Informationen diesbezüglich siehe z. B. Xu et al. (2021), S. 3.

7 Auf verschiedene Variationen des Constant Product Market Makers wird aus Gründen des Umfangs nicht weiter eingegangen. Für weitere Informationen dazu siehe z. B. Krishnamachari et al. (2021); Mohan (2020).

8 Für weitergehende Informationen bezüglich des Constant Product Market Makers siehe z. B. Lo und Medda (2020), S. 7–8.

Gleichzeitig übernimmt der Preis, der für ein Asset angezeigt wird (z. B. der Kurswert einer Aktie), den Wert, zu dem die letzte Transaktion durchgeführt wurde. Sobald die nächste Transaktion ausgeführt wird, aktualisiert sich der Preis wieder. Im Orderbuch wird u.a. auf der Käuferseite das höchste Kaufangebot und analog auf der Verkaufsseite das niedrigste Verkaufsangebot angezeigt. Die zwischen Kauf- und Verkaufsangebot bestehende Differenz wird als Spread bezeichnet. [10]; [6]

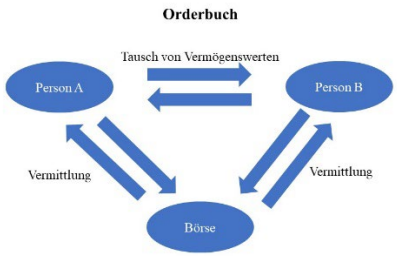

Abbildung 3: Funktionsweise eines Orderbuchs

Quelle: eigene Darstellung

Da die Dex's mit dem größten Marktanteil (gemessen am Handelsvolumen) gegenwärtig einen AMM verwenden, [21] liegt im Folgenden auf diesen der Schwerpunkt der Betrachtung. [37]

Beim traditionellen Wertpapierhandel wird das oben beschriebene Modell eines Orderbuchs verwendet. [40]

Vergleichskriterium	**Dex**	**Traditioneller Wertpapierhandel**
Regulierungsebene		
Rechtssicherheit	Unklar[27]	Eindeutige Jurisdiktion durch Regulierung der Intermediäre [13]
Verhinderung von illegalen Transaktionen	Durch hohen Grad an Privatsphäre erschwert [27]; 19]	Durch KYC erleichtert [12]
Sicherheitsebene		
Open-Source	Vorhanden [20]	nicht vorhanden
Kontrahentenrisiko	Niedrig[37]	Bei Verwahrung durch Intermediär hoch[12] Bei Selbstverwahrung niedrig
Hacker-Angriffe	Niedriges Risiko [37]	Hohes Risiko bei Verwahrung durch Intermediär [46]
Betrug	Durch die Börse nicht möglich [37] Durch Emittenten einfach möglich [52]	Durch die Börse möglich [45] Durch Emittenten von Wertpapieren erschwert möglich [17]
Marktmanipulation	Verschiedene Varianten, wie Pump-and-Dump-Schema [53] und Front- bzw. Backrunning möglich	Pump-and-Dump-Schema möglich [53] Front-bzw. Backrunning nur durch die Börse möglich [22]
Privatsphäre	Hoher Grad da kein KYC-Verfahren verwendet wird [51]	Geringer Grad, da ein KYC-Verfahren verwendet wird [4]
Liquiditätsmangel	Liquiditätsabzug wegen der Gefahr von Impermanent Loss [26]; [11]; [1]	Gefahr durch zu wenige Kauf- bzw. Verkaufsaufträgen [24]; [47]
Nutzungsebene		
Zugangsvoraussetzungen	Keine, lediglich Internetzugriff und Wallet mit Guthaben [43]	Zulassung durch Intermediäre [30]
Kosten	Gebühren für Liquidity Provider Hohe Gas-Gebühren [18]	Gebühren für Dienstleistungen der Intermediäre7] Geringe Gas-Gebühren beim Abzug der Vermögenswerte auf die private Wallet [41]
Kunden-Support	Abgesehen von Erklärungstexten auf der Website nicht vorhanden [49]	Durch die Intermediäre vorhanden [34]
Transaktionsgeschwindigkeit	Abhängig u.a. von der genutzten Blockchain	bei Kryptowährungen: sofort [37]

	Bei Ethereum durchschnittlich einige Minuten [37]	bei Aktien: zwei Tage [44]
Produktvielfalt	Große Zahl an ERC-20 Token [52] keine anderen Asset-Klassen [37] keine Zahlung mit Fiat-Währung möglich	Beschränkte Anzahl an ERC-20 Token [37] verschiedene Asset-Klassen [5] Zahlung mit Fiat-Währungen möglich
Orderarten	Geringe Auswahl [48]	Große Auswahl [36]

3. Vergleich

Regulierungsebene

Ein Nachteil der Nutzung einer Dex gegenüber dem traditionellen Wertpapierhandel ist, dass dort kein eindeutiger Rechtsrahmen vorhanden ist und dadurch Unsicherheiten für die Marktteilnehmer entstehen. Die unsichere Jurisdiktion führt ebenfalls zu dem Nachteil, dass die Attraktivität von Dex's für die Nutzung von Kriminellen zu Betrug und Marktmanipulation steigt.

Ein weiterer Nachteil der Dex ist, dass der hohe Grad an Privatsphäre illegale Transaktionen bspw. Geldwäsche erleichtert. Den untersuchten Quellen nach erfolgt allerdings die Mehrheit der Geldwäsche-Aktivitäten trotz vorhandener Anti-Geldwäsche-Richtlinien auf zentralisierten Börsen.

Sicherheitsebene

Die Nutzung einer Dex bietet im Vergleich zum traditionellen Wertpapierhandel bezogen auf den Sicherheitsaspekt sowohl Chancen als auch Risiken.

Ohne Staatliche Regulierung, die im traditionellen Wertpapierhandel sicherstellt, dass die Intermediäre keine betrügerischen Absichten verfolgen, kann der Handelsteilnehmer über den öffentlich zugänglichen Programmcode der Dex selbst sicherstellen, dass er nicht von den Entwicklern der Dex betrogen wird.

Durch die Offenlegung des Programmcodes können Entwickler sowohl an der Dex mitarbeiten und ggf. Fehler im Code melden als auch die Fehler ausnutzen, um bspw. die Dex anzugreifen. Ob das Offenlegen des Programmcodes die Sicherheit eines Programms insgesamt erhöht oder verringert, ist in der Literatur umstritten. [29]; [42]; [23]

Ein Vorteil der Dex ist, dass der Nutzer ein niedriges Kontrahentenrisiko eingeht, da er die Vermögenswerte in seiner privaten Wallet selbst verwahrt. Auch die Kunden der zentralisierten Börsen sind in der Lage, ihre Vermögenswerte auf die private Wallet abzuziehen. Die Kunden einer zentralisierten Börse hingegen, die entscheiden, ihre Vermögenswerte von dem Intermediär verwahren zu lassen, gehen ein hohes Kontrahentenrisiko ein, da der Intermediär seinen Verpflichtungen gegenüber dem Kunden ggf. nicht nachkommt oder nachkommen kann.

Beispielsweise kann der Intermediär die Zugangsdaten für die Vermögenswerte der Kunden verlieren. Das Risiko, die Zugangsdaten zu verlieren, besteht allerdings auch für den Nutzer, der die Vermögenswerte selbst verwahrt.

Außerdem kann eine Börse im traditionellen Wertpapierhandel gehackt und Vermögenswerte der Kunden entwendet werden. Auch wenn in einigen Fällen der Intermediär den entstandenen Schaden übernommen hat, zeigt das Beispiel von Mt. Gox, dass sich der Kunde nicht darauf verlassen kann. Aufgrund der Selbstverwahrung der Asset beim Verwenden einer Dex, kann der Angreifer durch einen Angriff keinen Zugriff auf die Vermögenswerte der Nutzer erhalten.

Das Kontrahentenrisiko durch den Intermediär im traditionellen Wertpapierhandel zeigt sich nicht nur durch die Gefahr, dass der Intermediär die Zugangsdaten verliert oder gehackt wird, sondern auch dadurch, dass in einigen Fällen, die Betreiber der Börse die Kunden um ihre Vermögenswerte betrogen haben. Diese Gefahr besteht bei der Verwendung einer Dex nicht, da der Nutzer die Vermögenswerte selbst verwahrt. Außerdem können betrügerische Absichten der Dex durch den offenen Zugang zum Programmcode der Dex entdeckt werden.

Der potenzielle Schaden, den das Kontrahentenrisiko auslösen kann, zeigt das Beispiel der Börse Thodex, deren Betrug 90% des gesamten Schadens von Rug-Pulls im Jahr 2021 ausmacht. [17] Für einen solchen Rug-Pull (siehe Abbildung 4) erschafft der Betrüger einen Token (im Folgenden als Scam-Token bezeichnet) (1.) und daraufhin an einer Dex einen Liquidity Pool für den Scam-Token und für eine andere Kryptowährung (bspw. Ether) und stellt sowohl Scam-Token als auch Ether als Liquidität bereit (2.). [52] Die Nutzer der Dex können anschließend Ether gegen den Scam-Token eintauschen, sodass die Menge an Ether im Pool ansteigt (3.). Daraufhin entfernt der Betrüger die gesamte Liquidität aus dem Pool und erhält die Ether, die durch die Opfer dem Pool hinzugefügt wurden, abzüglich der Transaktionskosten als Gewinn (4.)

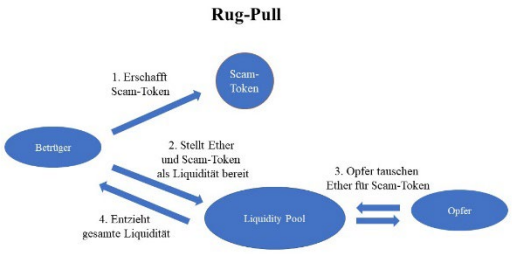

Abbildung 4: Ablauf eines Rug-Pulls

Quelle: Eigene Darstellung, in Anlehnung an Xia et al. (2021) S. 9

Nachteilhaft für die Handelsteilnehmer an einer Dex ist, dass betrügerische Emittenten von Wertpapieren in der Lage sind, dort ihre Token aufgrund der fehlenden Auflagen zu listen. An traditionellen Wertpapierbörsen sind diese Rug-Pulls aufgrund der Auflagen der Börse schwerer durchzuführen.

Ein Rug-Pull wird oftmals durch eine Marktmanipulation in Form eines Pump-and-Dump-Schemas ergänzt, um den Preis für den Vermögenswert künstlich zu erhöhen und den Gewinn für die Betrüger weiter zu steigern. [52] Auch wenn, die Gefahr eines Pump-and-Dump-Schemas ebenfalls beim Handel an einer zentralisierten Börse besteht, erleichtert die Abwesenheit der staatlichen Regulierung dies beim Handel an einer Dex, da v.a. Börsen mit wenig Regulierung häufiger von Pump-and-Dump-Schemata betroffen sind, als Börsen mit einem hohen Grad an Regulierung. [32]

Dadurch, dass die Reihenfolge der Abwicklung der Transaktionen an einer Dex basierend auf den Gas-Preisen, die die Handelsteilnehmer bereit sind zu zahlen, abgewickelt werden, kann Frontrunning beim Handel ohne Intermediäre von jedem Handelsteilnehmer betrieben werden. An einer zentralisierten Börse hingegen kann Frontrunning nur durch die Börse selbst betrieben werden, da nur sie dazu in der Lage ist, Einfluss auf die Reihenfolge der Abwicklung der Transaktionen zu nehmen. Die Gefahr, aufgrund des Frontrunnings einen gestiegenen Slippage-Betrag und damit einen höheren Preis für den Vermögenswert zu zahlen, ist entsprechend v.a. beim Handel an einer Dex gegeben.

Das Unternehmen Chainanalysis sieht den Grund für die gegenwärtige Anfälligkeit von DeFi-Anwendungen (und damit auch von dezentralen Börsen) für Marktmanipulationen darin, dass die Transaktionen schnell abgewickelt werden und gleichzeitig nur wenige Schutzmechanismen in den Programmcodes der Protokolle implementiert sind, die zweifelhafte Transaktionen verhindern. [15]

Ein weiterer Aspekt der Sicherheit, ist der Grad der Privatsphäre, den die Börse den Handelsteilnehmern bietet. Eine Dex können Nutzer verwenden, ohne zuvor einen KYC-Prozess zu durchlaufen. Dadurch bietet eine Dex einen höheren Grad an Privatsphäre als eine traditionelle Börse, bei der der Kunde zur Kontoeröffnung einen KYC-Prozess durchläuft und die Daten durch den Intermediär gespeichert werden. Dadurch ist eine Dex v.a. für Handelsteilnehmer attraktiv, die einen großen Wert auf Privatsphäre legen. Gleichzeitig erleichtert der hohe Grad der Privatsphäre Kriminellen, wie auf der Regulierungsebene beschrieben, illegale Transaktionen durchzuführen.

Beim Handel an einer Dex besteht das Risiko, dass die Liquidity Provider aufgrund des Impermanent Loss einen Wertverlust erzielen und sich entscheiden, die Liquidität abzuziehen. Ohne diese Liquidität wäre ein Handel an einer Dex nicht mehr möglich.

Nutzungsebene

Dadurch, dass jede Person mit einem Internetzugriff und einer Wallet von überall auf der Welt an einer Dex handeln kann, wird keine Person von der Nutzung der Börse ausgeschlossen. Im Gegensatz dazu kann der Intermediär beim traditionellen Wertpapierhandel Kunden, aufgrund von regulatorischen Auflagen, von der Nutzung der Börse ausschließen. Für Personen, die aus dem traditionellen Wertpapierhandel ausgeschlossen wurden, ist es vorteilhaft, dass sie trotzdem an einer Dex handeln können.

Ein Nachteil für die Nutzung einer Dex ist das Vorwissen, das die Handelsteilnehmer benötigen, um eine Dex zu verwenden. Auch können sprachliche Barrieren die Verwendbarkeit einer Dex einschränken.

In Bezug auf die Kosten, fallen die Gebühren an einer großen Zahl traditioneller Börsen im Vergleich niedriger aus als die Gebühren für eine Dex. Eine allgemeine Aussage ist allerdings schwer zu treffen, da die Kostenstruktur von Börse zu Börse unterschiedlich ist, und die Zusatzgebühren, die ggf. beim traditionellen Wertpapierhandel anfallen können, schwer mit den Transaktionskosten an einer Dex verglichen werden können. Allerdings zahlt der Nutzer einer Dex höhere Gas-Gebühren als die Nutzer einer traditionellen Börse, die ihre Vermögenswerte auf ihre private Wallet übertragen, da die komplexe Transaktion über die Smart Contracts einer Dex mehr Gas verbraucht als die einfache Transaktion für das Abziehen der Vermögenswerte. Außerdem kann der Nutzer einer traditionellen Börse die Vermögenswerte von den Intermediären verwahren lassen, sodass keine Gas-Gebühren anfallen. Dadurch geht er allerdings das oben aufgeführte Kontrahentenrisiko ein. Dadurch, dass die Gas-Gebühren nicht proportional zur Transaktionsgröße steigen, senken die Gebühren die Attraktivität der Dex v.a. für Handelsteilnehmer mit niedrigem Transaktionsvolumen. Dies zeigt sich ebenfalls in der durchschnittlichen Transaktionsgröße, die bei Dex's deutlich höher als bei zentralisierten Börsen ausfällt. [16]; [25] Auch Kunden, die mit einer hohen Frequenz

handeln, profitieren verstärkt von den gesparten Gas-Gebühren, da sie diese ansonsten sehr oft zahlen müssen.

Neben den höheren Kosten beim Handel über eine Dex, besteht für die Handelsteilnehmer das Risiko, dass die Transaktion aufgrund einer zu niedrig angesetzten Gas-Gebühr nicht ausgeführt wird. Durch die beinahe sofortige Ausführung einer Transaktion ist ein Vorteil des traditionellen Wertpapierhandel gegenüber einer Dex die höhere Transaktionsgeschwindigkeit.

Ein weiterer Vorteil des traditionellen Wertpapierhandels ist der Support, den die Intermediäre den Kunden bieten. Bei der Verwendung einer Dex erhält der Handelsteilnehmer hingegen keine Unterstützung durch einen Kundensupport.

An der traditionellen Börse ist der Kauf eines Wertpapiers mit Euro oder anderen Fiat-Währungen möglich. Um an einer Dex mit Fiat-Geld zu handeln, muss der Handelsteilnehmer zuerst an einer traditionellen Börse das Fiat-Geld gegen eine Kryptowährung tauschen, mit der er an der Dex handeln kann. Dadurch entstehen für den Handelsteilnehmer ggf. zusätzlicher Aufwand sowie weitere Kosten.

Ohne die Auflagen für das Listen eines Vermögenswerts an einer Dex profitiert der Handelsteilnehmer an einer Dex von der im Vergleich zur traditionellen Börse höheren Anzahl an handelbaren Vermögenswerten. V.a. Vermögenswerte mit einer geringen Marktkapitalisierung werden teilweise nur an Dex's gehandelt. Gleichzeitig haben die fehlenden Auflagen, wie auf der Sicherheitsebene beschrieben, zur Folge, dass auch Wertpapiere mit einer betrügerischen Absicht ohne großen Aufwand an einer Dex gelistet werden können.

Auch wenn die reine Zahl an handelbaren Vermögenswerten an einer Dex höher ist als an einer traditionellen Börse, ist die Produktvielfalt an einer Dex durch die erforderliche Kompatibilität mit der genutzten Blockchain eingeschränkt. Während an einer traditionellen Börse die Handelsteilnehmer verschiedene Asset-Klassen erwerben können, ist der Handelsteilnehmer einer Ethereum-basierten Dex auf die ERC-20 Token beschränkt. Die Umgehung dieses Nachteils durch die Verwendung von Wrapped Tokens ist nur beschränkt möglich, da zum aktuellen Zeitpunkt nur wenige Asset-Klassen von außerhalb der genutzten Blockchain als Wrapped Token ohne Intermediäre abgebildet werden und gehandelt werden können.

Ein weiterer Vorteil des traditionellen Wertpapierhandels ist, dass der Handelsteilnehmer mehr Auswahlmöglichkeiten bei der verwendeten Orderart hat. Bei der Verwendung eines AMM, der von den meisten Dex's genutzt wird, kann der Handelsteilnehmer nur zwischen wenigen Orderarten wählen.

4. Fazit

Die Beantwortung der, diesem Beitrag zu Grunde liegenden Forschungsfrage „Welche Chancen und Risiken bietet der Handel an einer Dex gegenüber dem traditionellen Wertpapierhandel?", führt zusammengefasst nach kritischer Reflexion zu folgender Erkenntnis:

Ein Nachteil der Nutzung einer Dex ist die im Vergleich zum traditionellen Wertpapierhandel unklare Jurisdiktion und die Unsicherheiten, die sich daraus für die Handelsteilnehmer ergeben. Auch die daraus resultierende erschwerte strafrechtliche Verfolgung von Betrügern ist als Nachteil einer Dex zu nennen. Ebenfalls kann die Nutzung einer Dex die Aufklärung von Straftaten wie z. B. Geldwäsche aufgrund der unklaren Jurisdiktion erschweren, während im traditionellen Wertpapierhandel die Intermediäre mit bspw. Anti-Geldwäsche-Richtlinien zur Bekämpfung von illegalen Transaktionen verpflichtet werden.

Auf der Sicherheitsebene ist der hohe Grad an Privatsphäre zu nennen, den die Nutzung einer Dex den Handelsteilnehmern im Vergleich zum traditionellen Wertpapierhandel bietet. Diese Privatsphäre kann allerdings auch von Kriminellen bspw. zur Geldwäsche genutzt werden und ggf. die Nachverfolgung von Straftaten erschweren. Durch den öffentlich zugänglichen Programmcode der Dex kann der Handelsteilnehmer die Programmierung der Dex einsehen und im Gegensatz zum traditionellen Wertpapierhandel selbst verifizieren, dass die Betreiber der Börse keine betrügerischen Absichten verfolgen. Ein Nachteil des traditionellen Wertpapierhandels gegenüber einer Dex ist das höhere Kontrahentenrisiko, das durch die Verwendung von Intermediären entstehen kann. Dadurch besteht für die Handelsteilnehmer an einer zentralisierten Börse das Risiko, die dort verwahrten Vermögenswerte bspw. durch einen Exit-Scam des Intermediärs zu verlieren. Bei der Nutzung einer Dex besteht zwar die Gefahr eines Betrugs des Intermediärs nicht, dafür allerdings ein höheres Risiko, Opfer von betrügerischen Emittenten von Wertpapieren, oder Marktmanipulationen zu werden. Eine traditionelle Börse bietet hingegen mithilfe der Auflagen für das Listen eines Vermögenswerts einen höheren Schutz vor Rug-Pulls und anderen möglichen Betrugsfällen durch Emittenten.

Durch diese Auflagen können allerdings viele kleine ERC-20 Token nicht an traditionellen Börsen gelistet werden und werden entsprechend nur an Dex's gehandelt. Im Gegenzug bietet die traditionelle Börse allerdings auch andere Vermögenswerte als Kryptowährungen, wie z. B. Aktien und Anleihen, zum Handel an. Dadurch, dass an einer Dex nur ERC-20 Token gehandelt werden können, können diese ebenso wie Fiat-Geld an einer Dex nicht gehandelt bzw. verwendet werden. Um mit Fiat-Geld an einer Dex zu handeln, muss der Handelsteilnehmer zuvor bei einer zentralisierten Börse sein Fiat-Geld bspw. gegen Stablecoins o.ä. tauschen. Ein weiterer Nachteil der Dex sind die hohen Gas-Gebühren der Ethereum-

Blockchain, die für das Handeln an einer Dex von den Nutzern gezahlt werden müssen. Dadurch, dass die Gas-Gebühren pro Transaktion und unabhängig von dem Transaktionsvolumen gezahlt werden müssen, reduzieren diese die Attraktivität einer Dex v.a. für Handelsteilnehmer mit niedrigem Transaktionsvolumen und/ oder hoher Transaktionsfrequenz.

Resümierend kann gesagt werden, dass der Handel an einer Dex v.a. Handelsteilnehmer mit einer höheren Sicherheitsorientierung anspricht, während der traditionelle Handel insbesondere Vorteile auf der Regulierungs- und Nutzungsebene aufweist.

Literaturverzeichnis

[1] Aigner, Andreas A.; Dhaliwal, Gurvinder (2021): Uniswap: Impermanent Loss and Risk Profile of a Liquidity Provider.

[2] Angeris, Guillermo; Kao, Hsien-Tang; Chiang, Rei; Noyes, Charlie (2019): An analysis of Uniswap markets.

[3] Antonopoulos, Andreas M. (2018): Bitcoin & Blockchain - Grundlagen und Programmierung: Die Blockchain verstehen, Anwendungen entwickeln, Sebastopol.

[4] Binance (2022): Create your Account, online abrufbar unter: https://accounts.binance.com/en/register, (Abrufdatum: 27.02.2022).

[5] Binance (2022): Trade Crypto Futures, online abrufbar unter: https://www.binance.com/en/futures, (Abrufdatum: 26.02.2022).

[6] Black, Fischer (1971): Towards a Fully Automated Exchange, Part I, in: Financial Analysts Journal, 27. Jahrgang, S. 29–34.

[7] Böhme, Philip. (2004): Transaktionskosten im Aktienhandel: Wettbewerbliche Analyse institutioneller und alternativer Handelssysteme in Europa, Wiesbaden.

[8] Börse Frankfurt (2022): DAX-Orderbuch, online abrufbar unter: https://www.boerse-frankfurt.de/aktien/offenes-orderbuch/DE0008469008, (Abrufdatum: 15.02.2022).

[9] Börse Stuttgart (2022): Über die blocknox GmbH, online abrufbar unter: https://www.boerse-stuttgart.de/de-de/gruppe-boerse-stuttgart/unternehmen/unsere-unternehmen/blocknox-gmbh/, (Abrufdatum: 13.02.2022).

[10] Bosch, Robert. (2001): Market-Maker als liquiditätsspendende Intermediäre in Börsenmärkten: Das Betreuerkonzept der Deutschen Börse AG, Wiesbaden.

[11] Boueri, Nassib (2021): G3M Impermanent Loss Dynamics.

[12] Bundesamt für Sicherheit in der Informationstechnik (2019): Blockchain sicher gestalten: Konzepte, Anforderungen, Bewertungen.

[13] Bundesanstalt für Finanzdienstleistungsaufsicht (2022): (Internetseite), online abrufbar unter: https://www.bafin.de/DE/Startseite/startseite_node.html, (Abrufdatum: 05.02.2022).

[14] Catalini, Christian; Gans, Joshua S. (2016): Some simple Economics of the Blockchain, NBER working paper series, Nummer 22952.

[15] Chainanalysis (2021): The 2021 Crypto Crime Report: Everything you need to know about ransomware, darknet markets, and more.

[16] Chainanalysis (2021): Cryptocurrency Exchanges in 2021: A Competitive Landscape Analysis November 2021.

[17] Chainanalysis (2022): The 2022 Crypto Crime Report: Original data and research into cryptocurrency-based crime.

[18] Coinmetrics (2022): ETH Mean & Median Fee, USD, online abrufbar unter: https://charts.coinmetrics.io/network-data/#928, (Abrufdatum: 22.02.2022).

[19] Cumming, Douglas J.; Johan, Sofia; Pant, Anshum (2019): Regulation of the Crypto-Economy: Managing Risks, Challenges, and Regulatory Uncertainty, in: Journal of Risk and Financial Management, 12. Jahrgang.

[20] Curve (2022): Curve: Effective on-chain market making, online abrufbar unter: https://github.com/curvefi, (Abrufdatum: 05.01.22).

[21] Dune Analytics (2022): Dex Metrics, online abrufbar unter: https://dune.xyz/hagaetc/dex-metrics, (Abrufdatum: 24.02.2022).

[22] Eskandari, S.; Moosavi, S.; Clark, J. (2019): SoK: Transparent Dishonesty: Front-Running Attacks on Blockchain, in: Bracciali, Andrea; Clark, Jeremy; Pintore, Federico, Ronne, Peter B.; Sala, Massimiliano, Financial Cryptography and Data Security, Cham, S. 170-189.

[23] Ford, Richard (2007): Open vs. Closed: Which is more secure?, in: ACM Queue, 5. Jahrgang, S. 32-38.

[24] Gärtner, Christian. (2007): Liquidität am deutschen Kapitalmarkt: Erholungsfähigkeit der DAX-30-Titel, Wiesbaden.

[25] Godbole, Omkar (2021): Large Traders Dominate DEXs as High Ethereum Fees Keep Retail Investors at Bay, in: Coindesk, online abrufbar unter: https://www.coindesk.com/markets/2021/12/02/whales-dominate-dexs-as-high-ethereum-fees-keep-retail-investors-at-bay/, (Abrufdatum: 19.01.2022).

[26] Heimbach, Lioba; Wang, Ye; Wattenhofer, Roger (2021): Behavior of Liquidity Providers in Decentralized Exchanges.

[27] Her Majesty's Treasury and Home Office (2020): National risk assessment of money laundering and terrorist financing 2020.

[28] Hickey, Liam; Harrigan, Martin (2020): The Bisq DAO: On the Privacy Cost of Participation.

[29] Hoepman, Jaap-Henk; Jacobs, Bart (2021): Increased security through open source.

[30] Holtmeier, Moritz; Sandner, Philipp (2019): The impact of crypto currencies on developing countries.
[31] Hsieh, Ying-Ying; Vergne, Jean-Philippe; Anderson, Philip; Lakhani, Karim; Reitzig, Markus (2018): Bitcoin and the rise of decentralized autonomous organizations, in: Journal of Organization Design, 7. Jahrgang, Heft 14.
[32] Kamps, Josh; Kleinberg, Bennett (2018): To the moon: defining and detecting cryptocurrency pump-and-dumps, in: Crime Science, 7. Jahrgang, Heft 18, online abrufbar unter: https://doi.org/10.1186/s40163-018-0093-5.
[33] Klitzsch, Wolfram. (2019): Grundbegriffe der Wirtschaft: Ein Nachschlagewerk für Einsteiger, Wiesbaden.
[34] Kraken (2022): Contacting Kraken Support, online abrufbar unter: https://support.kraken.com/hc/en-us/articles/215601908, (Abrufdatum: 16.02.2022).
[35] Krishnamachari, Bhaskar; Feng, Qi; Grippo, Eugenio (2021): Dynamic Automated Market Makers for Decentralized Cryptocurrency Exchange.
[36] Li, Sida; Ye, Mao; Zheng, Miles (2021): Financial Regulation, Clientele Segmentation, and Stock Exchange Order Types.
[37] Lin, Lindsay X. (2019): Deconstructing Decentralized Exchanges, in: Stanford Journal of Blockchain Law & Policy, S. 58 - 77.
[38] Lo, Yuen; Medda, Francesca (2020): Uniswap and the rise of the decentralized exchange, MPRA Working Paper, Nummer 103925.
[39] Mohan, Vijay (2020): Automated Market Maker and Decentralized Exchanges: A DeFi Primer.
[40] New York Stock Exchange (2022): The NYSE Market Model, online abrufbar unter: https://www.nyse.com/market-model, (Abrufdatum: 16.01.2022).
[41] o.V. (2022): Coinbase Gebühren 2022: Das kostet der Handel mit Bitcoin und Co. auf der Kryptoplattform, in: Wirtschaftswoche, online abrufbar unter: https://www.wiwo.de/finanzen/boerse/coinbase-gebuehren-2022-das-kostet-der-handel-mit-bitcoin-und-co-auf-der-kryptoplattform/27399498.html, (Abrufdatum: 22.02.2022).
[42] Payne, Christian (2002): On the security of open source software, in: Information Systems Journal, 12. Jahrgang, S. 61–78, online abrufbar unter: https://online-library.wiley.com/doi/full/10.1046/j.1365-2575.2002.00118.x, (Abrufdatum: 02.02.2022).
[43] Popescu, Andrei-Dragos (2020): Transitions and Concepts within Decentralized Finance (DeFi) Space, in: Research Terminals In The Social Sciences, S. 40–61.
[44] Santander, Oliver; Wyman, Anthemis (2015): The FinTech 2.0 Paper: rebooting financial services.
[45] Scharfman, Jason. (2022): Cryptocurrency Compliance and Operations: Digital Assets, Blockchain and DeFi, Cham.
[46] Scheider, David (2019): Die 5 größten Bitcoin-Börsen-Hacks, in: BTC-ECHO, online abrufbar unter: https://www.btc-echo.de/news/die-5-groessten-bitcoin-boersen-hacks-81710/, (Abrufdatum: 30.12.2021).
[47] Schier, Susanne (2022): Nach massiver Kritik: Trade Republic hebt Kaufsperre von Gamestop & Co. wieder auf, in: Handelsblatt, online abrufbar unter: https://www.handelsblatt.com/finanzen/banken-versicherungen/banken/neo-broker-nach-massiver-kritik-trade-republic-hebt-kaufsperre-von-gamestop-und-co-wieder-auf/26863918.html?, (Abrufdatum: 25.02.2022).
[48] Uniswap (2022): Range Order, online abrufbar unter: https://docs.uniswap.org/protocol/concepts/V3-overview/range-orders, (Abrufdatum: 16.02.2022).
[49] Uniswap (2022): Uniswap Help Center, online abrufbar unter: https://help.uniswap.org/en/, (Abrufdatum: 10.01.2022).
[50] Uniswap (2022): Uniswap Swap (Web-Interface), online abrufbar unter: https://app.uniswap.org/#/swap?chain=mainnet, (Abrufdatum: 16.02.2022).
[51] Werner, Sam M.; Perez, Daniel; Gudgeon, Lewis; Klages-Mundt, Ariah; Harz, Dominik; Knottenbelt, William J. (2021): SoK: Decentralized Finance (DeFi).
[52] Xia, Pengchen; Wang, Haoyu; Gao, Bingyu; Su, Weihan; Yu, Zhou; Luo, Xiapu; Zhang, Chao; Xiao, Xusheng; Xu, Guoai (2021): Trade or Trick? Detecting and Characterizing Scam Tokens on Uniswap Decentralized Exchange, in: Proceedings of the ACM on Measurement and Analysis of Computing Systems, 5. Jahrgang, Heft 3.
[53] Xu, Jiahua; Livshits, Benjamin (2018): The Anatomy of a Cryptocurrency Pump-and-Dump Scheme.
[54] Xu, Jiahua; Paruch, Krzysztof; Cousaert, Simon; Feng, Yebo (2021): SoK: Decentralized Exchanges (DEX) with Automated Market Maker (AMM) Protocols.

Context-based Role Object Pattern with On-Chain Smart Contract Programming

Orçun Oruç, Uwe Aßmann, Arbli Troshani
Technische Universität Dresden, Software Technology Group, Nöthnitzer Straße 46, 01187 Dresden

Dynamic object roles and corresponding contexts can model complex applications with higher-level abstraction. These abstracted applications can be used in wider areas such as financial institutions, health care, and supply chain network. Role management which consists of the creation of role objects, and binding role object between core objects still suffers from non-intrusive logging-monitoring, auditing, and resilient data source for role-based applications. Moreover, immutable smart contracts cause problems concerning bug fixing and maintenance without dynamic binding to new smart contract objects. An object that is created from a smart contract (contract class) can be transparently attached to a role object utilizing the Role Object Pattern (ROP). However, ROP itself does not contain a context definition and context-specific role assignment grouping the definition of smart contract relationships in abstracted data types. In this study, we would like to implement an extended version of the role object pattern called Context-based Role Object Pattern (ContextROP) with an on-chain smart contract language called Solidity to solve fundamental problems. To evaluate the proposal, we will implement a use case with the design pattern proceeding with qualitative and quantitative analysis.

***Keywords**: Smart contracts, Role-based Programming, Role-Object Pattern, Object-Oriented Programming*

1. Introduction

In software engineering, a design pattern is a repeatable solution for a common design problem. One can transform a specific design pattern directly into the code. A smart contract is an autonomous entity and verifiable agreements between participants. However, a bad design of a smart contract can cause immersive problems between participants. For instance, if there is a bug in a smart contract, it must be updated on-chain network. When you deployed a new contract to update a deprecated contract, smart contract data and application logic should be altered. That is why eternal storage and upgradable contract pattern have been proposed.

Smart Contracts are deterministic, isolated, and immutable programs that can work in decentralized networks. A smart contract must give the same results under the same inputs to comply with the determinism concept. Off-chain transactions rely on a blockchain network; however, the computational logic is stored in off-chain transactions without hashed values (TransactionX). On-chain smart contracts can only provide an isolation principle because an external computation in a smart contract cannot be isolated virtual machine such as Ethereum Virtual Machine (Ethereum VM). The most important principle that we need to emphasize is the immutability of smart contracts.

Immutability issue is an important characteristic of smart contracts [2]. The immutability character of Solidity contracts can harm the credibility of auditing while changing the smart contract data structure in case of an error. Another problem could be that misused or hacked contracts, smart contracts cannot be changed [2].

„Object schizophrenia or self-schizophrenia is a combination arising from the delegation and related techniques in object-oriented programming.“[1]. Objects can have a single behavior and attribute at a specific time; however, there are some programming techniques that could not lead us to distinguish the singularity of identity. For instance, the delegation in class-based programming languages causes differen attribute personalities for an object because a delegated method can call from a base method of a base class [1]. Analogous to the class-object concept of object-oriented programming languages, smart contracts use objects from contracts (class) relationship. Contracts can be defined as class-like structures. Once a contract is deployed, the storage (data) and application logic of a contract should be deployed together. Real-world entities can be represented with roles. Entities that have several behaviors and attributes can play several roles during their lifetime. Even in object-oriented programming, each object has a set of roles because objects can be created with different properties (attributes and behaviors) from a base class. To create roles, we have a set of methods like dynamic classification, multiple classification, multiple inheritance, type hierarchy with subtyping (overriding), and subclassing. For instance, a human can be classified as *Person, Employee*, *Manager, Teacher, Student*, and *Retired Employee. Employee*, Manager, and *Retired Employee* can belong to a Factory context because they have worked in this context with attributes (name, id, social security

1https://wiki.c2.com/?ObjectSchizophrenia

number). Some roles cannot co-exist like *Person* cannot be *Employee* and *Retired Employee* at the same time. Identity sharing can also happen in on-chain smart contracts because they use object-oriented language with the aforementioned features. This study would like to show the possible effect of identity sharing on smart contract development.

Each contract has deployment and execution asset costs concerning the operation of a smart contract in a blockchain decentralized network. Developers can redeploy a smart contract so as to eliminate outdated and deprecated storage and application logic from updated contracts; however, there is a dangerous point with regards to the security of smart contracts. This is called Reentrancy attack. The reentrancy attack can be eliminated with the concept of the deep role because a role that has been played before cannot be played by another core contract again. In the concept of deep roles concept (roles are playing roles), a core object can play roles, but played roles cannot play other roles. In this manner, smart contract security can prevent reverse calling for played roles by implementing role modeling.

The rest of the paper is structured as follows: We emphasize the research problem in Chapter 2 and describe our motivation with research questions in SubChapter 2.1 to conduct this research. Then, we provide background of role abstraction in smart contract design, design pattern concept in Solidity language, computational cost in stateful on-chain smart contracts in Chapter 3. Chapter 4 will be relevant to the current challenges that we have faced during the research study and the limitations of the study will be listed. After we have emphasized the key takeaways from related studies in Chapter 5, we will analyze the implementation of the proposed design pattern in on-chain smart contract programming. In Chapter 6, we will give details of implementation. In Chapter 7, we will discuss key findings regarding the conducted research with a list of conclusions to enlighten the reader. Finally, in Chapter 8, further key points in regard to development and research will be listed.

2. Research Problem

In this chapter, we will define our research questions and the major problems that have motivated us to complete this paper. Roles are abstraction layers of an object-oriented approach to solve multiple problems, which are:

- Extending key abstractions of roles should be represented as an aspect of suitability and cost-effectiveness in a smart contract language such as Solidity. Which smart contract language features are necessary to represent key abstractions of roles?

- Although managing dynamic roles is an important role-based language feature. Role Object Pattern (ROP) suffers from object schizophrenia and one can solve this problem with delegation and forwarding in object-oriented programming languages.

- Role-level constraints are necessary to maintain constraints among roles without a context. How can we implement constraints between roles?

- By implementing subclassing in a role modeling scenario, we can implement the Role Object pattern recursively. What are the drawbacks and benefits in terms of performance and gas cost for Solidity on-chain programming language?

In addition to the main problem interests, we would like to focus on the following research question:

Research Question 1 (RQ1): How to identify different role subtyping through interfaces in Solidity?

Research Question 2 (RQ2): How can type safety be ensured statically?

Research Question 3 (RQ3): What are the benefits and drawbacks of proxy pattern and interface selector according to role modeling in on-chain contract languages?

2.1. Motivation

The main motivation of this paper is to provide a preview of one of the important design patterns for role modeling, which is the Role Object Pattern (ROP). By implementing the extended version of this pattern, we will elaborate on possible implications while extending the design pattern with contexts in Solidity language. ROP focuses on the dynamicity of a role insertion into the system of the main design. Even if we have dynamic design patterns such as Proxy Delegate, Upgradable Standard for Proxy Delegate, and Eternal Storage, the ROP can support context which can provide a computational entity and grouping relationships in model-driven engineering.

3. Background

3.1. On-chain and Off-chain Smart Contract Programming Decentralized Networks

Concerning the programming concept in smart contracts, we have two different terms, which are on-chain and off-chain smart contract programming. The fundamental difference between off-chain and on-chain smart contract programming is being connected with an external service that is not part of a blockchain network.

A smart contract can check preconditions and postconditions in the on-chain network. On-chain smart contract programming has some advantages, which are:

Transactions are executed in an on-chain database, which is called blockchain network.

The state of the blockchain and smart contracts can be tracked by means of on-chain events.

With *event* and *emit* keywords, one can implement an advanced logging system without implementing third-party logging solutions. Beyond that, one can realize a domain-specific language for logging in the Ethereum

network that works with Solidity language to get information about transactions, transaction receipts, and states[2].

Off-chain data can be harmonized with external data sources such as specialized streaming data platforms, key-store databases, object databases, relational databases, interplanetary file systems or file regular file systems. The main difference between off-chain data and on-chain data is to manage data sources through a blockchain network or manually. Another property regarding off-chain data is supporting non-Turing complete smart contract languages. For instance, Bitcoin has an internal smart contract script language, however, it does support basic variable assignment without creating a loop and reference types.

3.2. Dynamic Contract Approach with Proxy Pattern is Solidity

Proxy patterns have been invented and implemented to realize hot bug fixes in Solidity programming since a contract code is immutable after deployment. Generally, the concept is widely used for gas savings and dynamic contract upgrading. After deploying a proxy contract, all messages will be transferred to the corresponding address, which can be a new version of a contract. In essence, we have three different types of proxy patterns[3].

- **Eternal Storage**: Updated contract remains in a blockchain network with old contract data layer and the data layer might consist of user information, account balances, or references to other contracts.
- **Unstructured Storage**: In this type of proxy contract, we need to follow the structure of reference data (attributes of a struct type) whether in the right order or not. Since the Solidity language sets up variables in a contract sequentially, the caller contract should move the references of storage variables (state variables) from the callee contract. The drawback of the pattern is that cannot be implemented to reference data structure of Solidity such as mapping and structs.
- **Inherited Storage**: This type of proxy contract ensures that the order and state of storage variables between caller and callee will be the same. The main aim is to protect the data layer of a smart contract without inserting complicated assembly code blocks in a smart contract[4].

All of the above-mentioned patterns require low-level dynamic calls that only should be invoked by experienced developers because they can easily contain a code snippet that has a hard-to-find bug. The main challenge in upgraded contracts is to preserve old storage (data layer) with updated contracts (application layer). All of the described patterns can be used to implement dynamic smart contracts; however, the main difference between them is being asset cost and handling storage of contracts because they share both proxy and contract behavior [5].

We have a couple of dynamic proxy patterns standards as below [6] :

Diamond pattern, Multi-Facet Proxy (EIP-2535): It solves the maximum contract size limit in the Ethereum world. A diamond pattern provides a way to organize smart contract code and smart contracts can be assigned as upgradable and immutable for the future. Moreover, the incremental upgradable smart contract is possible so that one can take the altered part of a smart contract is possible so that one can take the changed part of a smart contract, and can assign this part as upgradable by means of Diamond Pattern[7].

Transparent Proxy Pattern: The goal of the proxy pattern is to make indistinguishable an externally owned account with actual logic contract [8]. In order to prevent proxy selector clashing, which means that the same function signatures should be controlled in external contracts as well so that the transparent proxy pattern can be used because one can make a transaction without an admin of the proxy contract.

Universal Upgradable Proxy Standard (UUPS) (EIP-1822): This relies on a standard called EIP-1822[9]. In this standard, authors have two essential motivations which are [10]:

- Easy to deploy and maintain proxy and logic contracts.
- Standardization of proxy contract implementation by verifying the bytecode used by the Proxy Contract.

3.3. Role and Core Objects in Solidity

Although object-oriented programming solves major problems in software development, abstraction of objects and dynamicity have not been properly addressed and these are still hard to solve with object-oriented programming.

---

2 https://github.com/ChrisKlinkmueller/Ethereum-Logging-Framework
3 https://blog.openzeppelin.com/proxy-patterns/
4 http://blog.openzeppelin.com/upgradeability-using-unstructured-storage/
5 https://blog.openzeppelin.com/upgradeability-using-unstructured-storage/
6 https://blog.logrocket.com/using-uups-proxy-pattern-upgrade-smart-contracts/
7 https://eips.ethereum.org/EIPS/eip-2535
8 https://blog.openzeppelin.com/the-transparent-proxy-pattern
9 https://eips.ethereum.org/EIPS/eip-1822
10 https://eips.ethereum.org/EIPS/eip-1822

Single Role Type: All role features incorporate into one single role type. For instance, engineers, salesman, and directors can be differentiated by job descriptors and description IDs [3]. If each of the occupations has different features, different types can be generalized by means of interfaces from base interface classes. This concept is similar to role subtyping.

Role Subtyping: We can represent the many roles of an object in a smart contract language by making a subtype for each role [3].

Role Object: Common features can be inserted into a host object with a separate role object. In this case, occurrence constraints are hard to achieve, but it is easy to implement with client applications that work with host objects.

Role Relationship: Roles can be represented by many role objects. If a host object may have more than one role object, a role relationship comes into the game to represent occurrences between role objects.

4. Limitations and Challenges

This study is limited to the on-chain smart contract programming language that has object-oriented features to analyze and discuss the results of role modeling mapping in the object-oriented programming world. We have created qualitative and quantitative research parameters to test role-based applications. We exclude the networking and consensus layer of blockchain technologies because they are irrelevant to the implementation of ROP.

ContextROP is supporting only a static view of the context, which means that roles cannot be migrated from one context to another dynamically. We will mainly discuss on-chain crypto assets (gas cost optimization with role object pattern to reduce deployment, operational and computational costs of on-chain smart contracts. One of the biggest challenging points is to manage immutable smart contracts integrating role modeling. Roles can be assigned dynamically and static representation with interfaces does not provide all of the role-based modeling features such as dynamic loading, deep-role playing, and dynamic role type without interface definition.

One of the language limitations is the immutability of smart contracts in the runtime and advanced role-based type safety. Even if the Solidity programming language is statically typed, role subtyping could not be ensured with an extra effort of type safety structure. Another limitation can be mentioned regarding contexts, and one cannot easily describe constraints between roles. For instance, occurrence constraints can be implemented employing abstracted data types such as Set, HashSet, and HashMaps by checking the maximum or minimum number of occurrences at runtime. However, Solidity offers *Mappings* abstract data structure with limited functionality of *Map* data structure.

Another language limitation is the lack of *isInstance* or instanc*eOf* keyword like in an object-oriented language to provide type safety. Programming languages support static type safety for primitive data types such as integer, boolean, float, and double. If a developer wants to create an abstract type from a class, the possessiveness of a new object with an abstract type should be assured. Unlike Mappings and structs are major abstract non-intrusive types in Solidity language, one can create abstract new types with single, multiple, multi-level, and hierarchical inheritance systems with this language.

The last limitation is the dynamic deployment of a smart contract. A single smart contract has the limitation of a maximum 24KB contract size, which means that smart contracts cannot have a complex role-based application with extensive computational loops. ContextROP design pattern does not address the smart contract size limitation.

5. Related Work

The main paper about the role object pattern has been proposed by Bäumer et. al. [4] and they have claimed that attached role objects represent a role that can be played by an object in a client's context. In their design pattern description, they have described role objects and core objects.

Stolz and Steimann have proposed lightweight role objects that can refactory roles implemented as subclasses of a role player letting instances of three role objects share state and identity with an instance of the role player object [11] . Moreover, the authors have used the method that is called Replace Inheritance with Delegation Refactoring (RIWD) to allow reuse without role subtyping in order to avoid cumbersome and bloat interfaces that define role subtyping and supertyping [12] .

Martin Fowler has divided up different parts of role-based modeling, which are Single Role Type, Separate Role **Type, Role Subtype, Role Object, Role Relationship, Internal Flag, Hidden Delegate, State Object, Explicit Type Method, and Parameterized Type Method** [3]. The main motivation of this paper is to distinguish role-based modeling features from different conceptual ideas by emphasizing the main takeaways. In the *Conclusion* chapter of the study, the author stated that every selection of a design pattern in role-modeling has a trade-off in software modeling and programming. Another fact from the paper can be deducted as role-playing assumptions that may not be true for all condi-

11https://www.fernuni-hagen.de/ps/prjs/IROP/

12http://www.feu.de/ps/prjs/RIWD/

tional testing. A role player can be important for an individual use case, but another user may not need to constrain the role player because the role objects itself is more important than the role players in this case.

Stephan Hermann has claimed that roles define the intersection of objects and contexts. Contexts can be grouped by static and dynamic views, which means that either a set of roles can be assigned to a static context or they can migrate from one context to another [6]. In this paper, the author proposed a language called ObjecTeams that has the capability to group a number of roles into a context, more precisely in the paper is called team [6].

Steimann and Urs Stolz [7] have proposed refactored role object pattern by way of intensive usage of subclassing in an object-oriented language. These subclassing methods can be listed as follows [7]:

- **Entity Type:** A base class can be renamed as an entity type in order to create abstracted role types from a core component class.
- **Base Interface:** From an interface, an entity type and abstract role type can be created to constitute concrete role types.
- **Component Type:** This is the regular way of creating role types in the Role Object Pattern. It inserts a new abstract class between the entity class and intermediate subclasses to create role classes that do not change the behavior of a program because it does not add anything [7]

In this paper, the main idea is to replace inheritance with delegation refactoring to add roles to the component core. Cabot and Raventos emphasized the importance of the *Role as Entity Types* pattern that can be useful to represent roles while a role-based application requires full expressiveness [5]. Cabot and Raventos have started to list role features such as ownership, control, role-playing, role identity, adoption, and relationship. In the design and implementation phase, they have been categorized into three major topics, which are [5]:

- **Roles as Subtypes Pattern:** Roles can be designed by subtypes of a base class. For instance, Teacher and Student can appear as subtypes of Person class.
- **Roles as Interfaces Pattern:** Roles are represented as interfaces and this study utilizes the approach in the implementation. We can specify entity types that play a certain role through interfaces.
- **Roles as Reified Entity Types Pattern:** Roles are represented as reified entity types with a relation type. A Student type can represent a relationship between University and Person even if it is not clear possessive of role type to University or Person.
- **Roles as Participant Names Pattern:** A role is barely represented as a name assigned to an entity type in a relationship type. For instance, Project Manager and Branch Manager cannot be occurred in the same conceptual schema since in this case, a role cannot play other roles.

Steimann [6] claims that interfaces are a prominent Object-Oriented programming concept since they allow decoupling of implementation [8]. One can declare every variable and parameter with an abstract type in order to realize roles as interfaces. In the definition UML metamodel of the paper, a merger module can merge *Interface* and *ClassifierRole* to a new metaclass called *Role*. In the conclusion of the study, the conceptual representation of roles with interfaces does not cover all features of the role concept.

Wöhrer and Zdun [9] summarize a set of patterns such as contract register pattern, contract relay pattern, and satellite pattern. Through the contract register pattern, contract participants can be pointed to the latest contract version. The register contract keeps track of different versions (addresses) of a contract. Moreover, a contract relay pattern can be useful to handle the update process of a contract [9]. By means of the satellite pattern, one can store addresses of them in a base contract that allows for modification and replacement contract functionality.

6. Implementation

Implementation is twofold for the application of Solidity programming. Dynamic proxied and static interface separator for team activation. We would like to list both features to evaluate differences in asset cost (gas cost), and performance evaluation in deployment. The static interface has been implemented with a standard interface detector that is called EIP-165.

We have major 5 different classes, which are:

- ERC165 (EIP-165)
- Component
- ComponentCore
- ComponentRole
- Team
- ExtendedRole
- Each of them has a different purpose while creating role-based applications in specified contexts, which are:

ERC165 (EIP-165): Interfaces should be identified and differentiated in Solidity programming. The main aim is to detect if a contract implements any given interface[13].

13https://eips.ethereum.org/EIPS/eip-165

In the ERC165 contract, there is a function called *supportsInterface()* that takes an *interfaceID* bytes32 format.

Component: This is an interface that represents a key abstraction for *ComponentRole* and *ComponentCore* to define adding and removing role objects. *Component* is the base entity that provides a role management interface.

ComponentCore: A core object creates a role object from this «abstract» contract to play a role and it implements role management protocol through the *Component* interface.

ComponentRole: ComponentRole is the main component that can create role objects from core objects.

Team: Team smart contract provides context-based grouping for role-based applications. Principally, the Team represents the context concept that can activate and deactivate to single or multiple roles accordingly.

Extended Role: This smart contract utilizes the approach of a dynamic proxy pattern that can help us to deploy an updated contract with a low gas cost. ExtendRole can be used in the UUPS Proxy Contract implementation in order for providing dynamic upgradable contracts.

```
1  Interface Component {
2        function addRole(bytes32 spec, address
         role) external;
3        function removeRole(bytes32 spec) ex-
         ternal;
4        function isPlayingRole(bytes32 spec)
         external;
5        function getRole(bytes32 spec) external
         returns (address);
6        function activateTeam(address team)
         external;
7        function deactivateTeam() external;
8        function getActivateTeam() external
         view returns(address);
9  }
```

Listing 1: Component Interface in ContextROP

As listed in Listing 1, we have major functions activating context and dispatching role objects to them with bytes32 spec addresses. Bytes32 dynamic array of bytes can be selected because the data type can be utilized in function arguments to pass arguments and return a result from a contract.

```
1  library InterfaceCodes {
2        bytes4 constant COMPONENT_ID = type(Compo-
         nent).interfaceId;
3        bytes4 constant COMPONENT_ROLE_ID = type(Com-
         ponentRole).interfaceId;
4        bytes4 constant TEAM_ID = type(TEAM).interfaceId;
5  }
```

Listing 2: InterfaceCodes for EIP165 Contract Separator

As for Listing 2, *InterfaceCodes* can be customized to distinguish abstract types from base classes from each other. Interfaces are identified as a set of function selec

tors in the Application Binary Interface (ABI) definition of Solidity programming language. To prevent invoking different function signatures as if they were the same, *bytes4* of the function signature hash should be used with customized *InterfaceCodes.*

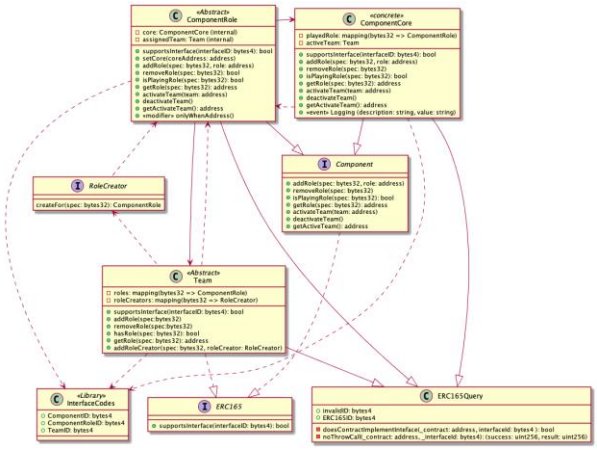

Figure 1: UML Class Diagram for ContextROP Standard Interface Detector (EIP-165)

As shown in Figure 1, we have different modules to create the fundamental requirements of the ContextROP design pattern that consists of ERC165, InterfaceCodes, Team, RoleCreator, ComponentRole, ComponentCore. Team, ComponentRole, and ComponentCore should inherit a set of functions such as doesContractImplementInterface, and noThrowCall. Chiefly, these two functions can control interface identification numbers to simulate functions like typeOf or isInstance in object-oriented languages. Since natural type safety mechanism is not found in on-chain smart contract language, namely Solidity, developers can provide the subclassed type safety by way of interface detectors.

To connect through an externally owned account (EOA) to the Context-ROP application, load, and deploy methods should be given. These methods are overloaded methods with function signatures that take contractAddress, Web3j credentials, unit value of the gas price, and gas limit. After one loaded a contract, they might be deployed with the same aforementioned parameters through RemoteCall.

Order to reach on-chain ContextROP application by means of a general-purpose language. Contract address, credentials, and contract gas provider should be defined by externally owned accounts.

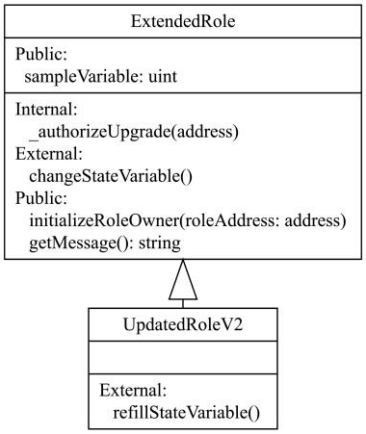

Figure 2: UUPS Diagram for Roles

As depicted in Figure 2, one of the concepts is the UUPS Proxy Pattern that originated from EIP-1822. This pattern relies on the storage holder (proxy) and logic contract implementation. In the proxy contract, the contract stores storage variables that can be used by a logic of an external contract. A state variable or storage layout organizational pattern is needed because Solidity's built-in storage layout system does not support proxy contracts [14]. Through advanced libraries, using *DelegateCall*[15] is not a hurdle that developers should cope with.

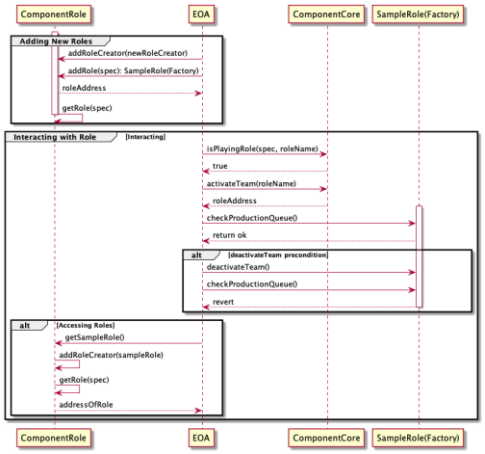

Figure 3: Sequence Diagram for Roles

As shown in Figure 3, we have different stages to interact with a role-based application from creation to termination. When a role creation function is invoked by an Externally Owned Account (EOA), a particular address should be given to the reciprocal function. It works with external clients or wallet accounts in the blockchain network. A smart contract naturally cannot activate another on-chain smart contract in a blockchain network. After adding a particular role, the role can be played with its name in a registered team (context) via *activateTeam(roleName)* function. A strict condition in the sequence diagram is to deny role-playing after deactivating with the function called *deactivateTeam().* Analogous to creating roles, accessing roles can invoke similar methods with *bytes4* or *bytes32* variables for Ethereum VM addresses in the shared memory.

7. Evaluation

In this chapter, we would like to evaluate the ContextROP application that we have created in Solidity Programming Language. In role-based definitions of Steimann [10], Kühn (PhD Thesis, A Family of Role-based Languages, Thomas Kühn), we can list 26 different statements. These statements cover most of the role modeling features from two different research studies. Result of the qualitative evaluations can be seen in Figure 4 and Listing 3.

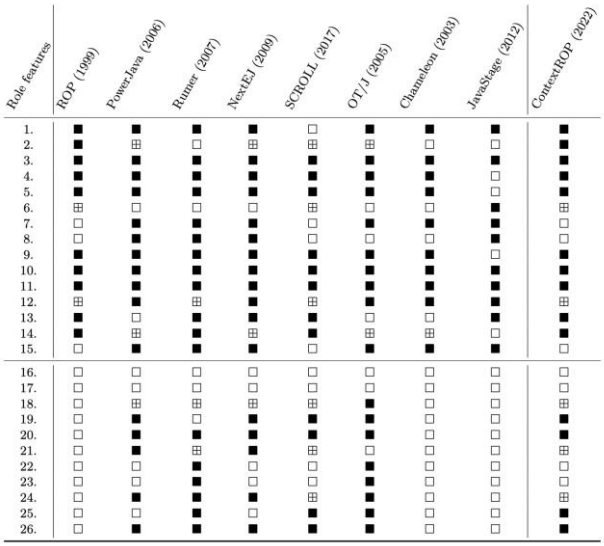

Figure 4: Assessment of approaches with regards to developing roles at runtime using 26 classifying features taken from [10] [11]. Features are completely supported (■), partially supported (⊞), and not supported (□) features.

14https://eips.ethereum.org/EIPS/eip-2535

15https://solidity-by-example.org/delegatecall/

A detailed list of the role features from [10] [11]:

1. A role comes with its own properties and behavior:
2. Roles depend on relationships:
3. An object may play different roles simultaneously
4. An object may play the same role several times, simultaneously
5. An object may acquire and abandon roles dynamically.
6. The sequence in which roles may be acquired and relinquished can be subject to restrictions.
7. Objects of unrelated types can play the same role.
8. Roles can play roles
9. A role can be transferred from one object to another.
10. The state of an object can be role-specific.
11. Features of an object can be role-specific
12. Roles restrict access.
13. Different roles may share structure and behavior.
14. An object and its roles share an identity.
15. An object and its roles have different identities.
16. Relationships between roles can be constrained.
17. There may be constraints between relationships.
18. Roles can be grouped and constrained together.
19. Roles depend on compartments.
20. Compartments have properties and behaviors like objects.
21. A role can be part of several compartments.
22. Compartments may play roles like objects.
23. Compartments may play roles that are part of themselves.
24. Compartments can contain other compartments.
25. Different compartments may share structure and behavior.
26. Compartments have their own identity.

Listing 3: Quantitative Evaluation for the Context-based Role Object Pattern (ContextROP)

In Table 1, we see deployment and execution costs to understand the difference between methods in ContextROP implementation. The UUPS and normal methods have already been discussed in previous chapters. In this section, we had a use case that simulates a banking application with a set of investors and borrowers. Borrowers can borrow a certain amount of money from Banking Institution and discharge the debt before the overdue payment. Borrowers and Investors have a creator method that will associate the ContextROP smart contract package to create abstract role types. In the following Table 1, readers can see the deployment and execution costs during the interaction between roles and objects.

The results have been taken from Remix (v0.25.1) with Hardhat Provider by interacting same functions with different methods. The calculation unit has been given as Gas. Deployment cost shows us the cost of contract deployment into the network. Transaction cost refers to the cost of method interaction with a parameter in on

chain environment. Normally, the transaction cost is utilized for sending the contract code to the blockchain, but we did not use that meaning. Execution cost is based on the cost of computational operations.

One of the important results is the deployment cost of EIP-165 for both roles is lower than UUPS Pattern roles. This can be understood because we are using additional libraries to implement UUPS Pattern; however, incresing gas costs can make the development process expensive. Even the execution cost has been doubled while implementing UUPS Proxy since it can solve the contract maximum size problem. Deployment and Execution costs are the initial cost to interact the contract with the blockchain network. Transaction cost should be considered when producing the cost to invoke a specific method. In Table 1, transaction costs of different role methods are similar to each other and one can say that runtime execution cost is not different from each other.

Method	Deployment Cost	Execution Cost	Transaction Cost
EIP-165 (Role Investor)	1333374 gas	1159455 gas	Invest () method - 54123 gas
EIP-165 (Role Borrower)	1467419 gas	1276016 gas	Borrow() method - 54145 gas
UUPS Pattern (Role Investor)	2863718 gas	2490189 gas	Invest() method – 54174 gas
UUPS Pattern (Role Borrower)	2987612 gas	2597923 gas	Borrow() method - 54106 gas

Table 1: Assessment of the gas cost while executing different methods in ContextROP Standard Implementation.

8. Discussions and Conclusion

Contexts and Roles are the modeling nature of programming languages and they can be used for producing key abstractions to model abstract states and behavior. While implementing this pattern, the most prominent feature of the on-chain smart contract programming occurs in non-intrusive dynamic contract behavior without coping with low-level calls such as D*elegateCall*. Even if we realize *DelegateCall* by way of proxy patterns such as diamond standard pattern, unstructured storage pattern, or transparent proxy pattern.

The first finding is that the type-safety can be implemented with Interface Separator (EIP-165) in role-based applications with Solidity programming language. Implementation of proxy pattern with the EIP-165 concept can reduce a great deal of gas cost initial development stage.

Moreover, it can be more flexible to deploy a contract in case of bug fixing and regular maintenance. However, hardcoded *InterfaceCodes* can cause the function selector clashing. To prevent this, a random UUID (Universal Unique Identifier) can be generated by external libraries.

The second finding is that deployment and execution costs can be reduced through the usage of the EIP-165 standard with a role-based application. Even though there is no difference between the transaction cost of similar function signatures, EIP-165 originated smart contracts can reduce deployment and execution costs more than pro contracts do. However, proxy patterns can solve the contract size limitation, unlike EIP-165 contracts.

The third finding is that most of the role features (14 features) can be completely supported by Solidity programming languages because it is utilizing object-oriented programming techniques. Abstraction of core objects and role subclassing are the fundamental techniques for role-based programming and most smart contract programming languages cannot provide OOP concept except for EOA client source code itself (not in on-chain contract language).

The fourth finding is that trust enabling, and auditable actions are a strong necessity for role-based applications because participants of external clients (roles) should be trustable and auditable. Smart contracts can provide trustable and auditable context-awareness by *Modifier* keyword (function modifiers) *to* role objects by enabling a trust layer on the network.

Additionally, source code of ContextROP can be found at the following link: https://github.com/zointblackbriar/Smart_Contract_Examples/tree/development/Context-Based-CROP-Solidity.

9. Future Work

Different adaptations, test cases, and a set of use cases have already been implemented; however, some parts are still open to research on them. Dynamic contexts can be added to migrate roles from one context to another. Even though there is no consensus on how to create a role, role features from various research studies can be implemented in an object-oriented approach with on-chain smart contracts.

Refactoring roles as subclasses for entity types and hierarchical interface methods can also define role object pattern with context. Different patterns can be compared to aspects of execution and deployment cost in the blockchain network.

Acknowledgment

The author would like to thank his supervisor, Prof. Dr. Uwe Aßmann, for the patient guidance, encouragement, and comments he provided to shape his paper vision. This work is funded by the German Research (DFG) within the Research Training Group Role-Based Software Infrastructures for Continuous Context-Sensitive Systems (GRK 1907, TU Dresden, Software Technology Group, Nöthnitzer Straße 46, 01187, Dresden).

References

[1] Herrmann, S. (2010). Demystifying object schizophrenia.

[2] Khan, S. N.; Loukil, F.; Ghedira-Guegan, C.; Benkhelifa, E. and Bani Hani, A. (2021). Blockchain Smart Contracts: Applications, Challenges, and Future Trends, Peer-to-Peer Networking and Applications: 2901-2925.

[3] Fowler, M. (1997). Dealing with roles, 97.

[4] Bumer, D.; Riehle, D.; Siberski, W. and Wulf, M. (1997). The Role Object Pattern.

[5] Cabot, J. and Raventós, R. (2006). Conceptual Modelling Patterns for Roles, Journal on Data Semantics - JODS 3870: 158-184.

[6] Herrmann, S. (2007). Programming with Roles in ObjectTeams/Java, Applied Ontology 2 : 181-207.

[7] Steimann, F. and Stolz, F. U. (2011). Refactoring to Role Objects: 441–450.

[8] Steimann, F. and Wissensverarbeitung, R. (2000). Role = Interface - A merger of concepts.

[9] Wohrer, M. and Zdun, U. (2018). Design Patterns for Smart Contracts in the Ethereum Ecosystem: 1513-1520.

[10] Steimann, F. (2000). On the Representation of Roles in Object-Oriented and Conceptual Modelling, Data & Knowledge Engineering 35: 83-106.

[11] Kühn, T.; Leuthäuser, M.; Götz, S.; Seidl, C. and Aßmann, U. (2014). A metamodel family for role-based modeling and programming languages: 141-160.

A blockchain-based local energy market

Giacomo Gritzan, Torben Petrow, Michelle Jakobi, Sibille Knodel, Richard Sethmann
Hochschule Bremen, Flughafenallee 10, 28199 Bremen

As part of the research project Trusted Blockchains for the Open, Smart Energy Grid of the Future (tbiEnergy), one of the objectives is to investigate how a holistic blockchain approach for the realization of a local energy market could be accomplished and how corresponding hardware security mechanisms can be integrated. This paper provides an overview of the implemented prototype and describes the system and its processes.

1. Introduction

In the course of the energy transition initiated in Germany, energy grid operators are facing the challenge to restructure the traditional energy grid based on central power plants to a decentralized and distributed power grid that is based on renewable energy sources. [1]

The centralized structure of the traditional energy grid provided predictable plannability to grid operators [1]. Through the rising numbers of prosumers [11] and dependence on the availability of localized renewable energy sources such as wind and photovoltaic, the administration effort grows dramatically. This results in an increasing demand for systems that can coordinate and document these processes in a tamper-proof and traceable manner. Furthermore, the German energy industry is striving for the development of smart grids that use intelligent measuring systems, named Smart Meter Gateways (SMGWs), to react more precise and faster to loads. [2], [3], [4], [5], [6]

The research project tbiEnergy demonstrates how a local blockchain-based energy market could be implemented to handle the described problems.

This is achieved by using controllable local systems (CLS) in form of ARMv7 based single board computers (CLS boxes) taking hardware security mechanisms into account. The blockchain infrastructure is implemented and operated in the cloud using the blockchain framework EOSIO. In order to integrate operators of generation, consumption and storage plants in regard of German national regulations, an existing central registry for power and gas generation plant data – the Marktstammdatenregister (MaStR) of the German Federal Network Agency – is used and augmented with additional functionalities. Energy suppliers act as intermediaries, operating a set of cloud-based microservices and managing the CLS. This local energy market differentiates itself from classic power exchanges and uses flexibilities and capacities of local participants to trade energy between customers and provide the energy supplier an additional option to regulate their own balancing groups. These balancing groups are formed in order to be able to control the supply and demand of electricity within the grids without having to define direct relationships between entry and exit points. [10]

This paper presents a concept for the realization of a blockchain-based local energy market and gives an overview of the necessary systems, processes and components.

2. Concept of a local energy market

The local energy market, developed within the scope of the research project, is limited to customers of the energy supplier and thus to its balancing groups. Currently, the focus is on energy facilities that do not receive subsidized feed-in rates under the Renewable Energy Sources Act (EEG). The energy supplier operates the local energy market and is responsible for the corresponding systems. The platform enables customers to buy and sell energy and at the same time it offers the energy supplier the possibility to manage its own balancing groups. The management obligations, remain on the side of the energy supplier as the balancing group manager. Discrepancies between the forecasts and the matching of energy supply and demand are compensated by the energy supplier, for which it receives processing fees. In order to avoid the shutdown of power plants, the local energy market was divided into a primary market and a secondary market.

On the primary market, customers can buy or sell energy from renewable energy production or storage facilities. Customers can choose between a passive and an active marketing model. In the case of active marketing, the plants are managed by the energy supplier and the customer receives a fixed payment for the flexibility it offers. On the other hand, if the customer opts for active marketing, offers for timeslots can be placed on the local energy market after the plants has been registered. Before timeslot offers are placed on the market, power generation and consumption forecasts are calculated based on the power plant data from the MaStR and utility's weather-based energy production forecast data. These calculations ensure that the energy consumption of consumers is matched with the offered generation quantity or storage capacity prior to acquisition in order to prevent the acquisition of very large quantities of energy due to incorrect input by end consumers or malicious market participants. The primary market is closed one hour before the timeslot starts and the sold timeslots go to the highest bidder. This is where the secondary market comes in: The forecasts are recalculated

and the initial forecast is compared with the new forecast. In the next step, the utility is given the opportunity to buy timeslots that previously have not been sold in order to prevent shutdown of facilities. In addition, the differences between the first and second forecasts are compared by the utility and could be used to supply its balancing group.

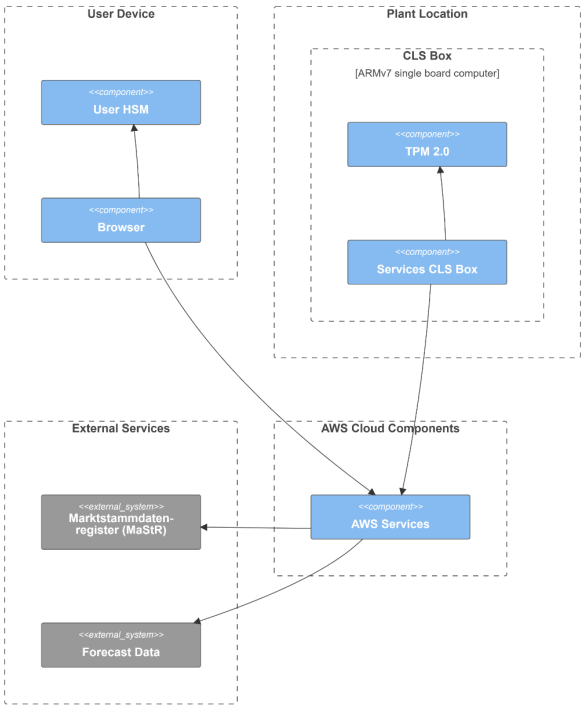

Figure 1 - Architectural Overview

3. Architectural Overview

Figure 1 gives an overview of the designed and prototyped demonstrator. As part of the conceptual design, a microservice approach was developed based on AWS Cloud Services. External services that are utilized are the MaStR of the Bundesnetzagentur and external forecast data e.g., for PV systems and heat pumps. Each plant location is equipped with a CLS box that has a hardware security module (HSM) and is able to communicate with the AWS cloud components using an IoT LTE connection. Interactions between users and the local energy market are processed via a web application. Access to the web application is secured by a user hardware security module. In the following sections, the prototyped components are discussed and an overview of the provided features is given.

4.1 Plant Location / CLS Box

All services on the CLS box are deployed as docker services based on docker-compose files. To allow flexible communication between the service containers they are separated in a docker network. The following subsections describe these various software components running on the CLS box based on *Figure 2*.

4.1.1 CLS-Box-Logic - REST-API

The CLS-Box-Logic is a RESTful web service that is implemented with the Python framework Flask-RESTX. It is designed as the control component of the CLS box. It forms the link between the respective CLS box and the microservice architecture in the AWS cloud. The status of the CLS box can be queried and data from connected devices such as smart meters or CLS devices can be retrieved indirectly via the OpenEMS energy management system (refer section 4.1.4 OpenEMS). In addition, infrastructure services deployable as docker services can be managed. The CLS-Box-Logic ensures that the connection of physically connected CLS boxes and the devices connected to them can be validated before they are added to the local energy market. In addition, it is able to react to events that have been forwarded by the Watcher component of the Blockchain-Connector (refer section 4.1.3 Blockchain-Connector) and process data for example collecting data from OpenEMS or send data to the chain via the Performer component of the Blockchain-Connector.

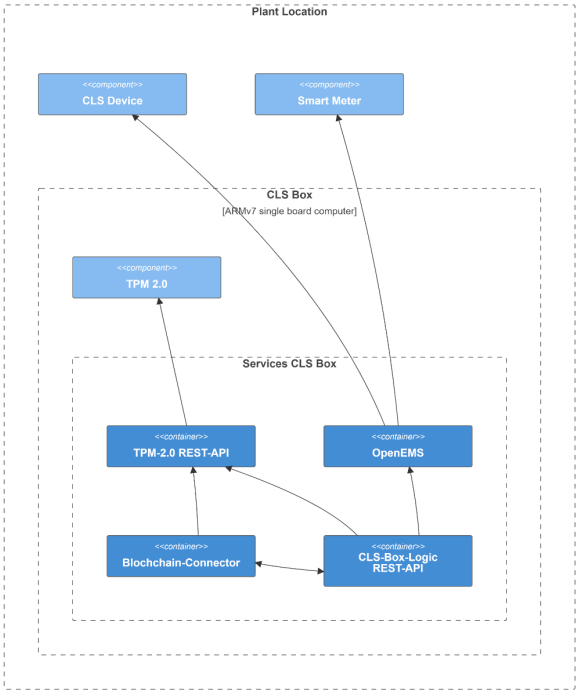

Figure 2 - Plant Location / CLS Box

4.1.2 TPM-2.0 - REST-API

One goal of the project is to secure the key material used for transaction signing on the CLS box. This task is performed by the TPM-2.0 - API. It provides the Trusted Platform Module (TPM) functions for generating key pairs, retrieving public keys and signing transactions via a rest interface secured with AWS Cognito. Currently, a software based TPM is used within the container, which will be replaced by a hardware TPM as part of the further implementation within the scope of the field test.

4.1.3 Blockchain-Connector

The Blockchain-Connector consists of several components that can be used independently. Within the scope of the project, the RESTful web services Watcher and Performer are deployed and utilized on the CLS box.

The Watcher's task is to react to on chain events and forward these events to the CLS-Box-Logic. The CLS-Box-Logic processes an event and decides whether data must be written to the blockchain. In that case, it uses the TPM-2.0 - API to sign the data and then writes it to the chain via the Performer.

As a result, the Watcher and the Performer form the link between the software components of the CLS box and the blockchain.

4.1.4 OpenEMS

"OpenEMS — the Open-Source Energy Management System — is a modular platform for energy management applications. It was developed around the requirements of monitoring, controlling, and integrating energy storage together with renewable energy sources and complementary devices and services like electric vehicle charging stations, heat-pumps, electrolysers, time-of-use electricity tariffs and more." [9]

In context of the project, it allows the development of manufacturer specific modules that can integrate external devices such as smart meters or CLS devices. The data of the connected devices can be retrieved and stored in a local database. The values collected are provided with the help of a RESTful webservice.

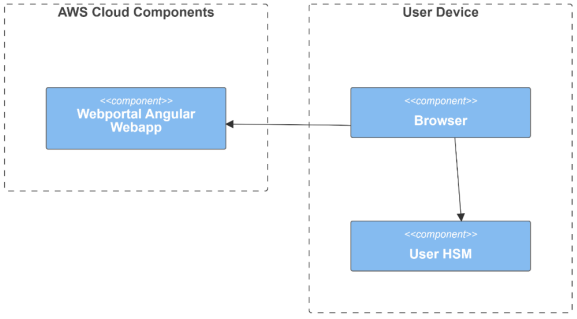

Figure 3 - User Device

5 User Device

The users can interact with the local energy market through the Webportal as shown in *Figure 3*. To authenticate to the Webportal, every participant has a User-HSM that acts as a second factor for the authentication process using the FIDO2 standard and utilizing AWS Cognito in the backend of the Webportal.

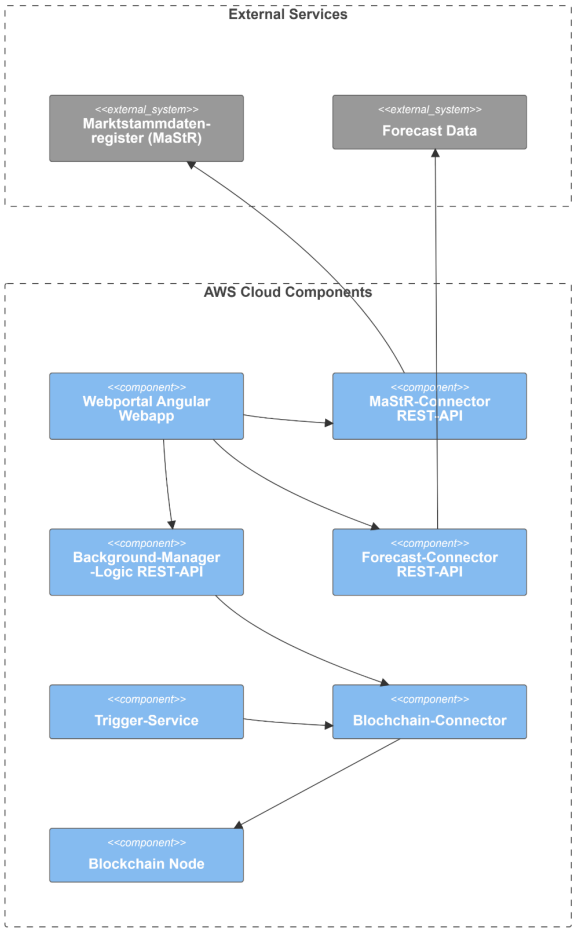

Figure 4 - AWS Cloud Components

6 AWS Cloud Components

The AWS Cloud Components shown in *Figure 4* are based on a set of AWS services. The RESTful webservices and the Webportal are deployed with AWS Fargate, the Trigger Service utilizes AWS Lambda and the Blockchain Nodes are deployed on an AWS -EKS-Cluster. The following subsection will give a description about the functionalities of the individual services.

6.1 RESTful Webservices

The RESTful Webservices are based on the Python framework Flask-RESTX, which is an extension of the Flask framework and integrates e.g., the documentation of interfaces with the help of the so-called OpenAPI specification. It generates OpenAPI documents based on annotations that contain a standardized, language-independent description of the functions provided by the RESTful web services. The OpenAPI document is also used to generate TypeScript clients for the web application and the possibility to display the available functions using Swagger-UI. Each webservice uses the service AWS Cognito for authentication and authorization purposes.

6.1.1 MaStR-Connector

In order to utilize existing databases that store Informations about facilities and their operators, the development of the MaStR -Connector was started. The MaStR contains information about power and gas production plants which must be registered on a mandatory basis and are assigned to clearly identifiable market players. The MaStR provides its data via a SOAP web interface, but this does not allow filtering of all units regarding market actors. The MaStR-Connector was therefore designed as a RESTful webservice that manages synchronized copy of the units of the MaStR, while providing a more flexible way to access the data. Other advantages are the control over the availability of the service and the avoidance of rate limits for data retrieval. The key functionalities of the MaStR-Connector are the synchronization via the MaStR SOAP web interface and the possibility to query units for a specific market actor. The MaStR-Connector retrieves the MaStR data of electricity and gas production plants, market actors such as plant operators, network operators and energy suppliers via the MaStR database and then synchronizes them with its own database. Two methods are used for this purpose:

When initializing the database for the first time, the MaStR Connector populates the database with entries read from XML files that are exported from the MaStR database. After this first initialization, new entries or changes since the last update are retrieved via the SOAP web interface of the MaStR. Subsequently, the MaStR data is parsed from XML into internal data types and stored or updated in a DocumentDB hosted in the AWS cloud environment. These functions are outsourced to Redis jobs to run in the background asynchronously. The current status of the jobs can be inspected by querying corresponding job IDs. The MaStR-Connector allows to query details of the stored units by their MaStR number. Furthermore, all units of a market actor can be retrieved via the MaStR-Connector.

6.1.2 Background-Manager-Logic

Along with the Trigger-Service and the Blockchain-Connector the Background-Manager-Logic represents the management sector within the microservice architecture. In addition to executing background tasks, this area bridges the blockchain network and the other microservices. The RESTful Background-Manager-Logic web service uses an Amazon DocumentDB for data storage. With the help of the collected data foundation of the database, the Background-Manager-Logic can provide the necessary auxiliary functions for the different user roles. For the administrative user, these functions include adding and querying energy-related components from the database and retrieving the status of the service. Users without extended usage rights for the background-manager-logic are given the opportunity to register their own units on the local energy market, place offers and bid on offers. These requests are forwarded to the Performer component of the Blockchain-Connector that executes the corresponding smart contracts to write the data to the blockchain.

6.1.3 Forecast-Connector

The Forecast-Connector is a RESTful web service that processes and provides forecasts and secures the balancing group of the local energy market against manipulations. These forecasts are calculated estimates of the power consumption and production over time periods (timeslots) of 15 minutes for a set of units from the MaStR. The forecast data is created by the energy supplier and uploaded daily to an Amazon Elastic File System (EFS) volume in the AWS cloud. The Forecast-Connector then extracts the forecast data and migrates the contained forecasts and timeslots into its own database. The imported timeslots and their affiliated forecasts can then be retrieved via REST routes.

6.2 Webportal

The Webportal is a responsive web UI based on web application framework Angular, which acts as an interface to the local energy market for consumers, plant operators, the energy supplier as well as administrators. Users are authenticated using credentials and a user HSM. Depending on their authorization level, users are offered different functionalities. Users holding administrative privileges are able to check the status of all associated microservices. They are also able to link physically attached hardware components such as CLS boxes, meters and units in order to provide users access to the local energy market as shown in Figure *5*.

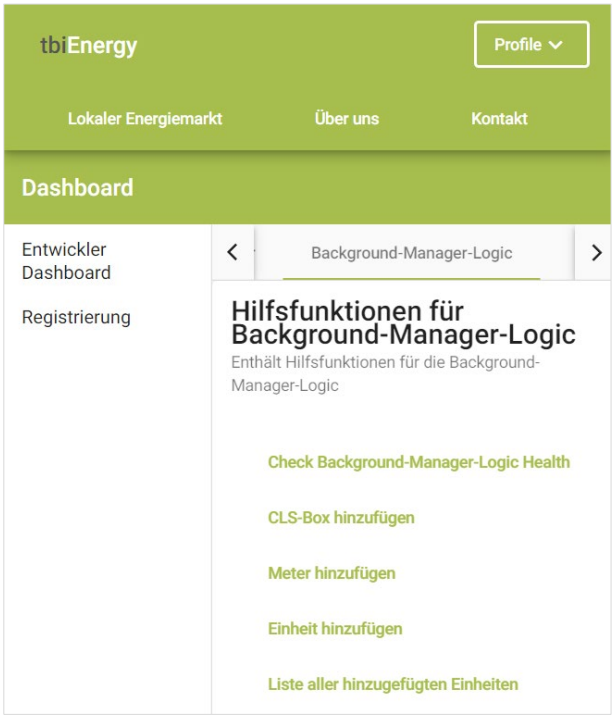

Figure 5 - Developer Dashboard Webportal

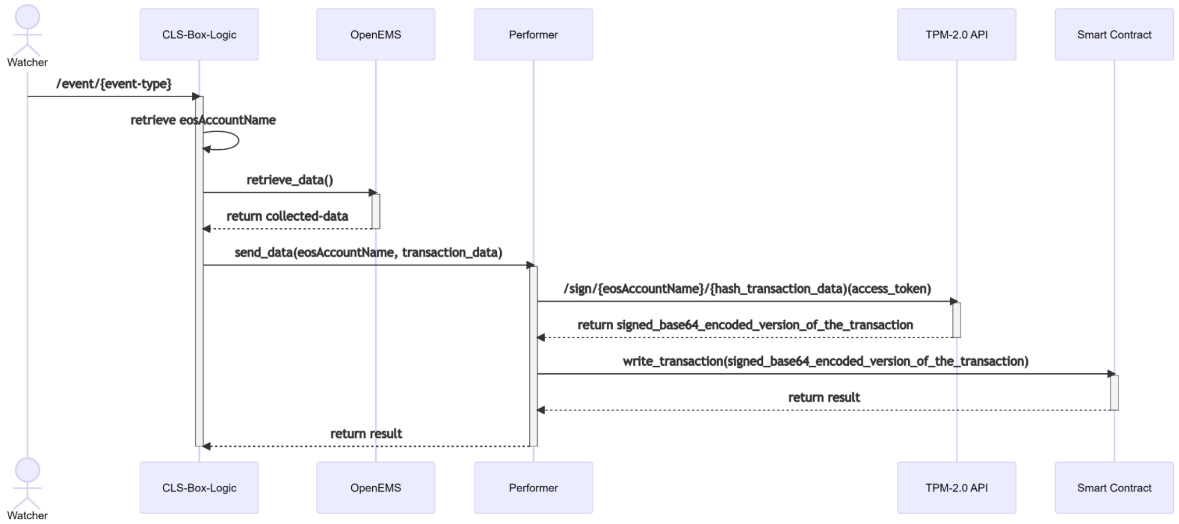

Figure 6 - Process of signing and sending data based on a triggered event

Based on these created links, users are able register their own units and place offers on the local energy market. Also, the energy supplier is able to get an overview over its balancing group. The required functionalities are provided by the web portal using the connected microservices in the backend (Forecast-Connector, Background-Manager-Logic, MaStR-Connector, CLS-Box-Logic instances).

6.3 Trigger-Service

The Trigger-Service is tasked with triggering the execution of functions of other system components under certain conditions. In specified time intervals it requests the synchronization operations of the MaStR-Connector, the update of the Forecast-Connector and generation of events through the Blockchain-Connector. The requests are sent by AWS Lambda functions which in turn are executed by AWS EventBridge rules that check for the preset time periods expiration.

6.4 Blockchain Node

The blockchain used within the project is the open-source platform EOSIO which uses the consensus mechanism “delegated Proof of Stake (dPoS)”. EOSIO executes industrial-scale blockchains with the support of smart contracts and the possibility to build private blockchain networks. [7], [8]

7 Securing the signing of transaction data

Figure *6* describes the process when a specific send_data event is triggered by the Trigger-Service. The Watcher on the CLS box reacts to this event and calls the CLS-Box-Logic that loads the eosAccountName generated within an initial registration process. During the next step the data for the corresponding meter or CLS device is received from the OpenEMS system and sent to the Blockchain Connector component Performer. The Performer sends the hash of the transaction data and the corresponding eosAccountName to the TPM-2.0 API which signs the transaction with the connected TPM 2.0. The signed and encoded version of the transaction is then passed back to the Performer which writes it to the chain. Doing this, the transaction signing process on CLS box has been secured by the utilization of the HSM. The private-key of the keypair initially created within the TPM-2.0 API thus, never leaves the TPM. A malicious attacker would therefore have to gain physical access to the system locations in order to transfer malicious data in the name of an CLS box. Consumption or generation data of the Smart Meters or CLS devices connected to the CLS boxes can thus only be transmitted to the blockchain with the key material generated on the CLS box within the TPM 2.0 REST-API and it is not possible to extract the private keys from the TPM.

8 Conclusion

Within the project, a concept for a local energy market was successfully developed and hardware security could be securely integrated into the CLS box and the Webportal. To validate the technical feasibility, a prototype was created, and its components have been described. During the implementation phase, we learned, that using the blockchain also requires some traditional components, such as RESTful web services and databases, to manage the infrastructure components and process the data before it could be written to the blockchain. Data tampering security has also been implemented using TPM 2.0 on the CLS box and authentication with the user HSM within the web frontend. The presented prototype implements the critical system processes that will be validated in the next steps of the project within a field test. In conclusion, the developed concept of a local energy market and application of hardware security can contribute to the desired energy transition in the German smart grid.

Acknowledgements

The authors would like to thank the German Federal Ministry of Economic Affairs and Climate Action (BMWK) for the funding and all tbiEnergy project partners for the good cooperation.

References

[1] Oliver D. Doleski. Die Energiebranche am Beginn der digitalen Transformation: aus Versorgern werden Utilities 4.0. Oliver D. Doleski Fiduiter Consulting Ottobrunn, Deutschland, 2017, S. 842. ISBN: 978-3-658-15737-1. DOI: 10.1007/978-3-658-15737-1. URL: http://dx.doi.org/10.1007/978-3-658-15737-1_38.

[2] Florian (Blockchainbundesverband) Glatz. Stellungnahme des Blockchain Bundesverband: Fragen für das Fachgespräch zum Thema Blockchain im Ausschuss Digitale Agenda. 2018. URL: https://www.bundestag.de/resource/blob/580950/6f592a83b376199a092e1616eaba5402/A-Drs-19-23-028-Glatz-data.pdf (visited 21. 02. 2019)

[3] H Leopold OVE und T Bleier OVE. "Innovationsdynamik durch Sicherheit im Smart Grid". In: 131 (2014), S. 79–84. DOI: 10.1007/s00502-014-0202-4. URL: https://link.springer.com/content/pdf/10.1007%2Fs00502-014-0202-4.pdf (Visited 17. 02. 2019).

[4] Dennis Laupichler, Stefan Vollmer, Holger Bast und Matthias Intemann. "Das BSI-Schutzprofil: Anforderungen an den Datenschutz und die Datensicherheit für Smart Metering Systeme". In: DuD 35.8 (2011), S. 542–546. ISBN: 1614-0702. DOI: 10.1007/s11623-011-0134-7. URL: https://link.springer.com/content/pdf/10.1007%2Fs11623-011-0134-7.pdf.

[5] Arbeitsgruppe 2 des Nationalen IT-Gipfels (AG2). Nutzen und Anwendungen intelligenter Energienetze Arbeitsgruppe 2 Vernetzte Anwendungen und Plattformen für die digitale Gesellschaft. 2015. URL: https://div-konferenz.de/app/uploads/2015/12/141218_AG2_UAG- IN_Nutzen_Anwendung_Energie.pdf (visited 02. 03. 2019)

[6] Bundesamt für Sicherheit in der Informationstechnik (BSI). Das Smart-Meter-Gateway - Cyber-Sicherheit für die Digitalisierung der Energiewende. Bonn, 2018. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Smart-Meter-Gateway.pdf?__blob=publicationFile&v=6 (Visited 19. 04. 2019).

[7] EOSIO. EOS.IO Technical White Paper v2. 2018. URL: https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md#consensus-algorithm-bft-dpos (visited 04. 08. 2022).

[8] EOSIO. EOSIO for developers. 2022. URL: https://eos.io/for-developers/ (visited 04. 08. 2022).

[9] OpenEMS // Docs. 2022. URL: https://openems.github.io/openems.io/openems/latest/introduction.html (visited 05. 08. 2022).

[10] A. Schwintowski, Hans-Peter; Scholz, Frank; Schuler, Handbuch Energiehandel, 4., völlig. Erich Schmidt Verlag, 2018.

[11] BMWI. Was ist ein "Prosumer"?. 2016. URL: https://www.bmwi-energiewende.de/EWD/Redaktion/Newsletter/2016/06/Meldung/direkt-erklaert.html (visited 09. 08. 2022)

Cyberpunk als Frame für institutionellen Wandel durch Blockchain-Anwendungen? Eine Narrative Analyse des Framings in drei Blockchain-Projekten

Jan-Peter Schmitten, Julien Bucher
Technische Universität Chemnitz, Professur für Innovationsforschung und Technologiemanagement, Thüringer Weg 7, 09126 Chemnitz

Diese Studie analysiert die Verwendung von Narrativen in drei Blockchain-Projekten im Hinblick auf institutionellen Wandel. Es wird aufgezeigt, wie Blockchain-Projekte Cyberpunk-Narrative nutzen, um einen institutionellen Wandel herbeizuführen. Ein kontrastierender Fall ohne Cyberpunk-Narrative verdeutlicht die interpretative Offenheit der institutionellen Eigenschaften von Blockchain-Technologien im Wettbewerb um Deutungshoheit. Die Untersuchung vertieft das Verständnis der Rolle fiktionaler Erzählungen für das Framing von Innovationen im Kontext institutionellen Wandels und zeigt, dass Greimas' Aktantenmodell für die Frame-Analyse geeignet ist.
(Eine umfangreichere Version dieses Artikels in englischer Sprache befindet sich gerade unter Begutachtung beim International Journal of Technology Management)

1. Einleitung

Im Zuge der internationalen Bankenkrise im Jahr 2009 eingeführt, ist die Entstehungsgeschichte von Blockchain-Technologien eine Geschichte vom Versagen des Bankensystems und der gescheiterten Versprechen von Freiheit und Gleichheit von Wissen des früheren Internets [1,2]. Blockchain-Technologien versprechen das verlorene Vertrauen wiederherzustellen indem sie zuverlässige, unveränderliche und transparente Transaktion von Werten und Informationen unter gleichberechtigten Peers ermöglichen. Intermediäre, die bisher Vertrauen zwischen Interaktionspartnern hergestellt haben, sollen dadurch überflüssig werden [3,4]. Banken, Clearing-Häuser und mächtige Plattform-Organisationen die den Konzernriesen aus dem Cyberpunk der 1980er Jahre gleichen, sollen durch Blockchain-Anwendungen ersetzt werden [5,6]. So erklärt etwa Vinay Gupta, Mitgründer von Consensys, einem bedeutenden Unternehmen für Blockchain-Technologien, dass wir diese und die Programmierer dahinter nur verstehen können, wenn wir Cyberpunk verstehen [7].

Diese Studie analysiert die Verwendung von Cyberpunk-Narrativen anhand von drei Blockchain-Projekten im Hinblick auf institutionellen Wandel. Wir gehen davon aus, dass Narrative als Frame für die Interpretation aktueller institutioneller Arrangements durch Blockchain-Projekte und als Mittel für die Adoption der Anwendungen dienen und stellen folgende Forschungsfragen:

- Wie werden Narrative verwendet, um spezifische Blockchain-Anwendungen im Hinblick auf institutionellen Wandel zu framen?
- Was sagen diese Frames über die Werte und Überzeugungen in Bezug auf die derzeitigen institutionellen Arrangements aus?

Theoretischer Hintergrund

Institutioneller Wandel und technologische Innovation

Institutionen sind regelmäßige, wiederkehrende Muster sozialer Interaktion und Organisation. Sie verringern Unsicherheit, indem sie Handlungsoptionen eröffnen und andere verschließen [8–10]. Institutionen sind träge aber wandelbar. Übergangsphasen lassen daher Raum für interpretative Flexibilität und damit für Akteure, die temporäre Unsicherheiten in ihrem Sinne interpretieren [10,11].

Alle Innovationen sind auch institutionelle Innovationen [12]. Innovationen stellen etablierte Werte, Wissensbestände und institutionelle Konfigurationen in Frage [12]. Genau wie Institutionen durchlaufen auch Technologien Phasen, in denen Akteure um die Einschreibung von bestimmten ermöglichenden oder beschränkenden Eigenschaften von Technologien konkurrieren [13–15].

> "Im Wesentlichen betonen diese Vorstellungen von Technik als Institution, dass Technik und technische Arrangements niemals neutral und beliebig nutzbar sind, sondern immer strukturierende und regulierende Eigenschaften haben, die individuelles, organisatorisches oder kollektives Handeln ermöglichen, kanalisieren und mitbestimmen" [13, eigene Übersetzung]

Framing und institutioneller Wandel

Ein Frame ist das Verständnis von Institutionen aus der Perspektive der Akteure, auf den diese ihr Handeln stützen. Wie Institutionen werden Frames sozial geteilt und oft nicht klar definiert, was Raum für Interpretationen lässt.

Der Akt des Framing ist der gezielte Versuch, um für gegebenen Arrangements alternative Interpretationsangebote zu machen und Menschen dazu zu bringen, soziale oder institutionelle Veränderungen herbeizuführen [16].

> „Framing lenkt die Aufmerksamkeit darauf, wie Missstände verstanden und von kollektiven Akteuren strategisch in Ungerechtigkeiten umgewandelt werden, die eine Mobilisierung rechtfertigen, [...]." [16, eigene Übersetzung]

Der Erfolg dieser Versuche hängt u.a. von den Merkmalen der angebotenen Frames, wie ihrer Flexibilität oder dem Grad der Resonanz bei der Zielgruppe ab [17]. Faktoren wie die Glaubwürdigkeit der Bedeutungsgeber oder die „narrative Treue" der Frames, d. h. das Ausmaß, in dem sie mit den Überzeugungen der Zielgruppe, ihren Ideologien und kulturellen Erzählungen übereinstimmen, spielen eine wesentliche Rolle [17].

Science-Fiction und Innovation

Science-Fiction ist ein Genre in dem Wissenschaft und Technologie eine zentrale Rolle bei der Erkundung imaginierter Zukünfte spielen. Die Zukunftsbilder sind dabei in zeitgenössischen Entwicklungen verwurzelt und anschlussfähig für Frames [18,19].

Narrative haben zwei wesentliche Rollen für Innovationen [20,21]: Fiktion kann Innovationen inspirieren und bietet Rahmen, die Innovationen interpretierbar und verständlich machen [22]. Sie werden daher auch genutzt um die Einsatzmöglichkeiten und Folgen von Technologien zu framen.

Menschen sind Geschichtenerzähler, und die von ihnen erzählten Geschichten sind wichtig für die Legitimierung sozialer und politischer Praktiken und haben das Potenzial, Wissensordnungen zu verändern [23,24]. Sie können dazu beitragen etablierte soziale Ordnungen und Praktiken zu stabilisieren oder sie als "Geburtshelfer möglicher Welten" [24,25] zu überwinden.

Cyberpunk Science-Fiction

Cyberpunk entstand als literarische Bewegung mit der Entwicklung des früheren Internets in den 1980er Jahren und brach mit den Traditionen klassischer Science-Fiction der ersten Hälfte des 20. Jahrhunderts. Bücher wie "Neuromancer" von William Gibson [26] und der Film "Bladerunner" [27], mit seiner düsteren Bildsprache, gelten als prägend für die zentralen Elemente und die Ästhetik des Genres.

Cyberpunk-Autoren reflektierten über Entwicklungen und Veränderungen in ihrer politischen, kulturellen und technologischen Umwelt, um deren mögliche Folgen „20 Minuten in die Zukunft" zu extrapolieren [5,6,28,29]. Anstelle von Technologien und ihren möglichen Folgen rücken die von Technik durchdrungenen Institutionen und die von ihnen betroffenen Menschen in den Mittelpunkt der Erzählungen. Zentrale Themen sind „Daten als Ware", künstliche Intelligenz, Überwachungsstaat und Bürokratie, sozialer Verfall und Ungleichheit, Umweltzerstörung sowie die Rolle und Macht globaler Megakonzerne, wobei beide Seiten der Konflikte dieselben Technologien nutzen [5,6,28]. Die Protagonisten richten sich mit subversiven, oft illegalen, meist ethischen, manchmal ritterlichen und in der Regel kreativen Aktionen gegen Unternehmen oder Regierungsbehörden [6].

Cyberpunk ist aufgrund seiner dystopischen Visionen, die sich zumindest teilweise bewahrheitet zu haben scheinen, auch heute noch relevant. Er ist Teil des soziotechnischen Imaginären von heute und hat sich seit seinen Anfängen zu einer multimedialen Kultur entwickelt.

Vom früheren Internet zu Blockchain-Technologien

1993 wurde das World Wide Web der Öffentlichkeit zugänglich gemacht. [30]. Es erleichterte die Kommunikation und Koordination der Bewegung für freie und quelloffene Software die bereits in den 1980er Jahren florierte und deren Geist auch bei den Internetpionieren der frühen 1990er Jahre präsent war. Sie erkannten das Potenzial des Internets für eine freiere und demokratischere Gesellschaft. Diskussionen über den Zugang und die Befähigung zur Nutzung und Erstellung von Software in der Open-Source-Gemeinschaft wurden auf Informationen im Internet ausgedehnt: "Das World Wide Web. Sollte ein Sammelplatz für Informationen werden. Eine weltweite Plattform für kritischen Austausch und Dialog." [31].

In den frühen 2000ern wandelte sich das WWW zu einem Medium, das immer mehr Möglichkeiten zur Interaktion bot [32] und den Aufstieg von Unternehmen wie Amazon, Alphabet, Meta und YouTube mit sich brachte. Während diese Unternehmen vieles erleichtert haben, basieren ihre Geschäftsmodelle zum großen Teil auf der Ausbeutung der Daten ihrer Nutzer und haben zu Quasi-Monopolen geführt, die den demokratischen Idealen des früheren Internet entgegenstehen [33].

Hoffnung darauf die verlorenen Träume des früheren Internet doch noch zu verwirklichen, brachten Blockchain-Technologien. Im Zuge der globalen Finanzkrise 2008 wurden sie erfunden, um elektronisches Bargeld zu ermöglichen [2]. Sie ermöglichen die eindeutige Registrierung und Validierung von Daten und deren Eigentümer, den Schutz ihrer Integrität und die eindeutige Übertragung von einem Nutzer zum anderen [2,34]. Neben Kryptowährungen ermöglichen sie viele Anwendungen, die zu einem breiten Interesse geführt haben [35–38].

Blockchain-Technologien werden häufig als neue Grundlagen- oder Transaktionstechnologien angepriesen, die die Produktivität oder Effizienz verbessern können [39]. Aufgrund ihres Potenzials für neue Formen wirtschaftlicher Koordination schlagen Davidson et al. [39] vor, sie eher als institutionelle Technologien zu interpretieren, die bestehende Institutionen verändern, ergänzen oder ersetzen könnten [39–41]. Ein Teil des Enthusiasmus für Blockchain-Technologien rührt vom Geist der Open-Source-Softwarebewegung her, der in vielen Blockchain-

Projekten ebenso präsent ist, wie im früheren Internet [42]. Aus dieser Perspektive leben wir in einer Cyberpunk-Gegenwart und Blockchain-Technologien versprechen diese trostlose Realität in eine bessere Zukunft verwandeln zu können [4,43].

Methode

Mittels eines Fallstudiendesigns sucht diese Studie die „semantischen Geister" [44] des Cyberpunks, die in den Narrativen von Blockchain-Projekten enthalten sind und als Frames verwendet werden [45–47].

Wir nehmen an, dass Blockchain-Projekte von Markteinsteigern [48] die Cyberpunk Elemente verwenden, dies tun, um ihre Adoption mit dem Ziel institutionellen Wandels zu fördern [49,50]. Bei Projekten etablierter Unternehmen ohne Cyberpunk-Elemente, gehen wir von keinem Interesse an grundlegendem institutionellem Wandel aus und dass sie Narrative verwenden, die Blockchains als komplementäre Technologien darstellen [14,39,40].

Durch ein theoretisches Sampling wurden zwei repräsentative und ein kontrastierender dritter Fall ermittelt [47]. Relevante Daten wurden mit Hilfe einer Online-Inhaltsanalyse [51,52] identifiziert und gesammelt und anhand von Greimas' Aktantenmodell der narrativen Analyse ausgewertet [53,54].

Narrative Analyse

Erzählungen sind zwischen Vergangenheit, Gegenwart und Zukunft angesiedelt und werden geteilt, um eine Botschaft zu vermitteln [55, nach 56]. Um die normative Botschaft zu vermitteln, konzentrieren sich Erzählungen auf die relevanten realen oder fiktiven Ereignisse. Dieses Grundverständnis gilt für individuelle Geschichten, die in lockeren Gesprächen erzählt werden, für Erzählungen in institutionellen Zusammenhängen, in sozialen Bewegungen und auch für fiktionale Erzählungen [57–59].

Aufgrund ähnlicher Ziele und verfügbarer Daten folgen wir Biegoń [60,61] bei der Wahl des Greimas'schen Aktantenmodells für die Analyse [54,60–62].

Das Greimas'sche Aktantenmodell unterscheidet 6 Aktanten, die in Beziehung zueinander stehen und auf drei Achsen angeordnet sind (siehe Abbildung 1). Aktanten können Menschen sein, aber auch „andere aktive und inaktive Kräfte, wenn sie eine bestimmte Rolle in der Geschichte übernehmen" [61,zitiert nach 63, eigene Übersetzung].

Sender und Empfänger befinden sich auf der Achse der Übertragung/des Wissens, auf der ein Sender das Subjekt auffordert, eine Verbindung mit einem Objekt zu suchen. Der Sender stellt hierbei die treibende Kraft dar, die die im Text aktiven Werte in Bewegung setzt. Der Empfänger ist die Entität, die von einer erfolgreichen Verbindung zwischen dem Subjekt und dem Zielobjekt auf der Achse des Begehrens profitieren würde. Die dritte Achse ist die Achse der Macht, verkörpert durch Helfer und Gegner des Subjekts. Entlang dieser Achse manifestiert sich der Konflikt um die Wertestruktur einer Erzählung, die durch die Verbindung von Subjekt und Objekt verwirklicht würde [53,54,61,60].

Abbildung 1: Aktantenmodell [53,54,61,60,64]

Um das Aktantenmodell für die ausgewählten Fälle zu ermitteln, haben wir das von Hébert vorgeschlagene dreistufige Verfahren angewandt [24,53]. Zunächst muss die allgemeine Handlung eines Textes identifiziert oder ausgewählt werden (1), denn sie gibt die Achse des Begehrens zwischen Subjekt und Objekt im Zentrum des Modells vor (2). In einem dritten Schritt müssen die verbleibenden Aktanten identifiziert und in Bezug auf die Aktanten auf der Achse des Begehrens begründet werden (3) [53].

Da Blockchain-Anwendungen Dienstleistungen anbieten, setzen wir das Zielpublikum mit dem Subjekt des jeweiligen Narrativs gleich und das Objekt mit dem Ziel, was das Subjekt (vermeintlich) erreichen will. Das angebotene Produkt ist Helfer bei der Erreichung dieses Ziels und wird gegen die „Gegner" ins Feld geführt.

Das Aktantenmodell ermöglicht die Identifikation relevanter Einheiten in den Erzählungen, ihrer Beziehungen zueinander sowie der Kernaspekte der Frames, ähnlich typischen Methoden der Frame-Analyse [65].

Ergebnisse

Die ausgewählten Projekte – das Cellarius-Netzwerk und das Erasure-Protokoll als Cyberpunk-Projekte und als Kontrastfall TradeLens – haben oder hatten ihren Sitz in den USA und wurden zwischen 2017 und 2020 gegründet. Beide Cyberpunk-Projekte nutzen eine öffentliche Blockchain und implementieren ihre Anwendungen auf

der Ethereum-Blockchain, während TradeLens die Hyperledger Fabric Blockchain nutz. Hyperledger Fabric wird von der Linux Foundation mit Beiträgen mehrerer Unternehmen, darunter IBM, als Open-Source-Projekt entwickelt. TradeLens selbst ist proprietär, während beide Cyberpunk-Fälle zumindest teilweise quelloffen sind oder planten, ihre Codebasis auf Open-Source umzustellen.

	Cellarius-Netzwerk	**Erasure Protokoll**	**TradeLens** (IBM, Maersk)
Ursprungsland	USA (New York)	USA (San Francisco)	USA (Jersey City, NJ)
Gegründet	2017-2018	2020	2018
Status	Eingestellt (Sep. 2019)	Aktiv	Aktiv
Art der Blockchain	Öffentlich	Öffentlich	Zugangsbeschränkt
Blockchain-Netzwerk	Ethereum	Ethereum	Hyperledger Fabric
Open-Source Status	Proprietär (Open-Source angekündigt)	Teilweise Open-Source	Proprietär
Analysierte Dokumente	Cellarius Homepage, Cellarius Whitepaper (PDF), 4 Blog-Artikel, Cellarius community guidelines (PDF)	Erasure.world Homepage, Code readme (GitHub), Smart-Contract readme (GitHub), Journalistischer Artikel	TradeLens Homepage, TradeLens Dokumentation, TradeLens Produkt-präsentation (39 m Konferenzbeitrag + Diskussion)

Tabelle 1: Fallübersicht

Das Cellarius-Netzwerk

Das inzwischen eingestellte Cellarius-Netzwerk [66] betonte ausdrücklich die Rolle von Science-Fiction und Cyberpunk für Innovation und Blockchain-Technologien [67,68]. Kurz vor dem Launch von Cellarius erklärte Vinay Gupta, Mitbegründer von Consensys, der Muttergesellschaft von Cellarius, dass man Cyberpunk-Literatur verstehen muss, um Blockchain und die Blockchain-Entwicklergemeinschaft zu verstehen [7]. Cyberpunk habe die Entwickler dazu inspiriert, dezentrale Lösungen für Probleme zu entwickeln, die heute von zentralisierten Entitäten und Netzwerken gelöst werden. Das Cellarius-Netzwerk stellte sich als das erste multinationale, medienübergreifende Franchise vor, das von seinen Schöpfern und Fans kontrolliert werden sollte. Es sollte Geschichten, Filme, Spiele und mehr umfassen, die in einer gemeinsamen Cyberpunk-Zukunft spielen, die positiver als der Cyberpunk der 1980er Jahre sein sollten [66,69]. Ziel sei es, die von zentralen "Monolithen" beherrschten Medien zu dezentralisieren, die auf Gewinn ausgerichtet hauptsächlich "sichere Kunst" produzieren und nicht auf Befreiung abzielen [43,70].

Der Start von Cellarius wurde erstmals am 17. Oktober 2017 auf ihrer Website angekündigt. Im Jahr 2018 war eine Menge Aktivität zu beobachten, bevor die Website im September 2019 eingestellt wurde [71].

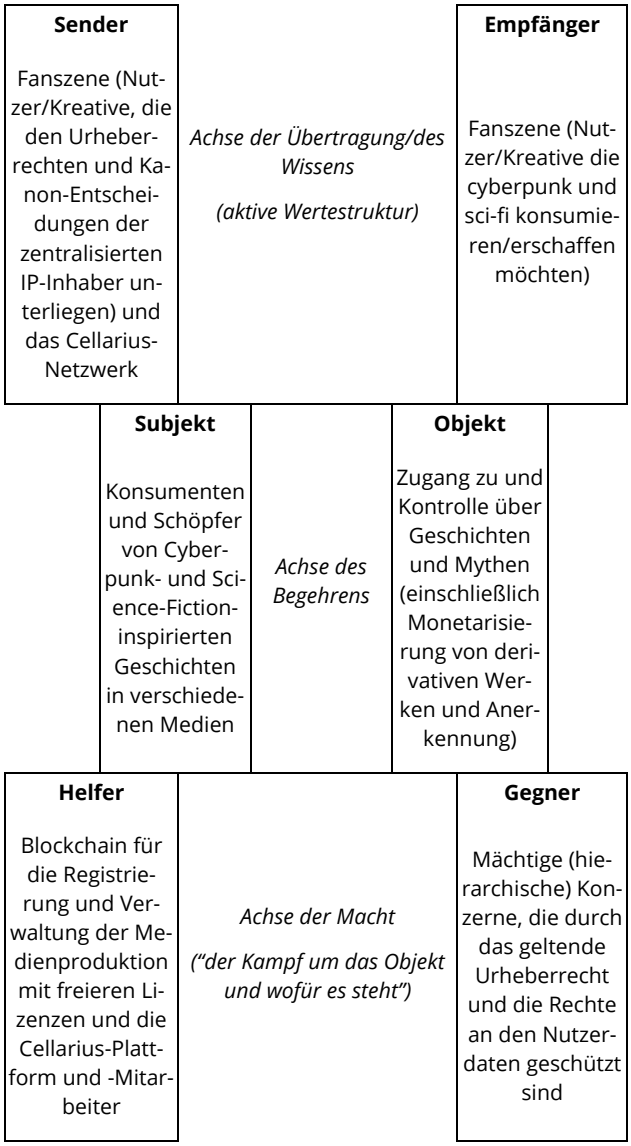

Abbildung 2: Cellarius-Netzwerk Aktantenmodell

Mit einer wärmeren Farbpalette und einem positiveren Ausblick als ihre dystopischen Vorgänger [68], war es das Ziel von Cellarius, Fans und Künstlern mehr Kontrolle über die Franchises zu geben, die sie konsumieren und für die sie Kunst schaffen [72] .

> "Das Cellarius-Universum (CX) ist ein originelles, medienübergreifendes Cyberpunk-Franchise, dass die Blockchain-Technologie und nutzergenerierte Inhalte nutzt, um eine kollaborative, von Fans kuratierte Geschichte zu schaffen. [...] Es ist auch ein kollektives Storytelling-Projekt, dessen Inhalt und Konturen von der Community gestaltet werden." [73, eigene Übersetzung]

Das Subjekt von Cellarius' Narrativ sind Konsumenten und Schöpfer von Cyberpunk-Medien mit dem Ziel, das

Franchise und die Fanszene, der sie angehören, zu besitzen, zu kontrollieren und dazu beizutragen oder in anderer Weise davon zu profitieren (siehe Abbildung 2).

Die Gegner dieses Bestrebens sind die derzeitigen Urheberrechtsgesetze, die um mächtige, hierarchische Konzerne und Inhaber von geistigem Eigentum aufgebaut sind, die die Inhalte kontrollieren. Diese Kontrolle führt nach Cellarius zu "sicherer Kunst" gegen den Willen der Community und zu einer ungerechten Behandlung von Urhebern und Fans. Diese haben häufig keine Möglichkeit, Anerkennung oder faire Bezahlung zu erhalten und es ist ihnen teilweise verboten, derivative Werke zu schaffen. Blockchain kann diese etablierten Institutionen und die von ihnen verursachten Probleme lösen, indem es nicht veränderbare Einträge von Kunstwerken erlaubt und neue Formen der Governance eines Franchise ermöglicht. Künstler und Fans sollten Anteile kaufen und über einen Kernkanon abstimmen können, der unter der Kontrolle der Gemeinschaft entwickelt wird. Restriktive Lizenzen sollen durch freizügige Lizenzen ersetzt werden, die von Open-Source- und Creative-Commons-Konzepten inspiriert sind.

Der Sender ist in diesem Fall die Fanszene, die von zentralisierten Rechteinhabern unterdrückt wird. Das Cellarius-Netzwerk verstand sich als Vorreiter für eine demokratischere und gerechtere Art der Verwaltung und Kontrolle geistigen Eigentums, von der Verbraucher, Urheber und die Gesellschaft insgesamt profitieren würden.

Das Erasure-Protokoll

Das Erasure-Protokoll wurde als Fall ausgewählt, weil Cyberpunk-Elemente hier in zahlreichen Illustrationen auf der Homepage und in Referenzen in Werbevideos von Numerai zu finden sind: so z. B. eine Skyline voller Leuchtreklamen oder eine Person, die ein VR-Headset trägt und dabei mit Computern aus verschiedenen Epochen verbunden ist [74]. Numerai ist eine von drei Anwendungen, die das Erasure-Protokoll nutzen und kann als ein Hedgefonds beschrieben werden, der über datenwissenschaftliche Wettbewerbe Marktprognosen crowd-sourced [75]. Numerai besteht seit 2016, während das quelloffene Erasure-Protokoll erst 2020 veröffentlicht wurde [76].

Ziel von Erasure ist es, das Problem schlechter Informationen zu lösen, das sich aus den durch Wettbewerb im Finanzwesen verursachten Informationssilos und aus dem verschwindend geringen Preis für die Verbreitung schlechter, falscher oder unerwünschter Informationen im Internet ergibt. Ersteres führt zu ineffizienten Redundanzen bei der Datenerfassung und -analyse und verhindert, dass wertvolle Signale aufgrund von Zugangsbeschränkungen wahrgenommen werden. Letzteres bezieht sich auf die Belastung von sozialen Medien, Dating-Apps und anderen Web-2.0-Phänomenen, die durch Bots und andere unlautere Akteure im Internet stark belastet sind, was das Filtern und die Überprüfung von Informationen erschwert.

Erasure erhöht die Barriere für schlechte Informationen, indem ein Einsatz für die bereitgestellten Informationen gefordert wird, der verloren geht, wenn die Empfängerpartei mit den erhaltenen Informationen nicht zufrieden ist [74]. Dies ermöglicht Vertrauen zwischen Parteien, die sich gegenseitig nicht kennen. Dies soll z.B. Menschen die Möglichkeit geben, Marktsignale anzubieten, die andernfalls aufgrund mangelnder Reputation und fehlenden Zugangs zu etablierten Institutionen wie Banken keine Chance hätten Gehör zu finden und soll die Kosten für unlautere Informationen hoch setzen.

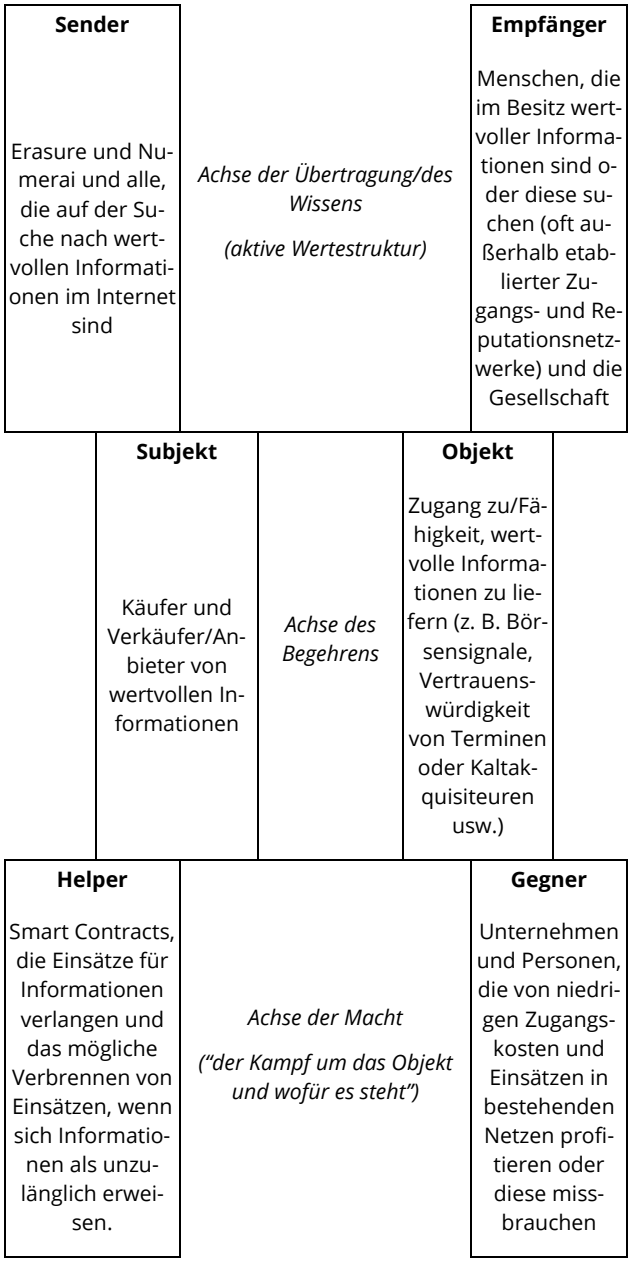

Abbildung 3: Erasure-Protokoll Aktantenmodell

Die allgemeine Handlung von Erasures Aktantenmodell ist der Austausch von Informationen, wobei das Subjekt

bessere Informationen sucht oder schlechte Informationen vermeiden will. Gegner dieses Zugangs zu wertvollen Informationen sind die bestehenden hierarchischen und konkurrierenden Strukturen im Finanzwesen und die geringen Zugangskosten des aktuellen Web 2.0. Diesen wirkt das Erasure-Protokoll entgegen, indem Vertrauen in Informationen erhöht wird. Das aktive Wertesystem ist hier das Recht, wertvolle Informationen senden und empfangen zu können, ohne im Lärm unterzugehen oder Teil exklusiver Zugangs- und Reputationsnetzwerke sein zu müssen. Neben Erasure ist der Absender und Empfänger jeder, der Zugang zu wertvollen Informationen sucht oder diese bereitstellen kann.

Kontrastierender Fall: TradeLens

Im März 2017 kündigten IBM und der Logistikriese Maersk TradeLens an: Eine Blockchain-basierte Plattform für das Dokumentenmanagement in Lieferketten, die im Dezember 2018 auf den Markt kam und rund 1,5 Millionen Ereignisse pro Tag erfasst.

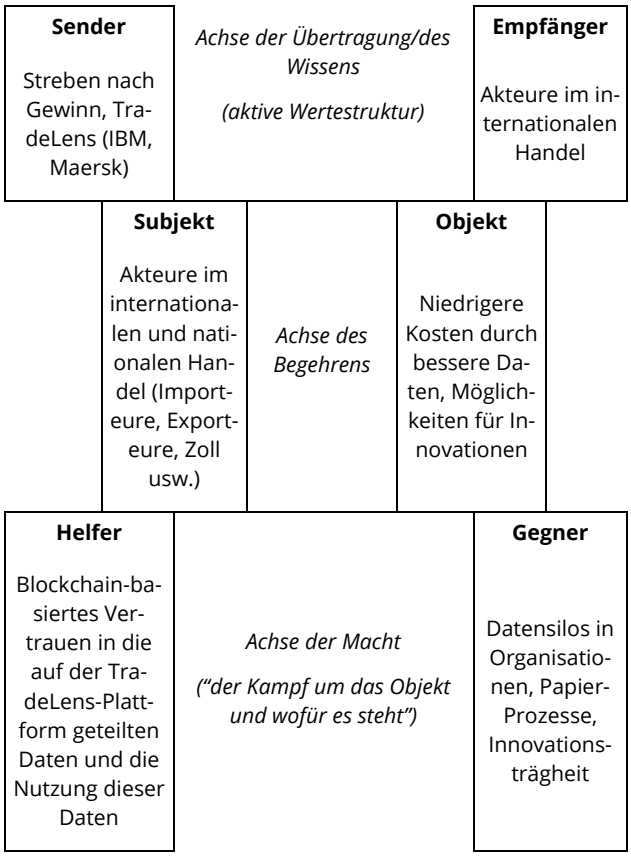

Abbildung 4: TradeLens Aktantenmodell

Obwohl es auf der quelloffenen Hyperledger Fabric [77] basiert, sind die Anwendung und das Blockchain-Netzwerk zugangsbeschränkt und werden von einer intermediären Organisation betrieben, die zwischen 8 und 22 USD pro Container oder Frachtbrief berechnet [77–79]. Das System schafft Vertrauen zwischen den Akteuren im internationalen Handel, die es für den Austausch von Dokumenten und anderen Daten nutzen, die ansonsten in isolierten, oft papiergestützten Systemen mit unterschiedlichen Standards verarbeitet werden würden [80]. Die Verlagerung dieser Prozesse auf eine Blockchain macht sie effizienter, weil Wartezeiten verkürzt werden und das System lernen kann, verschiedene Standards zu integrieren. Auch die Effektivität soll steigen, weil die aus getrennten Silos befreiten Daten nun für Innovationen genutzt werden können [78,79].

Die Subjekte in IBM/Maersks Erzählung sind Akteure im internationalen Handel, die versuchen Kosten durch eine effektivere Daten- und Dokumentenverarbeitung und Möglichkeiten für produktivitätssteigernde Innovationen auf der Grundlage zuverlässiger Versanddaten zu senken [79,80]. Das in diesem Modell aktive Wertesystem ist die Kosten-Nutzen-Optimierung, die von dem übergeordneten Ideal des Gewinnstrebens durch den Akteur TradeLens geleitet wird. Auf der Empfängerseite stehen die Akteure des internationalen Handels und ihre Kunden. Das auf Blockchain basierende Vertrauen in die auf TradeLens geteilten und ausgetauschten Daten und die Nutzung dieser Daten trägt zur Erreichung des Ziels bei, während traditionelle, organisatorische Datensilos und die Abneigung, etablierte Geschäftsabläufe zu ändern, dem entgegenstehen.

Diskussion und Fazit

Wir wollten wissen, wie Narrative verwendet werden um Blockchain-Anwendungen im Hinblick auf institutionellen Wandel zu rahmen, und was die Frames in verschiedenen Blockchain-Anwendungen über die Werte und Überzeugungen in Bezug auf aktuelle institutionelle Arrangements aussagen.

Die ersten beiden Fälle zeigen, wie einige Blockchain-Projekte etablierte Institutionen, die sie für schädlich für die Gesellschaft halten, reflektieren und zu verändern suchen. Durch die Verwendung von Cyberpunk-Elementen versuchen sie ihr Framing dieser Institutionen mit dem angenommenen Framing ihres Zielpublikums in Einklang zu bringen und können als „institutionelle Unternehmer" betrachtet werden, die Merkmale sozialer Bewegungen aufweisen. Wie Bewegungen nutzen sie Frames, um Akzeptanz und Legitimität zu finden und so soziale und institutionelle Veränderungen herbeizuführen [16]. Der kontrastierende Fall stellt nicht die zugrundeliegenden Institutionen des internationalen Handels in Frage, sondern wie dieser auf Ebene von Organisationen organisiert wird und setzt Blockchain-Technologien in komplementärer und nicht substitutiver Weise ein [39].

Die Ergebnisse scheinen die Annahmen von Davidson et al. [39] und Lumineau et al. [40] zu stützen, dass in Blockchain-Technologien das Potenzial gesehen wird, aktuelle Institutionen zu ergänzen, zu verändern oder zu ersetzen. Sie bestätigen die interpretative Flexibilität von Blockchain-Technologien und verweisen auf das Konfliktpotenzial der Konkurrenz um die Deutungshoheit.

Wenn die beiden ersten Fälle als Ausgangspunkt genommen werden können, enthalten sie Hinweise darauf,

dass ihr Erfolg aber weder mit der Verwendung von Cyberpunk-Elementen noch mit ihrem hohen Produktionswert zusammenhängt. Das Cellarius-Netzwerk wurde nach kurzer Zeit wieder eingestellt und das Erasure-Protokoll scheint, abgesehen von dem Hedge-Fond [81], ebenso wenig erfolgreich: Der letzte Tweet von Erasure Bay, einem Informations-Marktplatz, der das Protokoll verwendet, ist bereits von Januar 2021 [82,83].

Möglicherweise sagt die Analyse der zwei ersten Fälle also, wie Vinay Gupta annimt, etwas über die für die Projekte verantwortlichen Personen aus, nicht aber über die Passung von Cyberpunk-Narrativen mit potenziellen Nutzern. Die Attraktivität für Nutzer könnte durch dieses Framing sogar geschmälert sein, wenn man bedenkt, dass Cyberpunk-Science-Fiction ein Nischen-genre mit einem eingeschränkten Publikum ist. Dystopische Narrative scheinen zwar eine gewisse Wirkung auf die politische Meinungsbildung zu haben [84–86] aber vielleicht sind sie nicht die effektivsten Frames, um Nutzer zu gewinnen und institutionelle Veränderungen zu bewirken.

Literaturverzeichnis

[1] Berners-Lee T. One Small Step for the Web…. 2018; Im Internet: https://inrupt.com/blog/one-small-step-for-the-web; Stand: 02.04.2019

[2] Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2009;

[3] Swan M. Blockchain: blueprint for a new economy. First edition. Beijing: Sebastopol, CA: O'Reilly; 2015

[4] Tapscott D, Tapscott A. Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world. New York: Portfolio / Penguin; 2016

[5] Elias H. Cyberpunk 2.0: fiction and contemporary. Covilhã: LabCom Books; 2009

[6] Gözen JE. Cyberpunk Science Fiction. Bielefeld: Transcript; 2012

[7] Vinay Gupta at Michel Bauwens & the Promise of the Blockchain. 2016; Im Internet: https://vimeo.com/161183966

[8] Merton RK. Sozialstruktur und Anomie. In: Sack F, König R, Hrsg. Kriminalsoziologie. Frankfurt am Main: Akademische Verlagsgesellschaft; 1968: 283–313

[9] Nelson RR, Sampat BN. Making sense of institutions as a factor shaping economic performance. Journal of Economic Behavior & Organization 2001; 44: 31–54

[10] Yoshikawa T, Tsui-Auch LS, McGuire J. Corporate Governance Reform as Institutional Innovation: The Case of Japan. Organization Science 2007; 18: 973–988

[11] Thomas LDW, Ritala P. Ecosystem Legitimacy Emergence: A Collective Action View. Journal of Management 2022; 48: 515–541

[12] Rammert W. Technik und Innovation. In: Handbuch der Wirtschaftssoziologie. Springer VS, Wiesbaden; 2017: 415–441

[13] Dolata U, Schrape J-F. Collectivity and Power on the Internet. Cham: Springer International Publishing; 2018

[14] Joerges B, Czamiawska B. The Question of Technology, or How Organizations Inscribe the World. Organization Studies 1998; 19: 363–385

[15] Latour B. Technology is society made durable. Sociological Review 1990; 38: 103–131

[16] Moss DM, Snow DA. Theorizing Social Movements. In: Abrutyn S, Hrsg. Handbook of Contemporary Sociological Theory. Cham: Springer International Publishing; 2016: 547–569

[17] Benford RD, Snow DA. FRAMING PROCESSES AND SOCIAL MOVEMENTS: An overview and Assessment. Annual Review of Sociology 2000; 611-639

[18] Hubble N, Mousoutzanis A, Hrsg. The science fiction handbook. London: Bloomsbury; 2013

[19] James E, Mendlesohn F, Hrsg. The Cambridge companion to science fiction. Cambridge: Cambridge University Press; 2003

[20] Jasanoff S, Kim S-H, Hrsg. Dreamscapes of modernity: sociotechnical imaginaries and the fabrication of power. Chicago; London: The University of Chicago Press; 2015

[21] Sovacool BK, Hess DJ. Ordering theories: Typologies and conceptual frameworks for sociotechnical change. Social Studies of Science 2017; 47: 703–750

[22] Viehöver W. Diskurse als Narrationen. In: Reiner Keller, Andreas Hirseland, Wemer Schneider, et al., Hrsg. Band 1: Theorien und Methoden. Opladen: Leske + Budrich; 2001: 177–206

[23] Lyotard J-F. Randbemerkungen zu den Erzählunge. In: Engelmann P, Hrsg. Postmoderne und Dekonstruktion: Texte französischer Philosophen der Gegenwart. Ditzingen: Reclam; 2021

[24] Viehöver W. Die Wissenschaft und die Wiederverzauberung des sublunaren Raumes. Der Klimadiskurs im Licht der narrativen Diskursanalyse. In: Keller R, Hirseland A, Schneider W, et al., Hrsg. Band 2: Forschungspraxis. Opladen: Leske + Budrich; 2004: 233–270

[25] Ricoeur P, Kearney R. Myth as the Bearer of Possible Worlds. The Crane Bag 1978; 2: 112–118

[26] Gibson W. Neuromancer. 1. Aufl. London: Gollancz; 1984

[27] Scott R, Blade Runner. 1982

[28] McFarlane A, Murphy GJ, Schmeink L, Hrsg. The Routledge companion to cyberpunk culture. London□; New York: Routledge; 2020

[29] TV Tropes. 20 Minutes into the Future. TV Tropes 2022; Im Internet: https://tvtropes.org/pmwiki/pmwiki.php/Main/TwentyMinutesIntoTheFuture; Stand: 28.05.2022

[30] Berners-Lee T. The World Wide Web: A very short personal history. 1998; Im Internet:

https://www.w3.org/People/Berners-Lee/ShortHistory.html; Stand: 30.05.2022
[31] Kepplinger L, Zehetner J. Zurück in die Zukunft des Internets. In: Dobusch L, Hrsg. Freie Netze - freies Wissen: ein Beitrag zum Kulturhauptstadtjahr Linz 2009. Wien: Echo Media Verlag; 2007: 142–158
[32] O'Reilly T. What Is Web 2.0. 2005; Im Internet: http://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html; Stand: 17.08.2016
[33] Zuboff S. Surveillance Capitalism and the Challenge of Collective Action. New Labor Forum 2019; 28: 10–29
[34] Burgwinkel D. Blockchain Technology, Einführung für Business- und IT Manager. Berlin, Boston: De Gruyter Oldenbourg; 2016
[35] Adams R, Parry G, Godsiff P, et al. The future of money and further applications of the blockchain. STRATEGIC CHANGE-BRIEFINGS IN ENTREPRENEURIAL FINANCE 2017; 26: 417–422
[36] Casino F, Dasaklis TK, Patsakis C. A systematic literature review of blockchain-based applications: Current status, classification and open issues. Telematics and Informatics 2019; 36: 55–81
[37] European Commission. Ukraine to use blockchain technology in curtailing corruption when selling government assets » Brave New Coin. Bravenewcoin 2016; Im Internet: https://bravenewcoin.com/news/ukraine-to-use-blockchain-technology-in-curtailing-corruption-when-selling-government-assets/; Stand: 15.05.2018
[38] Thomason J, Bernhardt S, Kansara T, et al. Blockchain for Universal Health Coverage. In: Blockchain Technology for Global Social Change: IGI Global; 2019: 180–200
[39] Davidson S, De Filippi P, Potts J. Blockchains and the economic institutions of capitalism. Journal of Institutional Economics 2018; 1–20
[40] Lumineau F, Wang W, Schilke O. Blockchain governance-a new way of organizing collaborations? ORGANIZATION SCIENCE 2021; 32: 500–521
[41] Reijers W, Coeckelbergh M. The Blockchain as a Narrative Technology: Investigating the Social Ontology and Normative Configurations of Cryptocurrencies. Philos Technol 2018; 31: 103–130
[42] Miscione G, Ziolkowski R, Zavolokina L, et al. Tribal Governance: The Business of Blockchain Authentication. In: Proceedings of the 51st Hawaii International Conference on System Sciences 2018. 2018
[43] Anderson M. Cellarius and the Decentralized Renaissance – ConsenSys Media. 2018; Im Internet: https://media.consensys.net/cellarius-and-the-decentralized-renaissance-f1e2e16c4811; Stand: 02.05.2019
[44] William Gibson. The Gernsback Continuum. In: Sterling B, Hrsg. Mirrorshades: the cyberpunk anthology. New York: Arbor House; 1986
[45] Chaiklin H. Doing Case Study Research. American Journal of Dance Therapy 2000; 22: 47–59
[46] Ridder H-G. The theory contribution of case study research designs. Bus Res 2017; 1–25
[47] Yin RK. Case study research: design and methods. 3rd ed. Thousand Oaks, Calif.: Sage Publications; 2003
[48] Christensen CM. The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail. Boston, MA: Harvard Business School Press; 1997
[49] Andergassen R, Nardini F, Ricottilli M. Innovation diffusion, general purpose technologies and economic growth. Structural Change and Economic Dynamics 2017; 40: 72–80
[50] Rogers EM. Diffusion of innovations. 3rd ed. New York: London: Free Press; Collier Macmillan; 1983
[51] Herring SC. Web Content Analysis: Expanding the Paradigm. In: International Handbook of Internet Research. Springer, Dordrecht; 2009: 233–249
[52] McMillan SJ. The Microscope and the Moving Target: The Challenge of Applying Content Analysis to the World Wide Web. Journalism & Mass Communication Quarterly 2000; 77: 80–98
[53] Hébert L, Tabler J. An Introduction to Applied Semiotics: Tools for Text and Image Analysis. London: Routledge; 2019
[54] Titscher S, Meyer M, Wodak R, et al. Methods of text and discourse analysis. London; Thousand Oaks [Calif.]: SAGE; 2000
[55] Polletta F, Chen PCB, Gardner BG, et al. The Sociology of Storytelling. Annual Review of Sociology 2011; 37: 109–130
[56] Labov W, Waletzky J. Narrative analysis: oral versions of personal experience. Seattle: University of Washington Press; 1967
[57] Fludernik M. An introduction to narratology. London□; New York: Routledge; 2009
[58] Lieblich A, Tuval-Mashiach R, Zilber T. Narrative research: reading, analysis and interpretation. Thousand Oaks, Calif: Sage Publications; 1998
[59] Martens ML, Jennings JE, Jennings PD. Do the Stories They tell get them the Money They Need? The Role of Entrepreneurial Narratives in Resource Acquisition. Academy of Management Journal 2007; 50: 1107–1132
[60] Biegoń D. Specifying the Arena of Possibilities: Post-structuralist Narrative Analysis and the European Commission's Legitimation Strategies: Specifying the arena of possibilities. J Common Mark Stud 2013; 51: 194–211
[61] Biegoń D. Narrative Legitimation: The Capitalist Market Economy as a Success Story. In: Schneider S, Schmidtke H, Haunss S, et al., Hrsg. Capitalism and Its Legitimacy in Times of Crisis. Cham: Springer International Publishing; 2017: 159–189
[62] Beetz J. Latour with Greimas - Actor-Network Theory and Semiotics. 2013;
[63] Greimas AJ, Courtâes J. Semiotics and Language. Indiana, US: Indiana University Press; 1982
[64] Arnold M, Dressel G, Viehöver W, Hrsg. Erzählungen im Öffentlichen: Über die Wirkung narrativer

Diskurse. Wiesbaden: VS Verlag für Sozialwissenschaften; 2012
[65] David CC, Atun JM, Fille E, et al. Finding Frames: Comparing Two Methods of Frame Analysis. Communication Methods and Measures 2011; 5: 329–351
[66] Cellarius. Cellarius - Reshape how stories are told and shared. Join our Alpha now. 2018; Im Internet: https://cellarius.network/; Stand: 10.12.2018
[67] Anderson M. Why Blockchain Needs Sci-Fi Right Now. ConsenSys Media 2018; Im Internet: https://media.consensys.net/why-blockchain-needs-science-fiction-now-5522b3976ffb; Stand: 02.04.2019
[68] Apollo F. Blockpunk: The Cellarius Take on Cyberpunk. Genesis Thought 2018; Im Internet: https://medium.com/genesis-thought/blockpunk-the-cellarius-take-on-cyberpunk-77e4da7dc89d; Stand: 27.03.2022
[69] Genesis Thought Inc. Cellarius Community Guidelines. 2018
[70] Smith RT. Cellarius: The Vision. Genesis Thought 2018; Im Internet: https://medium.com/genesis-thought/cellarius-the-vision-ace11fa29f7a; Stand: 27.03.2022
[71] Cellarius.network snapshots on internetarchive.org. Internet Archive: Wayback Machine 2022; Im Internet: https://web.archive.org/web/20190715000000*/cellarius.network; Stand: 01.06.2022
[72] Genesis Thought Inc. cellarius-white-paper.pdf. 2018;
[73] Genesis Thought Inc. Cellarius Style Guide. 2018; Im Internet: https://cellarius.network/downloads/cellarius-style-guide.pdf; Stand: 02.05.2019
[74] Erasure World Homepage. 2020; Im Internet: https://erasure.world/index.htm; Stand: 12.03.2020
[75] Introducing Numerai Signals. 2020; Im Internet; https://www.youtube.com/watch?v=GWeC2PK4yXQ
[76] Gosselin S. The Erasure Protocol Awakens. Medium 2020; Im Internet: https://medium.com/numerai/the-erasure-protocol-awakens-48a34cc4b5d0; Stand: 20.03.2020
[77] Linux Foundation. Hyperledger – Open Source Blockchain Technologies. 2022; Im Internet: https://www.hyperledger.org/; Stand: 31.05.2022
[78] TradeLens. Solution Architecture - TradeLens Documentation. 2021; Im Internet: https://docs.tradelens.com/learn/solution_architecture/; Stand: 27.03.2022
[79] TradeLens. Supply chain data and docs. 2022; Im Internet: https://www.tradelens.com/; Stand: 27.03.2022
[80] TradeLens. Shipping in the Age of Blockchain. 2019; Im Internet: https://www.youtube.com/watch?v=Xwqo_fwPEJo
[81] Numerai. Im Internet: https://www.numer.ai/; Stand: 04.02.2022
[82] Erasure Bay. Im Internet: https://erasurebay.org/; Stand: 04.02.2022
[83] @ErasureBay. Erasure Bay (@ErasureBay) / Twitter. Twitter 2022; Im Internet: https://twitter.com/ErasureBay; Stand: 01.06.2022
[84] Gierzynski A. The Political Effects of Entertainment Media: How Fictional Worlds Affect Real World Political Perspectives. Rowman & Littlefield; 2018
[85] Mulligan K. Truth in Fiction: The Consequences of Fictional Framing for Political Opinions. 2009;
[86] Young KL, Carpenter C. Does Science Fiction Affect Political Fact? Yes and No: A Survey Experiment on “Killer Robots”. International Studies Quarterly 2018; 62: 562–576

A technical approach for blockchain-based parametric insurance

Tim Käbisch, Lucas Johns
Hochschule Mittweida, Technikumplatz 17, 09648 Mittweida

Humans started using the principles of insurance thousands of years ago when they lived in tribes in smaller villages. If one of the tribe members were injured, the others would take care of him and his family. The basic principle of insurance is several people covering each other against a particular risk. Today, most people in regions like Europe have access to insurance, while many people worldwide still have no access at all. The cost and accessibility may be improved with a blockchain-based parametric approach. The insurance process in a parametric approach is exclusively based on data, and decisions are made objectively. Blockchain is a necessary and integral part of the approach to create transparency and connect the customer's and investor's risk capital. The paper offers an overview of the opportunities and challenges of blockchain-based parametric insurance, a catalog of criteria for such insurance, a description of all components and their interaction for implementation on Ethereum, and a reference implementation of a train delay insurance in Germany.

1. Fundamentals

Insurance is based on the principle that a collective assumes the risk of the individual. The covered risk always needs to be measurable in money amounts. The insured pays a certain amount of money, the premium, to the insurer to receive a payout in the event of a covered loss. The conditions and circumstances under which the insurer makes a payout are set in a contract between the insured and the insurer. This contract is called a policy. The lifecycle of a policy primarily consists of the following sub-steps: an inquiry from the customer, an examination of the inquiry by the insurer, a payment of the premium by the customer, a claim, and a payout. [1] "Manual activities are required in many of the individual sub-steps in the classic insurance business" [cf. 1] (e.g., checking the details of a claim), thus incurring costs and taking a long time. Only about 60% of the premium ends up in the risk pool and is used to cover claims. [2] The remaining portion is used for administrative, distribution, and claim settlement costs, among other things.

The insurance process can be designed more time efficiently and more cheaply with a parametric approach. [3] Parametric insurance uses a purely data-driven process. It uses historical data for the risk assessment and approves a payout to the insured when a predefined triggering event occurs. This reduces the complexity and costs of claim handling and enables full automation of this process. For instance, triggering events can be certain weather conditions or a flight delay. [1]

The combination of parametric insurance and blockchain offers further advantages. [4] Blockchain-based parametric insurance creates transparency and accountability for record keeping, minimizes friction and transaction costs for payment handling, allows efficiency gains with fully automated policies, and enables immediate payouts. Due to the option of storing information regarding policies, claims, and payouts on-chain, a level of transparency is created that would be inconceivable with classic insurance businesses. Furthermore, handling the payment of premiums and payouts on-chain may be a significant efficiency boost. Finally, near-real-time payouts are enabled as no intermediate financial layers are required. [1]

2. Catalog of criteria

An overview of relevant criteria for blockchain-based parametric insurance products is presented in the following section. This catalog of criteria aims to function as a kind of template. By using this catalog, one should be able to quickly verify whether a new use-case idea is suitable for a parametric blockchain-based implementation.

a) Automation: It is essential that the entire process, from signing a policy to verifying a claim and possible payout, can be fully automated. The risk calculation must also be automated. The criterion of automation thus describes the requirement to minimize manual intervention in the process and ultimately offer an efficient policy. For most parametric products, this should be the case.

b) Independent triggers: It is necessary that the trigger value is not provided by the insured itself but ideally by an independent third party. This is to avoid moral hazard, i.e., the malicious exploitation of the insurance. [5] An excellent example is an insurance against natural disasters or general weather events. These cannot be manipulated to one's advantage, so there is no risk of moral hazard. It must be possible to verify the damage without questioning the person concerned. Therefore, the decoupling of the trigger and the policyholder is an essential requirement.

c) Data availability: To constantly offer a policy, the data required must also be continuously available. This includes historical data relating to the individual risk and current data that serves as a trigger. This data must be

available with sufficient reliability. This is important because a lack of recent data means the policy cannot be processed. It is then not known whether a loss has occurred or not. In turn, a lack of historical data means there is no basis for a risk calculation. The risk calculation is an integral part as it is the basis for policy offers and thus the foundation of the product itself. It is also the centerpiece to attracting risk capital from investors. Data availability considerations may include fallback methods, e.g. if an API fails.

d) Data quality: A central concept of parametric insurance is the so-called base risk. It represents that a customer may not get a payout, even though they had damage, and vice versa (i.e., payout even though there is no damage). That is because the damage evaluation is exclusively based on data. It may happen that the provided data does not reflect the actual state of the situation. For instance, a customer of flood insurance receives a payout due to a high-water level according to the data, although no water ran into their house. Thus, a parametric approach requires an exceptionally high data quality to keep the base risk as small as possible. The smaller the base risk, the more the situation represented by the data corresponds to the actual situation.

e) Market potential: An excellent economic attractiveness of the product is required. The problem must be big enough that it seems sensible to purchase insurance. Surveys conducted among a potential target group are usually most effective here.

f) Onboarding: The hurdle of the onboarding process, which typical blockchain applications usually involve, must also be included here. Often, at least a MetaMask wallet with funds is necessary to be able to use an application within this ecosystem. Depending on the product and target group, the potential user may have already overcome this hurdle.

g) Scalability: When evaluating a use case, it also plays a role in how the geographical area affects the implementation. Technical or regulatory adaptations may be required for expansion into other countries. It may also be that the use case is not subject to any restrictions in this regard. This point is less critical for the general implementation but should still be considered. In addition, the scalability of a product also has a corresponding effect on the market potential, which must be evaluated separately.

h) Occurrence versus damage: This point strives to discuss the relationship between the probability of a damage occurrence and the amount of damage. An insurance product is most useful when damage rarely occurs, and the amount of damage is relatively high. Insurance is interesting for a customer, and sound policies can be offered in this case. When it is the other way round (i.e., damage often occurs and is relatively small), insurance gets quite unattractive due to high premiums and low payouts. Furthermore, customers are most likely able to cover the damage themselves.

i) Object of insurance: The damage of a covered risk by insurance always needs to be measurable in money amounts. The loss of private pictures due to hardware failure or a wedding on a rainy day is considered emotional damage. In general, the value of such damage is not measurable in money. Therefore, the calculation of a premium and a possible payout is infeasible. While designing an insurance product, one should consider whether it covers financial or emotional damage.

j) Consistency of the risk: It should be sure that an insured risk is present in the future. This criterion works the best when the risk is not influenceable by anyone (e.g., risks caused by the weather). However, most risks are influenceable in some ways. One should think about if the presence of the risk depends on one entity or person. The insurance product could be obsolete once a rule, behavior, or process changes.

3. Proposal for an Ethereum-based architecture

This chapter forms the central part of the paper and proposes an Ethereum-based architecture for blockchain-based parametric insurance (see figure 1). It covers all components and sub-steps of the system in detail.

3.1 Components

Chainlink: A significant weakness of smart contracts is that they cannot independently access data outside the blockchain. They must be connected to an oracle, which is the source of the data. Chainlink enables the transfer of data from sources outside the blockchain to smart contracts within the blockchain. This architecture uses Chainlink to connect smart contracts with an API outside the blockchain and to automate smart contracts with the Chainlink Keepers. [6]

Generic Insurance Framework: The smart contracts of this architecture use the Generic Insurance Framework (GIF). The GIF is a collection of open-source smart contracts that implement essential functions and risk pool infrastructure that all insurance products share in common. This includes the lifecycle of a policy with all its substeps. Thus, it can be used to design and implement insurance products quickly and easily. Product-specific aspects such as pricing and the insurance logic need to be implemented individually. A so-called GIF Instance is required to operate insurance products. It is used for selling policies, collecting premiums, calculating trigger events, and handling payouts. GIF-based insurance products are managed and operated in such a GIF instance. There may be various GIF instances on different EVM-based blockchains, for example, Polygon or Gnosis Chain. One GIF instance may manage multiple insurance products. Not all GIF details are shown in the component diagram for better understanding. Some sub-steps may be more complex than described. [1]

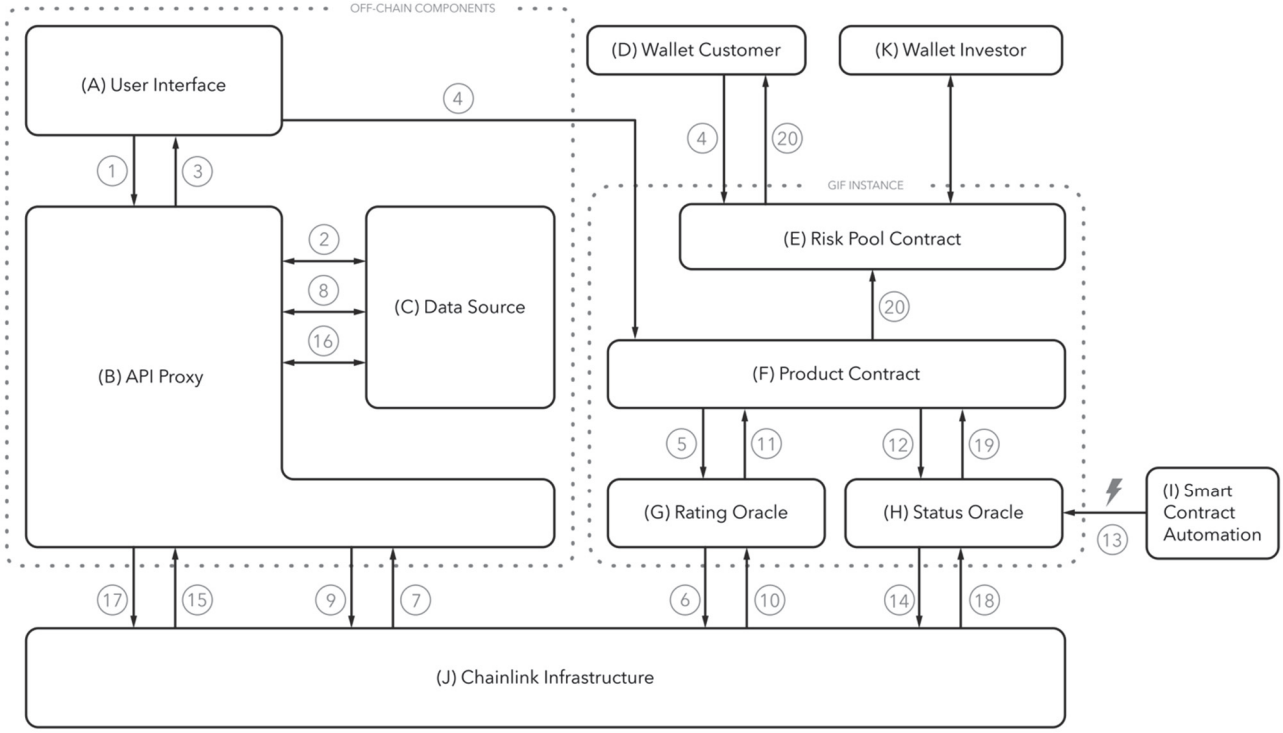

Figure 1: Component diagram

(A) User Interface: The system includes only one graphical component: the user interface. This could be a web application, for instance. The primary purpose of the user interface is to connect the user with the services in the back end. This includes purchasing a policy, displaying active policies, and other relevant status information for the user. To buy a policy, the user needs to have a wallet connected to the user interface. The wallet is required to sign transactions to interact with a smart contract. However, all calculations for a policy offer are conducted off-chain and only validated again in the smart contract once the user accepts the offer. This way, only one blockchain transaction is required.

(B) API Proxy: The primary purpose of the API proxy is wrapping the data source. It processes data from the data source and allows to query for risk and status for a specific policy. The risk calculation is done by querying historical data from the data source and applying a prediction model. Simple heuristic methods and more complex machine learning models can be used since it is local off-chain processing. Providing a status for a policy requires querying live data from the data source. A predefined data type can be guaranteed for every response required to process Chainlink requests by using a proxy in front of the API. Furthermore, the data source may work via licensed API keys, which can be protected this way. Thus, the API proxy is an essential part of the system as an additional abstraction layer. Values and processing steps could be made publicly available to create transparency.

(C) Data Source: Since a parametric insurance product is exclusively based on data, the data source plays a crucial role in the system. It must provide historical data as well as live data with good reliability. The data type depends on the insurance product, for instance, weather data.

(D) Customer Wallet: The interaction with a smart contract requires an Ethereum wallet. This wallet needs to be connected to the user interface. Buying a policy requires funds on the network the insurance product is deployed on, for instance, MATIC on Polygon or xDai on Gnosis Chain. The wallet must be used to sign a transaction during the purchase process of a policy. If the user gets a payout for their policy, it will be sent to the same address used to pay the premium. To view the status of a policy, the same wallet used to buy it needs to be connected with the user interface.

(E) Risk Pool Contract: The risk pool contract's primary purpose is insurance capital management. This consists of risk capital from investors and premiums from customers. A payout for a policy happens with funds from the risk pool. The GIF manages the flow of funds to and from the risk pool contract.

(F) Product Contract: The product contract makes use of the GIF and is part of a GIF instance. Thus, this contract only needs to implement the insurance logic and the pricing model, while the GIF instance takes care of the lifecycle of a policy. The product contract offers a function for policy applications. All off-chain information that is necessary for the processing of a policy is queried via so-called oracles. The GIF manages the communication between the product contract and the oracles. If a policy is entitled to a payout (i.e., the damage has occurred), the product contract initiates this payout at the risk pool contract.

(G) Rating Oracle: This smart contract links the product contract and the Chainlink Infrastructure. It is responsible for creating Chainlink Requests and handling the responses via a callback function. The rating oracle is used to query the risk for a policy.

(H) Status Oracle: Similar to the rating oracle, this smart contract links the product contract and the Chainlink Infrastructure. It contains a queue of active policies waiting for the resolution process (i.e., decide whether this policy is eligible for a payout or not). The status oracle is used to query the status of a policy once the Smart Contract Automation component triggers the execution.

(I) Smart Contract Automation: Every action in a smart contract needs to be triggered by another smart contract or a wallet (i.e., an externally owned account). Smart contracts cannot set a timer to execute themselves after some time. An incentivized bot network like Chainlink Keepers or Gelato Network can be used to achieve smart contract automation. The network checks if the automated contract needs to be called at every mined block. This check happens off-chain and does not require any gas. The checking logic heavily depends on the use case. For instance, it can be checked if a specific date is reached or if an event happened. Once the condition is met, a pre-defined contract function gets executed. This function triggers the policy resolution process. A different option is to make calls from a local server. Theoretically, anyone can call the policy resolution function. If a policy is eligible to receive a payout, the owner of the policy is automatically incentivized to call the function. Thus, if the automation fails, there is no trust issue, but it serves the user's convenience.

(J) Chainlink Infrastructure: Chainlink enables the transfer of data from sources outside the blockchain to smart contracts within the blockchain. This architecture uses the Chainlink network, as it has become the quasi-standard in the industry in recent years. [7] However, every oracle protocol that offers a similar functionality could be used, for instance, Tellor.

(K) Wallet Investor: Risk capital from external investors is required to ensure that the risk pool is solvent all the time. This is especially important if there is a disaster where many people get a payout. Investors risk their capital for such an unlikely event and earn a profitable yield. An investor does not actively affect the processing of a policy. It just interacts with the risk pool of the insurance product.

3.2 Interaction between components

(1) The user filled in all necessary information for the application for a policy. The user’s input data is sent to the API proxy for the risk calculation.

(2) The API proxy queries the corresponding data from the data source to conduct the risk calculation. The risk calculation is done by applying the prediction model to historical data.

(3) The result of the risk calculation is sent back to the user interface and appropriately displayed to the user. The result of the risk calculation defines the maximum payout the user can receive. The user can now decide whether they want to buy a policy for the shown conditions or not.

(4) The user decides to buy the policy. This requires an on-chain transaction. Thus, the user must have a wallet connected to the user interface. With the transaction, the information about the policy is sent to the product contract, and the premium is paid. In the best case, all information relevant to the policy can be saved in the product contract. In some cases, the data may require too much storage space and is therefore too expensive to be stored in a smart contract on-chain. It could be an option to store the information in a publicly accessible location, such as the InterPlanetary File System (IPFS). The link to that information would then be stored in the smart contract.

(5) The result from the risk calculation is the basis for the payout calculation, requiring the product contract to know that information. The information cannot be transferred in step 4 because the user can modify the transaction and the transmitted data. Thus, the user could change the information to gain an advantage (i.e., a higher possible payout). Therefore, this information must be queried from the API proxy independently from the user’s transaction. A smart contract needs an oracle to be able to query data from a server. This architecture uses the direct request jobs from Chainlink. [8] This step sends all relevant information to perform the risk calculation (i.e., the same information from step 1) to the rating oracle. In case the system requires storing data in the IPFS, the identifier of the information is transferred instead. The product contract receives the result for this query (i.e., the result of the risk calculation) in step 11.

(6) A Chainlink Request is built by the rating oracle. It contains the transferred information from the previous step. Finally, the request is sent to a Chainlink node.

(7) The Chainlink node queries the API proxy with an HTTP request that contains the transferred information from step 6 in its body.

(8) The API proxy queries the corresponding data from the data source to conduct the risk calculation. The risk calculation is done by applying the prediction model to historical data. This step is the same as step 2.

(9) The result of the risk calculation is sent back to the Chainlink node in response to the HTTP request.

(10) The result of the risk calculation is sent back to the rating oracle. The callback function manages the further processing of the result.

(11) The rating oracle calls the product contract's callback function, and the risk calculation result is transferred one last time. This result is the basis for the pay-

out calculation, as mentioned in step 5. The product contract needs a pricing model implemented to calculate a possible payout for the policy based on the result of the risk calculation. Once the payout amount is defined, the policy can be underwritten and is now eligible to receive a payout. The logic may also implement rejections. Policies with a high risk for damage or where the risk calculation has failed can be rejected, for instance.

(12) The product contract creates a request to query a policy's status information. The result of this query will later decide whether this policy is eligible for a payout. The request is put in a queue in the status oracle with a condition for when it can be executed. This condition most likely includes whether a specific time point or an event happened.

(13) The smart contract automation component regularly checks if the defined condition is met. Once the condition is fulfilled, a pre-defined function is executed, which triggers the execution of the queued request.

(14) A Chainlink Request is built by the status oracle out of the queued request. This request contains the necessary information about the policy. Finally, the request is sent to a Chainlink node.

(15) The Chainlink node queries the API proxy with an HTTP request that contains the necessary information for the policy in its body.

(16) The API proxy queries live data from the data source to determine the status of the policy.

(17) The status of the policy is sent back to the Chainlink node in response to the HTTP request.

(18) The status of the policy is sent back to the status oracle. The callback function manages the further processing of the result.

(19) The status oracle calls the product contract's callback function, and the policy's status is transferred one last time. The status is the basis for the damage evaluation. As described earlier, the damage assessment in a parametric product exclusively relies on data. Usually, this is a simple mathematical comparison if a trigger value is exceeded. If not, the policy expires without further action, and the process ends. However, if the trigger value is exceeded, a payout in the amount of the calculated value in step 11 is triggered.

(20) The risk pool contract is responsible for managing the funds of the insurance product. The product contract instructs the risk pool contract to transfer the calculated payout to the customer. Finally, the risk pool contract transfers the funds to the customer's wallet, and the policy expires.

3.3 Architectural drawbacks

The data source shown in the architecture is a central component. Furthermore, the proxy API has full sovereignty over the data and can theoretically manipulate it before an oracle retrieves it. Even if the blockchain is still necessary for payment flows and transparency reasons, the main advantage of a blockchain is being undermined: the possibility of building a trustless system.

Ideally, the architecture relies on a fully decentralized data source in the future. One central aspect that is necessary for this is an established data economy. This means more people and institutions must make data available and usable in an oracle network like Chainlink. [9] Second, risk calculations could also be performed on-chain in the future. This would make the API proxy and the central data source obsolete. However, the demonstrated architecture does not provide a fix for those two problems and therefore is not entirely decentralized. The user must trust the provider that builds a product with this architecture for the time being.

The complexity of the system is also an important aspect. This affects the maintenance of the system and the susceptibility to errors. The efficiency of the insurance process must make up for the operating effort. Only then is it worth using the system.

Another point to consider when using this architecture is that a blockchain with low transaction costs should be used. This is essential for products where the premiums are low. Otherwise, the operational costs due to transaction fees may be higher than the premium itself. It would also be reasonable to use a cryptocurrency that has a stable price, i.e., a stablecoin. Otherwise, the payout could be worth less due to volatility for products with a more extended period between payment of the premium and the claim.

4. Reference implementation: Train Delay

This chapter describes the implementation of a train delay insurance in Germany based on the stated architecture.

4.1. Covered Risk

Insurance against train delays works in such a way that a traveler specifies their train connection in an app within a period before the start of the journey. A policy is then created based on a forecast of the probability of a delay in the journey. The official timetable information from the transport companies, collected and made available by external aggregators, serves as the data source. The traveler activates the policy by paying the premium. A few minutes after the scheduled arrival, the real-time data is used to check whether the train arrived on time. If not, a payout is initiated.

A journey is defined by a departure station, a destination station, a departure time, and a list of legs, i.e., connection subsections. A leg consists of a train number, a departure station, a departure time, an arrival station, and an arrival time. The important thing is that the entire train connection becomes part of the policy. The subject of the policy is the final delay of a connection at the destination. Only in this way the insurance coverage for a

traveler makes sense. While querying information for a journey, the way the journey took place is checked. For example, a train might have been canceled, but an alternative connection still got the traveler to his destination or connecting train on time. From the real-time data, it can be determined with a very high degree of certainty whether a connecting train has been reached or missed. If a connecting train is missed, the next connection is selected accordingly. This means that cases can also be considered in which a delay occurred but was made up for in the end by a changed connection.

4.2. Implementation

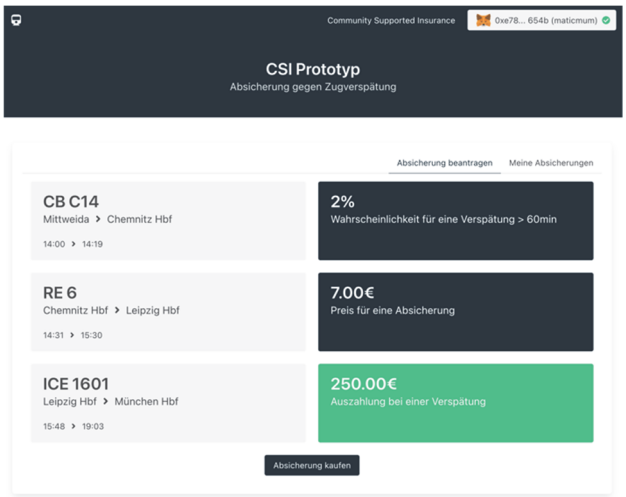

Figure 2: Policy offer for a train connection in Germany

A MetaMask wallet is assumed on the client side to interact with the contract. The on-chain components for this prototype are deployed on the polygon test network. The user interface is implemented as a web application in JavaScript. The user may select their train connection via an input mask. They input the connection by providing the departure station, the arrival station, and the departure time. The front end can retrieve the entire connection from a public timetable endpoint with that information. It is assumed that this query provides reliable data about future connections.

To offer a policy, the API proxy is queried for the delay risk of the selected train connection. The prediction model in this implementation is very basic as it just serves for testing in this case. It should be replaced with a real and more precise model in the future. Currently, the history of this connection in the past eight weeks is checked for a delay greater than 60 minutes. For instance, if one out of eight checked connections had a delay, a delay probability of 12.5% is assumed.

The user gets an overview of the policy with all corresponding conditions after the risk was successfully calculated (see figure 2). If they accept the shown conditions, they can buy it and interact with the product contract. In this interaction, they transmit the entire connection and pay the premium (see 3.2 step 4). The user's connected MetaMask wallet to the user interface must have a sufficient balance. The product contract can store the connection containing every leg on-chain as this information easily fits in a short string. The data is required to process a claim later. The contract then queries the delay risk via the rating oracle. The user interface and the oracle are using the same endpoint for this. After receiving the delay risk, a possible payout is calculated, and the policy is underwritten. Thus, making it eligible for a payout. Underwriting the policy triggers an event that is used to update the user about their policy status via the user interface.

From now on, no user interaction should be required. When underwriting the policy, a trigger time for further processing is defined. This results from the planned arrival time of the train at the destination plus an offset. Currently, this offset is set to 60 minutes. Chainlink Keepers trigger the further processing of the policy once the trigger time is reached. The product contract requests the arrival time of this connection via the status oracle. A payout is initiated if the train delays more than 60 minutes. If not, the policy expires without any further action.

The data source in this implementation forms a central component. A significant improvement in the implementation would be achieved by using a completely decentralized and trustless data source. Unfortunately, this is not trivial and illustrates the so-called oracle problem. [10]

5. Conclusion

This paper has shown a technical approach and the benefits of blockchain-based parametric insurance. The potential for automation, transparency, and fast payment flows has been highlighted. One should be able to quickly verify whether a new use-case idea is suitable for a blockchain-based parametric implementation by using the shown catalog of criteria. Once a use case is found, it can easily be implemented using the stated architecture.

Many use cases are infeasible in the classic insurance business due to high administration costs and long processing time due to manual activities. For instance, selling policies worth five euros and paying more than 30€ for the administration of that policy is infeasible. The stated approach may enable such use cases due to automatic processing and low administration costs.

The transparency of a smart contract offers the possibility to see the entire business logic of an insurance product. This is useful, especially in countries where corruption is a problem. People do not have to trust a big company representing a black box. This may play a less critical role in a stable and regulated market.

Classic insurance companies may decide who is allowed to participate and who is not. Blockchain-based insurance can be built virtually accessible by anyone with access to the internet and a wallet. Furthermore, a blockchain-based parametric approach allows for automatic

and instant payouts. Automation is enabled by design by using a parametric approach. Instant payouts are enabled by using a blockchain as the layer for payments.

A big downside of the stated architecture is the centralized data source. The main advantage of a blockchain is being undermined: the possibility of building a trustless system. The connection between a blockchain and real-world data is a much-discussed problem known as the oracle problem. This architecture does not solve this problem; however, it has many advantages in different areas. Ideally, the oracle problem can be tackled by providing and processing the data in a fully decentralized way in the future. New technologies and procedures may path the way to that state.

References

[1] Basics about the Generic Insurance Framework (GIF), (2022/07/25): https://blog.etherisc.com/basics-about-the-gif-framework-68127be1ce2a

[2] Versicherungsmagazin, (2022/07/26): https://www.versicherungsmagazin.de/rubriken/branche/verwaltungskosten-zu-hoch-2542184.html

[3] Parametric Insurance for Disasters, (2020/09): https://riskcenter.wharton.upenn.edu/wp-content/uploads/2020/09/Parametric-Insurance-for-Disasters_Sep-2020.pdf

[4] Parametric Insurance & Blockchain: A new dimension to the ever young Insurance Industry, (2018/09): https://medium.com/@srishtisawla/parametric-insurance-blockchain-a-new-dimension-to-the-ever-young-insurance-industry-53a26c0d4c79

[5] Moral hazard in the insurance industry, (2013/03): https://www.researchgate.net/publication/235988864_Moral_hazard_in_the_insurance_industry#pff

[6] Chainlink on EVM (Ethereum) Chains, (2022/07/20): https://docs.chain.link/ethereum/

[7] BofA Says Chainlink Likely Driver for DeFi's TVL Growth to $203B, (2022/02/17): https://www.coindesk.com/business/2022/02/17/bofa-says-chainlink-likely-driver-for-defis-tvl-growth-to-203b/

[8] Direct Request Jobs, (2022): https://docs.chain.link/docs/jobs/types/direct-request/

[9] Understanding How Data and APIs Power Next-Generation Economies, (2020/07/06): https://blog.chain.link/understanding-how-data-and-apis-power-next-generation-economies/

[10] A Study of Blockchain Oracles, (2020/07/14): https://arxiv.org/pdf/2004.07140.pdf

Speichern von grafischen Daten für NFTs auf der Blockchain

Marianne Poser
Hochschule Mittweida, poser@hs-mittweida.de

In dieser Forschungsarbeit wird ein Überblick darüber gegeben, wie Grafikdaten eines NFT auf der Blockchain gespeichert werden können. Es werden verschiedene Ansätze untersucht und vorhandene Projekte analysiert. Dabei werden vor allem die Aspekte Sicherheit, Ressourcen und Anwendbarkeit betrachtet. Mithilfe einer Testumgebung werden die recherchierte Ansätze vergleichbar, wobei sich in der Arbeit auf skalierbare Vektorgrafiken (SVG) konzentriert wird. Letztendlich zeigt sich, dass es für simple SVG sinnvoll ist, ihren Code als String oder auch in Base64 codiert im NFT selbst abzulegen. Für komplexere Grafiken wird ein Ansatz mit einem Smart Contract empfohlen, um die Kosten pro NFT zu reduzieren. Die Vorgehensweise, die Grafikdaten durch eine Funktion wiederherzustellen, eignet sich außerdem auch für Ansätze, die nicht auf Vektor Grafiken bauen. Es zeigt sich, dass durch einen gewissen Mehraufwand durchaus NFT und Grafikdaten auf der Blockchain abgelegt werden können und kein Risiko durch die Trennung zwischen On- und Off-Chain eingegangen werden muss.

1. Einleitung

Der Begriff NFT Kunst beschreibt die Verbindung von (digitaler) Kunst und einem NFT, welcher als Besitzurkunde über das Kunstwerk fungiert. Es wird als die Revolution und Zukunft der Kunstbranche bezeichnet und wird so bei Kunstsammler:innen, Spekulant:innen und Künstler:innen immer bekannter. [1]

Doch bei der Kaufentscheidung sollte nicht nur auf die Reputation der Künstler:innen oder die Rarität des Kunstwerks geachtet werden, sondern es sollte auch ein Blick auf die Technik dahinter geworfen werden. Wo ist der NFT und wo ist das dazugehörige Kunstwerk gespeichert? Denn auch wenn der NFT sicher auf einer Blockchain wie Ethereum abgelegt ist, so muss sich dort nicht auch das Kunstwerk befinden. Viel wahrscheinlicher ist es, dass im NFT nur ein Link zu dem Kunstwerk hinterlegt wurde.

In dieser Arbeit werden die damit verbundenen Probleme gezeigt und mögliche Lösungen dafür vorgestellt und miteinander verglichen. In den folgenden Kapiteln wird die Problemstellung erörtert, die Literaturrecherche vorgestellt und daraus abgeleitete Lösungen und Varianten verglichen.

Es wird gezeigt, wie grafische Daten auf der Blockchain sicher, kostensparend und anwenderfreundlich abgelegt werden können. Denn nur so ist das Wertgebende des NFT – die Kunst, genauso gut verwahrt wie der NFT selbst. Und dies sollte genauso im Interesse der Künstler:innen sein, wenn sie ihre Kunst für teilweise insgesamt 69 Millionen USD versteigern, wie auch der Besitzer:innen von NFT. [1]

2. Problemstellung

Für die digitale Ablage des Kunstwerks bzw. dessen grafischen Daten bestehen grundsätzlich drei Möglichkeiten. Das Bild kann auf einem zentralen Server abgelegt werden oder in einem dezentralen Serversystem. Die letzte Möglichkeit ist, dass das nicht nur der NFT sich auf der Blockchain befindet, sondern auch die grafischen Daten selbst. Mit diesem Ansatz soll sich in diesem Paper tiefergehend auseinandergesetzt werden. Zunächst sollen aber die beiden auf serverbasierenden Ansätze betrachtet werden.

Bei dem Ansatz, dass das Bildmaterial auf einem zentralen Server abgelegt wird, ist folgendes Szenario vorstellbar. Ein Start-up entwickelt verschiedene Bilddateien und erzeugt zu jedem Bild einen NFT. Die Bilddateien legt es auf einem Server ab und der NFT enthält einen Zeiger mit der URL auf die dazugehörige Datei. Mit dieser Ausgangslage würde das Unternehmen nun einen Launch ankündigen und die NFT versteigern. Die Person, welche den NFT erwirbt, wird von da an auch als Besitzer:in der Bilddatei angesehen werden.

Allerdings kann es schnell zu Problemen kommen, da die einzige Verbindung zwischen NFT und Bilddatei ein Link auf einen zentralen Server des Unternehmens ist. Dieser Single Point of Failure kann in verschiedenen Szenarien angegriffen werden, ohne dass die Person selbst etwas dagegen vornehmen kann. Zum einen kann der Server abstürzen oder generell abgeschaltet werden (bspw. bei Insolvenz des Unternehmens). Das Unternehmen kann die Bilddateien aber auch im Nachhinein abwandeln, austauschen, verschieben oder löschen. Auch könnte der Zugriff auf diese Bilddatei verwehrt werden. In jedem Fall wäre der Besitz des NFTs wertlos, da das wertgebende Bild nicht mehr erreichbar oder nicht mehr damit verbunden ist. [2]

Selbst wenn zuvor eine Kopie des Bildes gesichert wurde, kann dieses nicht mehr mit dem NFT verbunden werden. In diesem Fall wäre es hilfreich, wenn zusätzlich Hash über die Bilddatei in den NFT integriert wird. So kann bei Besitz einer Kopie zumindest nachgewiesen werden, dass der NFT sich tatsächlich auf dieses Bild bezieht. [2] Auch für den Fall, dass der Server (bspw. durch das Unternehmen) gewechselt werden muss und sich

dadurch die URL ändert, gibt es bereits eine Lösung. In dem Tokenstandard ERC1155 ist die Funktion integriert, dass die URI gewechselt werden kann und sich die einzelnen URL dann aus der NFT ID ergeben. [3]

Beide Ansätze sind aber keine Lösung für das Problem, dass eine Unterbrechung zwischen On-Chain NF und Off-Chain Bilddatei den NFT wertlos macht. Denn auch die eigene Kopie kann verloren gehen und das Unternehmen vielleicht gar kein Interesse mehr daran, die URL aktuell zu halten.

Dem Problem von zentralen Servern sind sich Blockchain-affine Menschen meist bewusst. Daher ist die populäre Alternative eine Art dezentrales Serversystem. Im InterPlanetary File System (IPFS) können mehrere Kopien einer Datei abgelegt werden und so die Absicherung gegen Ausfälle erhöht werden. Allerdings speichern IPFS Server Daten nur so lange, wie ein Node des Netzwerkes dies fordert. Überlässt man die Sicherung der Bilddateien wieder nur dem Herausgeber der NFT, so kann dieser sie zu einem späteren Zeitpunkt von seinem Node entfernen und damit entsteht die Gefahr, dass es komplett vom IPFS gelöscht wird. [4, 5] Dass es nicht ungewöhnlich ist, dass Dateien im IPFS nicht mehr gefunden werden, zeigen verschiedene Twitter-Posts des Dienstes CheckMyNFT. [6]

Die Betrachtung der beiden Server-Speichermöglichkeiten zeigt, dass beide nicht ausreichend sind, um die Bilddaten eines NFT sicher aufzubewahren. Aus Sicherheitsgründen wäre es also am sinnvollsten, Kunst und NFT am gleichen Ort zu speichern - auf einer Blockchain. [7] Diese Möglichkeit und welche Varianten sie besitzt soll im folgenden Kapitel betrachtet werden.

3. On-Chain Speichermöglichkeiten

Der Ansatz, neben dem NFT auch die eigentliche Kunst auf der Blockchain zu speichern, wurde vor allem aufgrund der Kosten erst von wenigen Projekten umgesetzt. [7] Doch vor allem aus Aspekten der Sicherheit sollte sich intensiver mit dieser Möglichkeit befasst werden. Grundlegend gibt es zwei Varianten, wie das Kunstwerk auf der Blockchain abgelegt werden kann. Beide werden im Folgenden vorgestellt.

Die erste Möglichkeit ist, dass die Kunst durch eine Funktion in einem Smart Contract generiert wird. Als Beispiel für diese Variante eignet sich das Projekt Autoglyphs von LarvaLabs. Auf ihrer Webseite bezeichnen sie sich als Herausgeber der ersten On-Chain generierten Kunst. [8] Die Kunstwerke basieren auf einer Auswahl von Symbolen, wobei der ID eines NFT jeweils ein Symbol zugewiesen wird. Mit der draw-Funktion im Smart Contract wird dieses Symbol ausgelesen und basieren auf einem Seed bzw. dessen Hash geplottet. Also wird für jede Stelle des Kunstwerks entschieden, ob ein Symbol gesetzt wird oder ein Leerzeichen entsteht. Das Ergebnis wird als Base64 codiert ausgegeben und kann mit dem Präfix "data:text/plain;charset=utf-8," von allen gängigen Browsern interpretiert und ausgegeben werden. [9] Die dadurch entstandenen Kunstwerke sind einzigartig und werden so lange bestehen, wie es die Ethereum Blockchain geben wird.

Die Kosten für das Erzeugen eines solchen NFT sind recht gering. Betrachtet man die dazugehörige Transaktion, so hat diese laut Etherscan zum damaligen Zeitpunkt knapp $0.90 (0.0053 Eth) gekostet. [10] Und auch das Erzeugen des Smart Contract selbst kostete nur etwa 0.012 Ether. [11] Um das Bild aus dem Seed erneut erstellen zu lassen, reicht ein Funktionsaufruf, der draw-Funktion, welche pure ist. Der Aufruf verursacht dementsprechend keine Kosten. Diese Variante ist also nicht mit horrenden Kosten verbunden und bietet dennoch die komplette Sicherheit für NFT und Bild. Die günstigen Preise hängen allerdings auch mit der simplen Art der Kunst und Symbole zusammen. Für komplexere Bilder oder Bilder, welche nicht (komplett) mit einem Algorithmus erzeugt werden sollen, bestehen andere Möglichkeiten.

Eine andere Möglichkeit, welche auch von verschiedenen Projekten umgesetzt wurde, ist, die Bilddaten in den Metadaten des NFT zu speichern. Dabei handelt es sich zumeist um eine Vektorgraphik (SVG), welche anschließend in einen Base64-String codiert wurde. Dieser wiederum muss nur mit dem entsprechenden Präfix in einen Browser eingefügt werden und wird von diesem in die Grafik umgewandelt. [12] Ein Projekt, welches darauf basiert, ist CardanoTrees, welches ebenfalls generative Kunsttechniken nutzt und das Ergebnis dann in dem NFT auf der Cardano-Blockchain ablegt. [13]

Neben den genannten Projekten gibt es einige weitere NFT Projekte, welche komplett On-Chain arbeiten. Dabei unterscheiden sie sich in verschiedenen Faktoren. Wie bereits vorgestellt, können die Daten, welche in der Blockchain abgelegt wurden, auch in der Blockchain gerendert werden. Das Ergebnis kann dann von einem Browser als Bild interpretiert werden. Oder aber die gespeicherten Grafikdaten müssen durch ein externes Skript bearbeitet und gerendert werden. Dies ermöglicht ein komplexeres Vorgehen und kann neben grafischen Daten auch Musik verarbeiten. [14]

Neben dem Ablegen in den Metadaten und dem Generieren der Kunst On-Chain gibt es also weitere Zwischenlösungen, welche teilweise ein externes Skript benötigen. Dieses Skript kann beispielsweise auf der Blockchain gespeichert werden, ohne dass es dort ausgeführt werden kann. Dieses Skript entspricht also eher einer Anleitung, was Nutzer:innen Off-Chain durchführen müssen, um aus den Informationen auf der Blockchain ihr Kunstwerk zum NFT wiederherstellen zu können. Wichtig ist dabei, dass die Anleitung tatsächlich On-Chain abgelegt wird. Schreibt man die Anleitung hingegen in die Kommentare, so wird sie in den Metadaten des Contracts abgelegt, welche in einem automatisch generierten JSON gespeichert werden. Diese Datei wiederum ist dafür gedacht, auf IPFS abgelegt zu werden, der Hash der Datei wird am Ende des Bytecodes angehängt.

Auf diese Weise kann die Korrektheit authentifiziert werden, allerdings liegt die Anleitung dadurch nicht auf der Blockchain, sondern im IPFS. Um auch die Anleitung auf der Blockchain abzulegen, muss sie bspw. in einer Variablen im Contract abgelegt werden. Um Kosten zu sparen, kann diese Variable als Konstante definiert werden.

Je nach Art der Anleitung sollte geprüft werden, ob eine Base64 codierte Ablage Sinn macht oder nicht. Für die Anwendbarkeit kann es sinnvoller sein, die Daten ohne Codierung abzulegen, sodass leichter erkennbar ist, was in der Anleitung erklärt wird und nicht erst in lesbare Form gebracht werden muss. Sollen die Daten hingegen direkt von einem Browser in ein Bild übersetzt werden können, so ist der Base64 codierte String leichter händelbar als bspw. der Code einer SVG. Für eine nicht codierte Ablage spricht, wenn Informationen in der ID selbst oder in Form eines Seeds abgelegt werden und dann in eine Art Maske eingesetzt werden müssen. Das Ablegen von Informationen in der ID ist besonders sinnvoll, um eh bezahlten Speicherplatz effektiv zu nutzen. In den 256 Bit der ID können bereits Informationen über die Bilddaten abgelegt werden. [15]

Eine weitere Möglichkeit, um bei der Ablage On-Chain, Kosten zu sparen, wird im EIP4883 vorgestellt. Dabei wird eine neue SVG für ein NFT erzeugt, indem bereits bestehende SVGs anderer NFT verkettet werden. Dadurch könnten neue On-Chain Bilder für NFT kostensparend erzeugt werden, wenn sie auf bereits hinterlegtes Bildmaterial zurückgreifen. Dieser EIP befindet sich allerdings noch in Bearbeitung und klärt beispielsweise noch nicht, unter welchen Bedingungen die Grafikdaten anderer NFT genutzt werden dürfen. [16]

4. Vergleich der Möglichkeiten

Für eine bessere Entscheidungsgrundlage wurden verschiedene Ansätze in einem Test umgesetzt. Die Ausgangslage war dabei, dass auf der Ethereum-Blockchain sowohl NFT als auch Bilddaten abgelegt werden sollten. Die Bilddaten sollten nicht durch eine Funktion im Smart Contract erzeugt werden müssen, sondern es kann auf ein externes Skript zurückgegriffen werden. Allerdings ist die Anleitung für das Erstellen der Grafiken mit im Smart Contract abgelegt. Geprüft werden sollte nun, welches die optimale Lösung für das Ablegen der SVG auf der Blockchain sein könnte. Als Grundlage für den Token wurde der Umsetzung des Standards ERC1155 durch Open Zeppelin genutzt. [3]

Als Umgebung wurde die Truffle Suite mit einer lokalen Blockchain mit Ganache genutzt. Und für die Entwicklung selbst wurde Visual Studio Code verwendet. Für den ersten Vergleich wurde eine SVG mit dem Bild einer Fackel genutzt. Sowie der SVG Code in Base64 codiert.

Abbildung 1: Fackel

```
<?xml version="1.0" encoding="UTF-8"?>
<svg width="190.2mm" height="155.2mm" version="1.1" viewBox="0 0 190.2 155.2" xmlns="http://www.w3.org/2000/svg">
 <g transform="matrix(.3533 0 0 .3533 -.1957 -.1402)" stroke="#000" stroke-miterlimit="11.34" stroke-width="5.7">
  <rect x="403.7" y="98.3" width="20.4" height="160.4" fill="#630" stroke-linecap="round"/>
  <circle cx="419" cy="223" r="26.9" fill="#f69c7f"/>
  <g stroke-linecap="round">
   <path d="m413.9 16.1s28.8 21.6 28.8 47.1-12.9 46.1-28.8 46.1-28.8-20.6-28.8-46.1 28.8-47.1 28.8-47.1z" fill="#f63"/>
   <path d="m413.9 41.6s21.1 15.1 21.1 33.8-9.4 33.8-21.1 33.8-21.1-15.2-21.1-33.9 21.1-33.7 21.1-33.7z" fill="#f93"/>
   <path d="m413.9 78.3s9.1 6.9 9.1 15.5-4.1 15.5-9.1 15.5-9.1-6.9-9.1-15.5 9.1-15.5 9.1-15.5z" fill="#ff6"/>
  </g>
 </g>
</svg>
```

Abbildung 2: SVG Coder der Fackel

PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiPz4KPHN2ZyB3aWR0aD0iMTkwLjJtbSIgaGVpZ2h0PSIxNTUuMm1tIiB2ZXJzaW9uPSIxLjEiIHZpZXdCb3g9IjAgMCAxOTAuMiAxNTUuMiIgeG1sbnM9Imh0dHA6Ly93d3cudzMub3JnLzIwMDAvc3ZnIj4KIDxnIHRyYW5zZm9ybT0ibWF0cml4KC4zNTMzIDAgMCAuMzUzMyAtLjE5NTcgLS4xNDAyKSIgc3Ryb2tlPSIjMDAwIiBzdHJva2UtbWl0ZXJsaW1pdD0iMTEuMzQiIHN0cm9rZS13aWR0aD0iNS43Ij4KICA8cmVjdCB4PSI0MDMuNyIgeT0iOTguMyIgd2lkdGg9IjIwLjQiIGhlaWdodD0iMTYwLjQiIGZpbGw9IiM2MzAiIHN0cm9rZS1saW5lY2FwPSJyb3VuZCIvPgogIDxjaXJjbGUgY3g9IjQxOSIgY3k9IjIyMyIgcj0iMjYuOSIgZmlsbD0iI2Y2OWM3ZiIvPgogIDxnIHN0cm9rZS1saW5lY2FwPSJyb3VuZCI+CiAgIDxwYXRoIGQ9Im00MTMuOSAxNi4xczI4LjggMjEuNiAyOC44IDQ3LjEtMTIuOSA0Ni4xLTI4LjgtMjAuNi0yOC44LTQ2LjEgMjguOC00Ny4xIDI4LjgtNDcuMXoiIGZpbGw9IiNmNjMiLz4KICAgPHBhdGggZD0ibTQxMy45IDQxLjZzMjEuMSAxNS4xIDIxLjEgMzMuOC05LjQgMzMuOC0yMS4xIDMzLjgtMjEuMS0xNS4yLTIxLjEtMzMuOSAyMS4xLTMzLjcgMjEuMS0zMy43eiIgZmlsbD0iI2Y5MyIvPgogICA8cGF0aCBkPSJtNDEzLjkgNzguM3M5LjEgNi45IDkuMSAxNS41LTQuMSAxNS41LTkuMSAxNS41LTkuMS02LjktOS4xLTE1LjUgOS4xLTE1LjUgOS4xLTE1LjV6IiBmaWxsPSIjZmY2Ii8+CiAgPC9nPgogPC9nPgo8L3N2Zz4K

Abbildung 3: Code der Fackel in Base64

Bereits der Vergleich der Dateigrößen zeigt, dass die Base64-Codierung mehr Speicherplatz benötigt. Für einen Vergleich auf der Blockchain bzgl. der Gas-Kosten wurde zweimal der gleiche Contract aufgesetzt. Dabei wurde die öffentliche Konstante „torch“ einmal codiert und einmal als SVG Code eingefügt. Dabei wurde der SVG Code insofern verändert, dass die doppelten Anführungszeichen (“) durch einfache Anführungszeichen (‘) ersetzt wurden und alle Zeilenumbrüche entfernt wurden. Beide Contracts wurden auf der lokalen Blockchain deployed und die Gaskosten konnten verglichen werden. Dabei entstanden die folgenden Werte: Bei der Base64 Variante wurden 2.728.024 Gas verbraucht und bei der SVG Code Variante 2.665.545 Gas. Der Unterschied beträgt also etwa 60.000 Gas zwischen codiert und nicht codiert.

Je nach Anwendung kann die Codierung mit Base64 weitere Nachteile oder auch Vorteile in der Anwendung mit sich bringen. Wird zu jedem einzelnen NFT in den Metadaten das Bild mit abgelegt, ist es für den Anwender leichter, einen Base64 codierten String zu kopieren und von einem Browser (mit entsprechendem Präfix) interpretieren zu lassen. Sollen jedoch im SVG-Code selbst noch Anpassungen oder Personalisierungen vorgenommen werden, so ist dies in nicht codierten Form leichter.

Zusätzlich könnten in verschiedenen Grafiken mehrfach vorkommende gleiche Codezeilen als Overhead extrahiert werden und müssten nicht redundant, sondern nur einmal in einer weiteren Konstante abgelegt werden. Verzichtet man in dem genutzten Beispiel auf die ersten beiden Zeilen des SVG Code, verringern sich die Gas-Kosten beim Deployen des Contracts um etwa 39.000 Gas. Diese müssten zwar dennoch im Contract hinterlegt werden und in der Anleitung das Zusammensetzen erläutert werden, dennoch spart es für jede weitere zu speichernde SVG diese Menge an Gas. Zusätzlich ermöglicht die nicht codierte Ablage eine Weiterverarbeitung durch andere Programme/Skripte, ohne dass diese erneute decodieren müssen.

Eine weitere genannte Variante, um Gas-Kosten zu sparen, ist das Ablegen von Informationen in der ID. In den NFT Tokenstandards ERC721 und ERC1155 bekommen die einzelnen NFT eine ID zugewiesen. Diese ist 256 Bit groß und könnte dafür genutzt werden, bereits Informationen über die Gestalt des NFT zu enthalten. Dabei muss beachtet werden, wie viele NFT es geben wird und wie viele Stellen der ID noch frei sind, sodass die IDs dennoch eindeutig bleiben. Die größte (Dezimal-)Zahl, welche mit dem Datentyp uint256 dargestellt werden kann, ist
‘115.792.089.237.316.195.423.570.985.008.687.907.853.269.984.665.640.564.039.457.584.007.913.129.639.935‘. Diese Zahl hat 78 Ziffern, zieht man eine davon ab, hat man 77 Ziffern, welche man mit Informationen füllen kann. Ist beispielsweise geplant, 120 NFT zu erzeugen, so benötigt man nur drei dieser 77 Stellen für die eindeutige Zuordnung. Die restlichen Stellen können für andere Informationen genutzt werden.

Ausgehend vom Beispiel der Fackel könnte die Farbe des Fackelstabs variiert werden und diese Information mit in der ID abgelegt werden. Würde man den RGB-Farbcode dafür nutzen, würden für diese Information dreimal drei Stellen, also 9 insgesamt benötigt werden. Auf diese Weise könnten auch die Farbcodes für die verschiedenen Schattierungen der Flamme und der Hand in der ID hinterlegt werden. Insgesamt wären dann fünf Farbcodes mit je neun Stellen in der ID hinterlegt. Und selbst dann wären immer noch 29 Ziffern der ID ungenutzt.

Doch auch die Nachteile werden im inspirierenden Twitter-Post genannt. So kann ausgehend von der ID nicht so einfach abgelesen werden, wie viele NFT es gibt und auch URL, welche die ID enthalten, werden sperriger. Auch wenn über verschiede NFTs diskutiert oder die ID anderweitig angegeben werden soll, muss so mit großen Zahlen hantiert werden. Eleganter kann es daher sein, das Gas für ein zusätzliches Mapping id=>seed zu investieren. Dabei werden die genannten Metadaten (Farbinformationen) im Seed (ebenfalls uint256) abgelegt und den IDs zugeordnet. Hier müssen die Seeds nicht eineindeutig sein, sondern nur die IDs.

In der Testumgebung ergab das Einsparen des Mappings und der Funktion zur Abfrage des Seeds zur gegebenen ID einen Unterschied von 28.000 Gas. In der mint-Funktion zum Kreieren eines neuen NFT ergab sich ein Unterschied von 6000 Gas, da keine Information im Mapping abgelegt werden musste. In beiden Fällen müsste in der Anleitung erklärt werden, welche Stellen was codieren und inwiefern sich daraus Anpassungen des SVG-Codes ergeben. Im Fall der Fackel könnten die Farbcodes für die Füllung der einzelnen Elemente im SVG durch Platzhalter ersetzt werden, wobei Platzhalter 1 durch den Farbcode der ersten neun Stellen des Seeds bzw. der ID ersetzt werden soll.

Als weitere Möglichkeit, Gas-Kosten zu sparen, wurde sich mit den SVG auseinandergesetzt. SVG sind im Allgemeinen recht platzsparend, da nicht einzelne Punkte definiert werden, sondern geometrische Elemente. Je näher man bei diesen Elementen bleibt, umso kleiner die SVG-Datei. Diesen Effekt erkennt man beim Vergleich der beiden Versionen der Fackel.

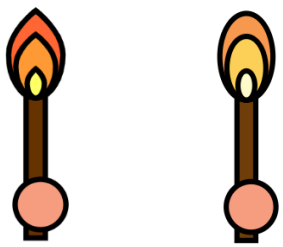

Abbildung 4: Vergleich Fackel Version 1 und Version 2

Der Unterschied zwischen den Fackeln liegt in der Gestaltung der Flammen, bei der Version 1 wurden diese durch Pfadelemente erzeugt und in der Version 2 durch Ellipsen. Durch den vermehrten Einsatz von geometrischen Elementen (Ellipsen statt zu definierende Pfade) unterscheiden sich die beiden Versionen bereits in der Dateigröße um fast 200 Bytes. Beim Speichern im Smart Contract als Konstanten ergab sich für die Version 2 eine Einsparung von etwa 26.000 Gas gegenüber der Version 1.

Neben diesen offensichtlichen Unterschied in Kosten und Gestalt konnten außerdem Verbesserungen geschafft werden, in dem die Anzahl der Nachkommastellen reduziert wurde. Eine weitere Vereinfachung des Codes der SVG kann durch automatisierte Optimierung mit Programmen wie Inkscape erreicht werden. Zusätzlich gibt es weitere Tools wie SVGminify, welche unnötige doppelte Informationen entfernt. [17] So reicht beispielsweise die einmalige Angabe der Strichbreite (stroke-width) innerhalb einer SVG und muss nicht für jedes Element neu mit angegeben werden. Neben dem Entfernen der Zeilenumbrüche könnten auch noch die Leerzeichen entfernt werden, was allerdings die Lesbarkeit verschlechtern würde. [18] Ebenso bringt die Vereinfachungen der Grafik Einbußen in Bezug auf die gestalterische Freiheit bzw. die künstlerische Finesse.

Grundsätzlich sollte beim Abwägen der verschiedenen Ansätze und Möglichkeiten nicht nur auf die Kosten geachtet werden, sondern auch auf die Anwendbarkeit. Für die Besitzer:innen der NFT ist es am komfortabelsten, wenn die Grafikdaten ihres NFT auch im NFT abgelegt werden und nicht im Smart Contract. Wenn die Ablage im Smart Contract ist es wiederum leichter aus Sicht der Anwender:innen, wenn eine Funktion aufgerufen werden kann, welche die Grafikdaten zurückgibt und nicht erst eine Anleitung gelesen, nachvollzogen und umgesetzt werden muss. Auf der anderen Seite ist die Ablage auf der Blockchain vorrangig für ein Notfallszenario gedacht und muss nicht jedes Mal beim Anzeigen des NFT vollzogen werden. Für die normale Nutzung könnten die Bilddaten eines NFT auch weiterhin auf einem Server abgelegt werden und von dort bezogen werden. Und nur in der Situation, wo dieser nicht (mehr) erreichbar ist, kann auf die Informationen im Smart Contract zurückgegriffen werden.

5. Fazit

Nachdem in diesem Paper verschiedene Speichermöglichkeiten für grafische Daten auf der Blockchain vorgestellt und zum Teil verglichen wurden, sollen die Erkenntnisse an dieser Stelle zusammengefasst werden.

Zunächst hat sich gezeigt, dass SVG, als Format für die grafischen Daten, verschiedene Optimierungsmöglichkeiten bereithält. So wären bereits bei der Entwicklung der Bilder große Einsparungen möglich. Dabei muss allerdings eine Balance zwischen Kostenreduktion und Einschränkung der künstlerischen Freiheit gefunden werden.

Ausgehend von den Vektor-Grafiken kann dann entschieden werden, ob der Code als solcher gespeichert werden soll oder ob er in Base64 codiert werden soll. Dies ist vor allem dann praktikabel, wenn die einzelnen Bilder direkt im zugeordneten NFT abgelegt werden soll. Besonders praktisch ist dies für die Nutzer:innen, welche diesen String nur in ihren Browser einfügen müssen. Der Nachteil daran ist, dass dieses Verfahren teurer ist und Anpassungen nur mit Zwischenschritten möglich sind.

Hat man viele ähnlich aufgebaute Grafiken, dann ist es sinnvoll, gleiche Codeteile zu separieren und in einer Anleitung das Zusammensetzen zur ursprünglichen Grafik zu erklären. Dieses System kann als Back-up zusätzlich zur Ablage im IPFS genutzt werden, sodass Nutzer:innen nur im Notfall die Grafik selber zusammensetzen müssen.

Auch bei der Entscheidung, wo Metadaten des NFT abgelegt werden sollen, muss zwischen Anwendbarkeit und Kosteneinsparung abgewogen werden. Speichert man Metadaten direkt in der ID des NFT, wird diese unhandlich und schwer lesbar. Das Speichern der Metadaten in einem struct für jeden NFT wiederum sollte aus Kostengründen vermieden werden. Eine gute Zwischenlösung scheint der Einsatz eines Mappings von ID zu einem Seed zu sein, welches die Metadaten enthält.

Letztendlich konnte gezeigt werden, dass die Möglichkeit, grafische Daten für NFT auf der Blockchain abzulegen, durchaus umsetzbar ist und mit verschiedenen Abwandlungen an die Gegebenheiten des eigenen NFT-Projekts angepasst werden kann. So können sichere NFT-Projekte entstehen, deren Kunst genauso lange erhalten bleibt wie der NFT selbst.

Literatur

[1] Christoph Peterson, „NFT Kunst kaufen und verkaufen 2022: So funktioniert es!“, 23. März 2022, 2022. [Online]. Verfügbar unter: https://coincierge.de/nft/nft-kunst/. Zugriff am: 1. August 2022.

[2] J. Benson, „Yes, Your NFTs Can Go Missing—Here's What You Can Do About It“, *Decrypt*, 19. März 2021, 2021. [Online]. Verfügbar unter: https://decrypt.co/62037/missing-or-stolen-nfts-how-to-protect. Zugriff am: 2. August 2022.

[3] OpenZeppelin, *ERC1155.sol.* [Online]. Verfügbar unter: https://github.com/OpenZeppelin/openzeppelin-contracts/blob/master/contracts/token/ERC1155/ERC1155.sol (Zugriff am: 4. August 2022).

[4] B. Dale, „It's an NFT Boom. Do You Know Where Your Digital Art Lives?“, *CoinDesk*, 23. Feb. 2021, 2021. [Online]. Verfügbar unter: https://www.coindesk.com/tech/2021/02/23/its-an-nft-boom-do-you-know-where-your-digital-art-lives/. Zugriff am: 2. August 2022.

[5] V. Tangermann, „NFTs Have a Huge Persistence Problem“, *Futurism*, 17. März 2021, 2021. [Online]. Verfügbar unter: https://futurism.com/nfts-have-huge-persistence-problem. Zugriff am: 2. August 2022.

[6] CheckMyNFT, *Check My NFT 🔎🖼 auf Twitter: „@jonty @cloudinary Btw we've been tracking this for 7 days now and most of the files we check from @niftygateway on IPFS fail“ / Twitter.* [Online]. Verfügbar unter: https://twitter.com/CheckMyNFT/status/1372253288863825925 (Zugriff am: 4. August 2022).

[7] ART HAUS, *On-chain NFTs and Why They're Better - ART HAUS.* [Online]. Verfügbar unter: https://art.haus/on-chain-nfts-and-why-theyre-better/ (Zugriff am: 1. August 2022).

[8] LarvaLabs, *Autoglyphs* (Zugriff am: 4. August 2022).

[9] Etherscan.io, *Ethereum Transaction Hash (Txhash) Details | Etherscan.* [Online]. Verfügbar unter: https://etherscan.io/tx/0x10757d45a56f93afdc78cc712553ba999e5a1a881be9139200be9f021a716712#eventlog (Zugriff am: 4. August 2022).

[10] Etherscan.io, *Ethereum Transaction Hash (Txhash) Details | Etherscan.* [Online]. Verfügbar unter: https://etherscan.io/tx/0x10757d45a56f93afdc78cc712553ba999e5a1a881be9139200be9f021a716712 (Zugriff am: 4. August 2022).

[11] Etherscan.io, *Ethereum Transaction Hash (Txhash) Details | Etherscan.* [Online]. Verfügbar unter: https://etherscan.io/tx/0x754661a46f11f62b311866a608d20034f940c3d3db6697564d26c2ad1fe9774a (Zugriff am: 4. August 2022).

[12] A. |. @Ruttkowa, „Completely “on chain” stored NFTs— what? - Alex | @ruttkowa - Medium“, *Medium*, 25. Sep. 2021, 2021. [Online]. Verfügbar unter: https://ruttkowa.medium.com/a-nft-stored-on-chain-what-fb890b6261ff. Zugriff am: 4. August 2022.

[13] *CardanoTrees.* [Online]. Verfügbar unter: https://cardanotrees.com/ (Zugriff am: 4. August 2022).

[14] 0xchain.art, *On-Chain Art.* [Online]. Verfügbar unter: https://www.0xchain.art/info (Zugriff am: 5. August 2022).

[15] w1nt3r_eth, *WINTΞR 🤍🤍 auf Twitter: „Next frontier in the NFT gas optimization game: put the data into the token id itself! The thread goes into more details ↓ https://t.co/FjlC0u98H3“ / Twitter.* [Online]. Verfügbar unter: https://twitter.com/w1nt3r_eth/status/1538229135897554944 (Zugriff am: 8. August 2022).

[16] A. Coathup, D. Martinelli, blockdev und A. Griffith, *EIP-4883 Composable SVG NFT by abcoathup · Pull Request #4888 · ethereum/EIPs.* [Online]. Verfügbar unter: https://github.com/ethereum/EIPs/pull/4888/files (Zugriff am: 8. August 2022).

[17] *SVG Minifyer.* [Online]. Verfügbar unter: https://www.svgminify.com/de.html (Zugriff am: 9. August 2022).

[18] A. Malz und I. Junghans, *Badges [internes Dokument].*

Verwendete Tools

Inkscape - https://inkscape.org/de/

Visual Studio Code - https://code.visualstudio.com/

Truffle Suite - https://trufflesuite.com/

Remix - https://remix.ethereum.org/

Base64 Encoder - https://base64.guru/converter/encode/image/svg

Polkadot-Governance versus Rechtliche Konzepte für Unternehmen, Staaten und DAOs

Gustav Hemmelmayr
Hochschule Mittweida, Technikumplatz 17, 09648 Mittweida

Blockchain-Governance wird immer wieder mit der Führung von Unternehmen oder von Nationalstaaten verglichen, obwohl diese sich oft eher als Decentralized Autonomous Organizations (DAOs) definieren. In diesem Beitrag werden rechtliche Konzepte, die den Rahmen für die Entscheidungsfindung in Unternehmen und Staaten bilden, sowie die Grundlagen einer DAO mit der Governance von Polkadot verglichen.
Im Ergebnis weist der Staat aufgrund der starken Prägung durch die physische Sphäre und der Selektion seiner Bürger die größten Unterschiede zur Polkadot-Governance auf. Von den Unternehmen ist die Genossenschaft in ihrem Ziel der Förderung der Mitglieder und Verwaltung gemeinsamer Infrastruktur, die sich jeweils auch in den Rechten der Mitglieder und der Besetzung der Organe niederschlägt, am nächsten. Die höchste Übereinstimmung hat die Polkadot-Governance jedoch mit der DAO, insofern als sie über die Zeit immer stärker den Gedanken der dezentralen und autonomen Entscheidungsfindung umsetzt.

Blockchain governance is often compared to the governance of companies or nation states, even if they often self-define as Decentralized Autonomous Organizations (DAOs). This paper compares legal concepts that provide the framework for decision-making in companies and nation states, as well as the fundamentals of a DAO, with Polkadot's Governance. In the result, the nation state is the most different due to the strong characterization through the physical sphere and the selection of its citizens. Of the enterprises, the cooperative is closest in its objective of promoting members and managing common infrastructure, which are also reflected in the rights of members and the composition of bodies. However, Polkadot governance is most similar to a DAO in that it gradually implements the idea of decentralized and autonomous decision-making.

1. Einleitung

In dieser Arbeit soll zu Beginn die Polkadot-Governance in ihrer aktuellen und ihrer zukünftigen Form dargestellt und in der Folge analysiert werden, in welchen Punkten es Ähnlichkeiten zu oder Unterschiede von rechtlich gesetzten Rahmenbedingungen für Entscheidungsfindung in Unternehmen, Staaten und DAOs gibt, um letztlich auch darzustellen, welchen dieser Konzepte die Polkadot-Governance am ähnlichsten ist.

2. Blockchain & Polkadot-Governance

Im Gegensatz zu Governance-Strukturen aus der realen Welt, könnte man annehmen, dass Governance in IT-Systemen einfacher zu überblicken sind, weil sie sich im Code direkt manifestieren, unmittelbar und eindeutig erfahrbar und damit auch einfach analysierbar sind. Fischer & Valiente [1] hingegen schreiben, dass jede Art von Governance letztlich ein soziales Konstrukt ist, das nicht nur aus Gesetzen (oder Satzungen), sondern auch aus Normen, Kultur, Institutionen und Personen besteht. Mini & Gregory [2, S. 2] attestieren, dass man traditionell im Bereich Software-Governance von Governance *of* IT sprach; man beschäftigte sich beispielsweise damit, wie ein bestehendes IT-System am Laufen gehalten oder an neue Bedürfnisse oder Technologien angepasst werden kann. Mit dem Aufkommen von Decentralized Autonomous Organizations, kurz DAOs, ist ein Shift in Richtung Governance *via* IT zu bemerken. Das spezifisch Neue an Blockchains ist laut Fischer & Valiente [1], dass sie Systeme ermöglichen, in denen die Einhaltung von Verfahren automatisch durchgesetzt wird, wobei sie sich weder auf Normen noch auf ein Rechtssystem stützen und keinen Raum für individuellen Ermessensspielraum lassen.

Ein weiteres Missverständnis ist laut Fischer & Valiente [1], dass die Bezeichnung Blockchain-Governance in zwei völlig unterschiedlichen Kontexten nahezu unterscheidungslos gebraucht wird. In der einen Verwendung referenziert Blockchain-Governance auf die Governance *über* die Blockchain, während die andere Blockchain-Governance sich der Frage der Nutzung von Blockchain *für* Governance widmet.

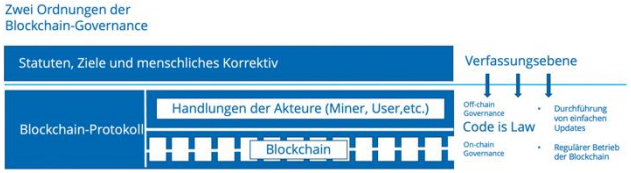

Abbildung 1: Zwei Ordnungen der Blockchain-Governance
Grafik des Autors nach Fischer & Valiente und Mini & Gregory

Auf der Ebene des Protokolls wirken Blockchain und ihre Akteure zusammen, um on-chain und off-chain Governance im regulären Betrieb der Blockchain sowie Durchführung von einfachen Updates zu koordinieren, während auf einer darüberstehenden Ebene die Governance über die Blockchain selbst stattfindet, die sich nach Statuten und Zielen richtet und ein menschliches Korrektiv ermöglicht.

In Polkadot sind diese zwei Ordnungen der Governance auf einem Metaprotokoll aufgesetzt [3, 12:11], sowie mit Parachains, Bridges und der Ausgabe von Geldern an andere Projekte über die Treasury-Schnittstellen geschaffen, die die Interaktion innerhalb des eigenen, sowie mit anderen Ökosystemen erlauben und zusätzlich die Förderung neuer Ökosysteme ermöglichen, sodass die Struktur in Polkadot wie in Abbildung 2 aussieht.

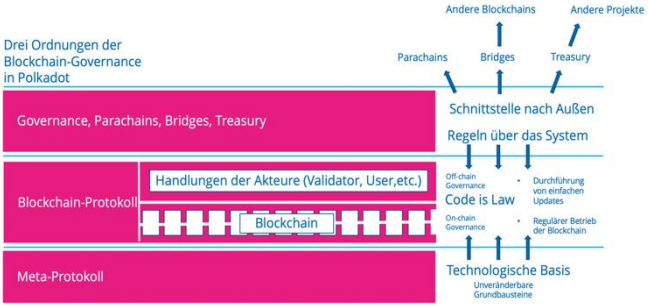

Abbildung 2: Drei Ordnungen der Polkadot-Governance
Grafik des Autors auf Basis Wood, 2020 [3],

Im Folgenden soll nun die Governance über das Polkadot-Protokoll[1] dargestellt werden, die in der Grafik als „*Regeln über das System*" bezeichnet ist.

2.1. Polkadot-Governance 1.0

Die Governance in Polkadot ist autonom und besteht aus drei zentralen Elementen: stimmengewichteten Referenda, dem gewählten Council und einer finanzierten Treasury [3, 18:50]. Einen Überblick über das aktuelle Dreikammern-System der Governance [4, 3:33], bestehend aus Token-Holdern[2], Council und Technical Committee gibt Polkadot mit Abbildung 3. In der Grafik erkennt man, wie alle Governance-Entscheidungen von den DOT-Holdern ausgehen, die direkt Public-Proposals

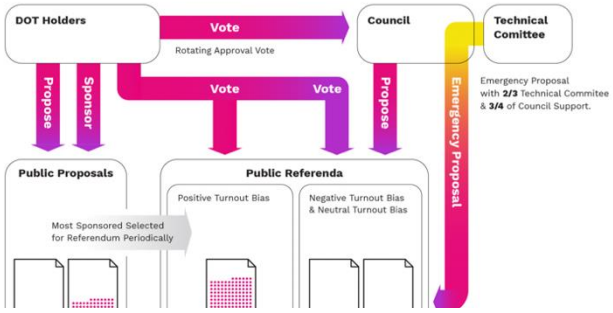

Abbildung 3: Überblick Polkadot-Governance [17]

vorschlagen und unterstützen, über Public-Referenda abstimmen und das Council wählen können. Das Council wiederum kann selbst Proposals für Referenda abgeben sowie die Mitglieder des Technical-Committee bestimmen. Das Technical-Committee kann mit Unterstützung des Councils Emergency-Proposals für Public-Referenda einbringen. Alle Public-Referenda benötigen wiederum die Zustimmung der DOT-Holder, die über Public-Referenda abstimmen, wobei immer abwechselnd ein Public-Referendum des Councils und eines aus einem Public-Proposal abgehalten wird und die erforderlichen Zustimmungsquoren davon abhängen, ob es sich um ein Public-Proposal, ein Proposal des Councils mit Stimmenmehrheit, ein Proposal des Councils mit Einstimmigkeit oder ein Proposal des Technical-Committees mit Zustimmung des Councils handelt.

Neben den oben beschriebenen Mitteln der on-chain-Governance gibt es zahlreiche off-chain-Vernetzungen und Zusatzinformationen über die Governance –beispielsweise über *Subscan* [26]. Dadurch werden die Inhalte von anstehenden Entscheidungen laufend publiziert und können in Referenz darauf auch in anderen online-Foren wie *Riot/Element*, *Twitter*, *Discord*, etc. dezentral diskutiert werden oder auch dafür geworben werden, an der Abstimmung teilzunehmen.

2.2. Änderungen in der Polkadot-Governance 2.0

Am 29. Juni 2022 verkündete Gavin Wood im Rahmen der Konferenz „*Polkadot Decoded*", wie die nächste Generation der dezentralisierten Governance in naher Zukunft aussehen soll. [4]

Mit der neuen Governance sollen einerseits konkrete Probleme der bestehenden Governance gelöst werden [4, 5:30], die neue Governance soll aber auch einen nächsten Schritt zur weiteren Dezentralisierung darstellen, indem das Council und das Technical Committee abgeschafft werden. Über die Mitglieder des Council wurde zwar dezentral gewählt, nichtsdestotrotz sind bisher Mitglieder mit ihren Namen sichtbar für bestimmte Entscheidungen zuständig und dies stellte ein Risiko der Zentralisierung auf diese Personen dar. [4, 6:20]

Die Sicherheit von Vorschlägen für ein Referendum wird zukünftig anhand von zwei Kriterien in Bezug auf ihre möglichen Auswirkungen kategorisiert: nach der Operation, die vorgeschlagen wird, und nach dem Ursprung des Vorschlags [4, 12:57]. Nun soll es dementsprechend in der Governance zahlreiche unterschiedliche Tracks – quasi Pipelines – mit unterschiedlichen Parametern und Schwellenwerten geben. Dafür wird der Abstimmungszyklus eines Referendums in der Governance 2.0 angepasst und soll nunmehr aus den folgenden Phasen bestehen: Vorschlag, Entscheidungsphase, Bestätigungs-

[1] Außer Acht bleibt dabei die Ebene „*Code is Law*", die den jeweiligen Stand der Blockchain herstellt, also die oben als Governance *über* die Blockchain bezeichnet wurde, sowie die darunterliegende technologische Basis des Meta-Protokolls.

[2] Ebenfalls außer Acht bleibt für diese qualitative Betrachtung des Polkadot-Governance-Systems die Aufteilung der DOTs auf bestimmte Personen oder Personengruppen, sowie deren jeweiliges Abstimmungsverhalten in der Governance.

phase, Ende sowie ggf. Umsetzungsphase. [4, 17:35], wobei ein Referendum in jeder dieser Phasen gekippt werden kann. [4, 30:10] Durch agile Delegierung können DOT-Holder ihre Stimme für jeden Ursprung eines Referendums auf unterschiedliche Wähler übertragen [4, 31:24] und für zeitkritische Referenda soll es einen Whitelisting-Prozess geben, in dem diese eine Art Vorprüfung durch eine neu geschaffene Fellowship durchlaufen und dann eine vereinfachte Abstimmung bekommen [4, 37:00]. *Last but not least* werden in der Governance 2.0 durch die Abschaffung des Councils auch Tipps, Treasury-Ausgaben über Referenda gemacht. [4, 43:50]

In der Governance 2.5 sollen dann zusätzlich passive Delegierungen, also das Delegieren der Stimmen ohne Transaktion und damit ohne Gebühren, sowie die kostenfreie Aufhebung der Delegierung implementiert werden. [4, 33:57]

3. Vergleich Polkadot mit Unternehmen

Ähnlich wie ein Unternehmen wurde auch Polkadot gegründet, allerdings nicht als Unternehmen, sondern als Vorzeigeprojekt der Web3 Foundation, einer Stiftung nach Schweizer Recht, und mit Hilfe der Parity Technologies Limited [11, 12].

Die Intention der Gründung war dabei nicht der unternehmerische Zweck oder die Bindung an ein bestimmtes Gewerbe, sondern ein Beispiel für ein voll funktionierendes und nutzerfreundliches, dezentrales Netz zu erschaffen.

Teil des Polkadot-Ökosystems, das als Blockchain-Protokoll angelegt ist, ist die Kryptowährung DOT. Der DOT wurde in mehreren Sales Runden verkauft [5, 6].

Damit hat Polkadot insofern eine Gemeinsamkeit mit Aktiengesellschaften, als der Verkauf des DOT *prima facie* ähnlich aussieht, wie ein Aktienverkauf zur Finanzierung einer Aktiengesellschaft. Tatsächlich hat aber mangels eigener Rechtspersönlichkeit nicht Polkadot, sondern die Web3 Foundation die DOTs verkauft [7]. Diese kann nur im Rahmen ihres Stiftungszwecks tätig werden und ist gemeinnützig [8].

Die Einnahmen aus den Sales kommen nicht nur Polkadot zugute, sondern werden auch zur Förderung von Projekten im Rahmen eines Grants-Programmes verwendet [9], sowie für andere Projekte [10, 11 ,12]. Aufgrund der Zweckgebundenheit des Vermögens der Web3 Foundation scheiden Gewinnauszahlungen aus. [13]

Im Unterschied zu Aktien als Anteile einer Aktiengesellschaft ist der DOT durch den Polkadot zugrundeliegenden Code determiniert und ist seine Funktionalität im Netzwerk durch Governance-Beschluss veränderbar, während Aktien nur in jenen Arten ausgegeben werden können, die diesen rechtlich zugesprochen werden. [14]

Ein weiterer Unterschied zu Aktien ist die konkrete Governance-Ausübung über den DOT, während Aktionär*innen keinen direkten Einfluss auf das unternehmerische Handeln der Aktiengesellschaft haben [14, 15]. DOT-Holder haben wie oben gezeigt schon in der Governance 1.0 eine direkte Mitbestimmung hinsichtlich aller Proposals. Darüber hinaus sind sie derzeit noch an den personellen Entscheidungen über die Mitglieder des Councils unmittelbar beteiligt. Mit der neuen Polkadot-Governance 2.0 und der Abschaffung des Councils und des Technical-Committees fallen personelle Entscheidungen weg und sollen alle Entscheidungen – auch Tipps und Treasury Ausgaben – über Referenda gemacht werden. [4, 43:50] Damit wird die Entscheidungsfindung in Polkadot hinsichtlich aller Angelegenheiten vollständig in die Hände der DOT-Holder gelegt.

Im Gegensatz zur Aktie ist mit dem Halten des DOT keinerlei Gewinnausschüttung verbunden.

Auch die Genossenschaft [16] gibt ihren Mitgliedern nicht mehr Rechte an der Mitbestimmung als die Aktiengesellschaft – Hauptunterschied in der Entscheidungsfindung ist, dass die Genossenschaftsmitglieder ein Stimmrecht pro Kopf statt pro Anteil haben.

Die Idee einer Stimme pro Person wie sie in der Genossenschaft gelebt wird, scheitert in einem Blockchain-Ökosystem daran, dass die Identität hinter der Wallet nicht offengelegt ist und die Anzahl der Wallets einer Person nicht begrenzbar ist. Stattdessen wird mit dem Conviction-Voting [17] jenen, die ein langfristigeres Interesse am Ausgang der Entscheidung und an dem Netzwerk an sich haben, ein Vielfaches ihrer DOTs als Stimmen gegeben [4, 4:40].

Hinsichtlich der Repräsentation – in der Kapitalgesellschaft [15] wie in der Genossenschaft [16] typischerweise durch den Vorstand, ggf. kontrolliert von einem Aufsichtsrat – hat Polkadot derzeit noch Vertretungsorgane, die mit der Governance 2.0 wegfallen.

Das noch existierende Council hat mit den repräsentativen Organen der Genossenschaft gemein, dass nur Personen, die auch über DOT verfügen, Mitglied des Council werden können.

Hinsichtlich der DAO LLC aus Wyoming sei noch kurz angemerkt, dass die Polkadot-Governance sehr wahrscheinlich die gesetzliche Grundlage der zugrundeliegenden Norm WY Stat § 17-31-109 [18] erfüllen könnte. Dafür müsste sie die konkrete Ausgestaltung der Governance in einer Satzung regeln, könnte dann einen in Wyoming ansässigen eingetragenen Vertreter bestimmen und eine DAO LLC anmelden.

Allerdings würde durch eine solche Anmeldung einer DAO LCC die Identität von Polkadot geändert werden – Polkadot wäre dann eine Gesellschaft beschränkter Haftung, also eine Kapitalgesellschaft.

Die Eintragung einer DAO LLC hat eine gesellschaftsrechtliche Funktion, die DOT-Holder wären damit automatisch Eigentümer*innen von Polkadot. An ihren Rechten in Polkadot mitzubestimmen, würde dies nichts ändern, aber die Qualität des DOT wäre verändert – die DOT-Token würden dann unmittelbar für das anteilige Eigentum an Polkadot stehen.

Als Gründer einer DAO LLC müsste am ehesten die Web3 Foundation auftreten, deren Projekt Polkadot ist. Ob das mit ihrem Stiftungszweck vereinbar ist, müsste man nach Schweizer Stiftungsrecht prüfen.

Zusammenfassend kann man sagen, wenn man nach dem Grundsatz *substance over form*, den auch die United States Securities and Exchange Commission (in der Folge kurz SEC bezeichnet) [24, S. 11] anwendet, dass Polkadot im Vergleich zu Unternehmen am ehesten als Genossenschaft zu sehen ist. In Polkadot wird eine gemeinsame Infrastruktur geschaffen, von den Beteiligten verwaltet und kontinuierlich weiterentwickelt. Das enge Korsett einer DAO LCC passt hier ebenfalls nicht, weil hier zwar die Form der virtuellen Organisation mit eingebunden ist, die Substanz der Rechtsform aber auf Eigentumsverhältnissen an der Infrastruktur, Gewinnorientierung und Haftungsbeschränkung liegt, nicht auf der angestrebten Schaffung einer gemeinsamen technischen Infrastruktur und eines gemeinsamen Ökosystems. Die Struktur einer Aktiengesellschaft passt hier noch weniger, weil es bei der Aktiengesellschaft um gemeinschaftliche Investition, zur Streuung von Risiko und zur Erlangung von Gewinnen geht, ohne dass gemeinschaftliche Nutzung miteinbezogen wird.

4. Vergleich Polkadot mit Staaten

Ausgehend von den Voraussetzungen eines Staates in Form von Staatsgewalt, Staatsvolk und Staatsgebiet [25, S. 32ff], findet man einige Parallelen im Polkadot-Ökosystem.

So ist die Staatsgewalt repräsentiert durch den Code, der im Meta-Protokoll die Etablierung von Polkadot als Blockchain mit Parachains samt Governance erlaubt. Innerhalb dieses Codes werden Entscheidungen per Referendum oder vom Council gefällt und direkt im Code umgesetzt. Diese Polkadot-Staatsgewalt ist funktional, solange kein Fehler im Code den Vollzug von Entscheidungen verhindert oder Hackerangriffe Änderungen vornehmen – ähnlich wie die Staatsgewalt intakt ist, solange nicht eine Armee einmarschiert oder ein Bürgerkrieg sie außer Kraft setzt.

Als Staatsvolk kann man die DOT-Holder sehen, die ähnlich wie Staatsbürger oder Bewohner eines Landes von der vorhandenen Infrastruktur profitieren, dort ihre Businessmodelle umsetzen und sich über die Polkadot-Governance an den Entscheidungen des Netzwerks beteiligen können. Derzeit werden die DOTs in knapp einer Million Wallets gehalten [26], es handelt sich also noch eher um einen kleinen Staat. Anders als im Staat, in dem Bürger*innen den Status beispielsweise automatisch *qua* Geburt oder auf Antrag erwerben, müssen Personen, die im DOT-Ökosystem mitwirken wollen, DOT-Token erwerben. Ebenfalls anders als im Staat gibt es keine Beschränkungen, wer DOT-Holder*in werden kann oder darf und auch keine Exklusivität, sodass jemand auch nebenbei zahlreiche andere Kryptowährungen halten kann. Es gibt – ebenfalls anders – auch gar keine Erfassung, wer einen Coin hält, sodass Polkadot selbst zumindest allein aufgrund des Besitzes von DOT gar nicht weiß, wer Teil ihrer Community ist und wer nicht. Die Möglichkeit, einer Wallet einen Namen zu geben, kann darauf hinweisen, wer die Wallet hält – eine Überprüfung der dahinterstehenden Identität wird allerdings nicht durchgeführt [27, 28]. DOT-Token können von natürlichen Personen, juristischen Personen und jeglicher anderen handlungsfähigen Entität gehalten werden und Exchanges können auf einer oder mehreren Wallets die DOTs für sämtliche ihre Kunden verwalten; auch der Zugriff auf DOT-Token per Bot ist denkbar, solange dahinter jemand steht, der diese bezahlen kann und für den der Bot dann tatsächlich agiert. Als Bewohner der Polkadot-Infrastruktur, ggf. sogar, ohne im Besitz von DOT-Token zu sein, kann man die Nutzer der Parachains sehen – diese nutzen die Vorteile der Relay-Chain indirekt mit ohne dass sie deswegen in Polkadot direkt involviert sein zu müssen.

Bezüglich des Staatsgebietes gibt es kein entsprechendes, physisches Territorium, man könnte aber die technische Infrastruktur in dem Polkadot lebt, als Gebiet sehen, in dem auch die Staatsgewalt ausgeübt wird.

Zusammenfassend kann man sagen, dass es zu den drei Säulen des Staates teilweise parallele Konstrukte in Polkadot gibt, dass diese aber aufgrund der Natur des Polkadot-Protokolls als virtuelle Infrastruktur und digitales Netzwerk andere Ausprägungen hat.

Hinsichtlich der Aufgaben eines Staates [25, S. 198] und ob diese mit Polkadot vergleichbar sind, meint Gavin Wood, dass schon Bitcoin zwei wesentliche Elemente eines Staates aufweist – die Miner, die wie eine militärische Einheit für die Sicherheit des Netzwerkes zuständig sind, und eine eigene Währung. Er ist überzeugt, dass es in Blockchain- bzw. Krypto-Ökosystemen viel mehr solcher staatlichen Elemente und Staatsapparate geben wird. Eines der Elemente, die diese staatsähnlichen Gebilde ausmachen, ist, dass diese Botschaften brauchen, um mit anderen Staaten interagieren zu können. Dies ist im Interesse aller, denn wer miteinander interagieren kann, kann Handel treiben und davon profitieren alle Beteiligten. [3, 5:55]

In diesem kurzen Abschnitt sind schon mehrere Komponenten und Aufgaben eines Staates angesprochen – die innere und äußere Sicherheit, ein funktionierendes Währungssystem und eine Außenpolitik zur Verbesserung der wirtschaftlichen Lage [25, S. 198].

Die Sicherheit von Polkadot wird auf der Ausführungsebene der Blockchain durch die Relay-Chain und ihren

Proof-of-Stake Algorithmus, das Zusammenspiel von Validatoren, etc. gewährleistet, notfalls kann das Technical-Committee eingreifen, wenn die Sicherheit durch einen Fehler bedroht ist. [29] Auf der Ebene der Governance über die Blockchain, also der Entscheidungsfindung rund um die eigentliche Blockchain, gibt es derzeit das Council, das mit einer Regierung vergleichbar, eine Richtung vorgibt, dabei aber Legitimation durch öffentliche Abstimmungen benötigt. Nach Abschaffung von Council und Technical-Committee soll die Sicherheit durch ein komplexes, aber anwenderfreundliches Wahlsystem gewährleistet werden [4, 20:55].

Das funktionierende Währungssystem ist über den DOT-Token repräsentiert. Dieser ist für das Abstimmen über Parachains und für die Governance-Teilnahme verwendbar, Belohnungen werden damit ausbezahlt und er kann frei gehandelt werden, sodass die Belohnungen auch in andere Ökosysteme transferiert werden können.

Die Kommunikation zwischen unterschiedlichen Parachains in Polkadot funktioniert mit XCM und die Kommunikation nach außen findet über sogenannte Bridges statt. Dadurch wird der von Wood erwähnte Handel möglich – über Bridges können direkt DOT oder andere Währungen aus dem Polkadot-Ökosystem mit Währungen anderer Blockchains – beispielsweise Ethereum – getauscht werden. [29]

Hinsichtlich der Ziele des „Staates" Polkadot kann man in der Einleitung zum Whitepaper nachlesen, dass andere Blockchains schon einige Anwendungen ermöglichen, dass aber die technologischen Versprechungen noch auf relevante Umsetzung in der realen Welt warten. Als Gründe dafür werden das Fehlen von Skalierbarkeit, Isolierbarkeit, Entwickelbarkeit, Governance sowie Anwendbarkeit angeführt [30, S.1]. Mit den im Whitepaper etablierten Grundlagen sollen die ersten beiden Problemfelder – die Skalierbarkeit und die Isolierbarkeit – gelöst werden. Aber auch die anderen Themenkreise hat Polkadot inzwischen adressiert – für die Entwicklung hat Polkadot umfassende Materialien im Polkadot-Wiki zur Verfügung gestellt [beispielsweise 29], für die Governance gibt es kontinuierliche Weiterentwicklungen und um Polkadot ist ein ganzes Ökosystem von Anwendern gewachsen, die sich in den Parachains von Polkadot und Kusama mit ihren speziellen Anwendungen befassen [31, 32].

Bisher gab es drei Gremien, die als Organe der Polkadot-Governance fungieren – die DOT-Holder, das Council und das Technical Committee. Aufgrund der geringeren Anzahl an Organen, der gleichzeitigen Zuständigkeit für alle Entscheidungen und den Vorbehalt der Zustimmung der DOT-Holder in allen Referenda, gab es keine Gewaltenteilung in Legislative, Exekutive und Judikative in dem Sinn, wie das in Staaten üblich ist (vgl. beispielsweise Art. 20 Grundgesetz für die Bundesrepublik Deutschland – in der Folge mit GG abgekürzt). Man könnte allerdings argumentieren, dass es diese auch nicht braucht, weil Staaten diese ja einführen, um zu verhindern, dass die Organe die vom Volk kommende Macht missbrauchen, während in Polkadot alle Gesetzgebung direkt von den DOT-Holdern bestätigt werden muss. Damit ist anstelle der Gewaltenteilung eine sehr ausgeprägte Partizipation der Betroffenen, insbesondere die Einflussnahme des „Volkes" auf die Willensbildung und Entscheidungsfindung, gegeben.

Die Ausführung von Entscheidungen erfolgt direkt im Code, sodass es dafür keiner gesonderten Ausführungsorgane bedarf.

Polkadot hat eine quasi-föderale Struktur ähnlich wie der deutsche Staat mit seinen Bundesländern (Art. 20ff GG) – es gibt nicht nur Polkadot als Blockchain-Projekt, sondern die in Polkadot etablierten Parachains beherbergen jeweils nochmal eigene Projekte. Über die Aufnahme als Parachain-Projekt stimmen die DOT-Holder ab, indem sie im Rahmen eines Crowd-Loans ihre DOT für ein bestimmtes Projekt gelockt halten. Auch hier gilt, wie im deutschen Grundgesetz, dass quasi Bundesrecht Landesrecht schlägt (Art. 31 GG) – wenn die Relay-Chain ein Update bekommt, so müssen die Parachains dieses ggf. in ihren eigenen Strukturen weitertragen, um das weitere Funktionieren ihrer Infrastruktur sicherzustellen. [33]

Im Unterschied zu den Bundesländern sind die Parachains immer nur für einen bestimmten Zeitraum vergeben [33].

5. Vergleich Polkadot mit Decentralized Autonomous Organizations

Laut der SEC ist eine Decentralized Autonomous Organization eine virtuelle Organisation, die in Computercode verkörpert ist und auf einem verteilten Ledger oder eine Blockchain ausgeführt wird [24, S. 1]. Des Weiteren geht aus dem Report über *The DAO* hervor, dass für die Qualifizierung als DAO der Erfolg eines Projektes nicht unbestreitbar von den Bemühungen einzelner Personen oder Gruppen abhängen sollte und dass die Governance tatsächlich autonome Entscheidung durch die Token-Holder zulässt [24, S. 12ff]. Für die Qualifikation als DAO ebenfalls dienlich erscheint es, wenn ein Projekt die Technologie, die Verwendbarkeit für User und Features in den Vordergrund stellen und die technologische Infrastruktur tatsächlich genutzt wird, sowie, dass in diesen Zusammenhängen auch die Vermarktung und der Verkauf von Token so von statten geht, dass die technologische Perspektive über Anreize zur Spekulation etc. überwiegen [34]. Darüber hinaus erkennt die SEC an, dass Dezentralisierung eines Netzwerkes ein Projekt ist, das über einen bestimmten Zeitraum erfolgt, sodass selbst wenn die Voraussetzungen ursprünglich nicht erfüllt gewesen sein sollten, ein Projekt dennoch mit der Herstellung der entsprechenden Voraussetzungen, als vollständig dezentralisiert gesehen werden kann [34, 35].

Wenn es gegen ein autonomes Netzwerk spricht, dass die Anstrengungen von anderen als dem Investor unbe-

streitbar bedeutsam sind und derartig essenzielle Managementbemühungen darstellen, dass diese über den Erfolg oder Misserfolg des Unternehmens entscheiden [24, S. 12], heißt das im Umkehrschluss, dass bei einem autonomen dezentralen Netzwerk der Erfolg oder Misserfolg nicht von einzelnen Personen oder Gruppen abhängen sollte bzw. es zumindest bestreitbar sein sollte, dass deren Managementbemühungen essenziell wären. Die Argumentation der SEC selbst ist hier eine Gratwanderung und Begriffe wie „*unbestreitbar*" und „*essentiell*" sind relativ dehnbar.

Relativ griffig jedoch ist der Begriff Managementbemühungen – „*entrepreneurial or managerial efforts of others*" – dabei geht es um jene Bemühungen auf Managementebene, die den wirtschaftlichen Erfolg eines Unternehmens ausmachen. Mehrere Argumentationen sprechen dafür, dass die Bemühungen von Gründern, Foundation und Parity keine solchen Managementbemühungen sind.

Generell kann man sehen, dass eine komplexe Governance wie oben für Polkadot beschrieben, effektiv dazu dient, dass die tatsächlichen Entscheidungen, unabhängig von den jeweiligen Vorarbeiten, eben nicht von den Gründern oder dahinterstehenden Unternehmen gefällt werden, sondern von jenen, die die Infrastruktur benutzen und daher über entsprechende DOTs verfügen.

Einer der wichtigsten Faktoren für den Erfolg des Polkadot-Ökosystems ist die Wahl der Projekte, die sich in den Parachains niederlassen, weil diese innerhalb von Polkadot unterschiedlichste Features und Anwendungsmöglichkeiten bauen, die auch eine kommerzielle Nutzung erlauben [31, 32]. Die Entscheidung, wer einen solchen Slot bekommt, treffen die DOT-Holder.

Die Arbeit von Gavin Wood zur Erneuerung der Governance, wie sie von ihm am 29. Juni 2022 als „*meine Arbeit im letzten Jahr*" [4, 1:35] vorgestellt wurde, findet sich tatsächlich auf GitHub als Pull-Request, das zur Genehmigung aussteht. Öffentlich sichtbar haben vier Accounts darin gearbeitet, möglicherweise waren es mehr, die nicht *public* gestellt sind [36]. Bei einer Management-Entscheidung würde typischerweise nun jemand, der die hierarchische Befugnis dazu hat, beschließen, ob dieser Code verwendet werden soll, oder eben nicht. In Polkadot wird die tatsächliche Managemententscheidung, ob die neue Governance eingeführt werden soll, von der Community getroffen, nachdem sie Gelegenheit hatte, die neue Governance zu prüfen und auszuprobieren. [4, 44:20]

Die Web3 Foundation unterstützt Web 3.0-Teams und Open-Source-Projekte durch Finanzierung, Förderung, Forschung und Kooperationen [9, 10]. Parity Technologies Limited ist ein Unternehmen in der Software-Entwicklung und arbeitet ebenfalls an Polkadot mit [11]. Diese Art der Arbeit, die die Foundation und Parity unter anderem für Polkadot leisten, ermöglicht neue Projekte, greift aber nicht in deren Management ein.

Hinsichtlich der Dezentralität der Entscheidungsfindung kann man mit Verweis auf die Ausführungen zur Governance von Polkadot sagen, dass in Polkadot effektiv alle Abstimmungen sowohl direkt als auch ggf. zusätzlich indirekt von den DOT-Holdern ausgehen und letztlich der Zustimmung der DOT-Holder bedürfen. Nur die Quoren, die für die Annahme eines Referendums notwendig sind, variieren, je nach Herkunft des Referendums.

In der Governance 2.0 fallen das Council und das Technical-Committee weg, sodass alle Entscheidungen, die getroffen werden, allein von der DOT-Öffentlichkeit eingebracht, abgestimmt und in der letzten Phase nicht verhindert werden.

Mit dem Fellowship-Programm [4, 37:00] soll darüber hinaus eine möglichst große Anzahl an Experten geschaffen werden, sodass einerseits eine wachsende Gruppe selbst hohe Kompetenz in den für Polkadot relevanten Themen entwickelt, diese dann aber auch der*m einfachen Wähler*in für Fragen zu anstehenden Referenda, für entsprechende Evaluationen bezüglich der geplanten Änderungen, und für breite öffentliche Diskussionen zur Verfügung steht – ähnlich, wie das bei *The DAO* die Gründer und die Kuratoren getan haben, nur eben dezentral organisiert und nicht eingeschränkt auf eine bestimmte, abgeschlossene Gruppe.

Diese Fellowship soll auch dazu dienen, im Falle von Angriffen oder Schwachstellen, ein Referendum durch einen schnelleren Prozess zu schicken [4, 37:00], sodass auch hier immer größere Unabhängigkeit von den Gründern oder Gesellschaften hinter Polkadot bestehen soll.

Diese Änderungen in der Governance 2.0 zeigen auch gut, wie Dezentralisierung als Projekt funktioniert, indem anfangs die Entscheidung für alle Teilnehmer*innen geöffnet wird, dann aber dieser *status quo* auch immer weiter verbessert wird, sodass mit dem Wachstum des Ökosystems und der Verbreitung des Wissens über die Technologie auch bestehende und erprobte Strukturen hinterfragt und weiter aufgeweicht werden, ohne dabei die Sicherheit des Netzwerks zu gefährden.

Hinsichtlich der technischen Verwendbarkeit des Polkadot-Protokolls sei nochmal auf die zahlreichen Parachains verwiesen, die dort unterschiedliche, nützliche Projekte im Ökosystem vorantreiben. Nebenbei bemerkt scheint dieses Feature öffentlich als sehr wertvoll eingeschätzt zu werden, sind doch teilweise sehr hohe Summen für Parachains gebunden [31,32].

Auch die öffentliche Kommunikation beispielsweise auf *Twitter* oder *Youtube* [38, 39] fokussiert sich auf Software, technologische Neuerungen, Hackathons, Wachstum des Ökosystems durch neue Parachains sowie Governance, um nur einige Themen zu nennen, und spricht gar nicht von DOTs als digitalem Vermögenswert oder regt sonst irgendwie zu spekulativen Investitionen in DOT an.

Insgesamt sieht man starke Parallelitäten zwischen der Polkadot-Governance und der von der SEC im Umkehrschluss für *The DAO* definierten Governance einer Decentralized Autonomous Organization. Polkadot könnte damit eine DAO sein, auch weil, deren technologische Funktionalitäten in ihrer Kommunikation im Vordergrund stehen und diese Funktionalitäten auch tatsächlich schon genutzt werden. Darüber hinaus findet sich Polkadot in einem kontinuierlichen Prozess, der danach strebt, die Dezentralisierung und Autonomie von den ursprünglichen Gründern auf allen Ebenen immer weiter zu verstärken.

Als einzige zentralistische Elemente der dezentralen Struktur könnte man – derzeit noch – das Council und das Technical Committee ansehen; bei näherer Betrachtung ist die Besetzung des Council allerdings einer ständigen demokratischen Bestätigung unterworfen und damit auch das Technical Committee, das von Council ernannt wird.

6. Fazit

Mit Staaten hat Polkadot einiges gemein, insofern als Polkadot ähnlich wie ein virtueller Staat funktioniert – also Entscheidungen autonom trifft und sich nicht als eine Gesellschaft nach einer bestimmten Rechtsordnung verhält. Die Aufgaben, die zur gemeinschaftlichen Erledigung stehen und die Organe, die dafür tätig werden, weisen einige Ähnlichkeiten zu einem Staat auf, allerdings ist Polkadot aufgrund der fehlenden physischen Komponente sehr anders konfiguriert, hat eine viel niedrigere Komplexität und verwendet anstelle von Gewaltenteilung zunehmend starke Elemente direkter Legitimation von Entscheidungen durch die DOT-Holder.

Abbildung 4: Gemeinsamkeiten und Unterschiede
Grafik des Autors

Als Unternehmen wäre Polkadot am ehesten mit einer Genossenschaft zu vergleichen, weil in Polkadot eine technische Infrastruktur gemeinschaftlich verwaltet wird und über deren weitere Entwicklung gemeinschaftlich bestimmt wird. Vertretungsorgane sind ebenso wie bei Genossenschaften mit Mitgliedern der Community besetzt, die entsprechend auch DOT halten müssen um teilnehmen zu können. Im Gegensatz zur Genossenschaft, die ihre Mitglieder durch die Schaffung von gemeinsamem Vermögen oder gemeinschaftliche verwalteter Infrastruktur gegen die Konkurrenz durch mächtigere Unternehmen schützen möchte, versucht Polkadot mit Innovation der Öffentlichkeit einen Web 3.0 Baustein zur Verfügung zu stellen, um die im Web 2.0 zu mächtig gewordenen Unternehmen in Schranken zu weisen.

Am ähnlichsten sieht Polkadot der DAO, wie sie von der SEC abgegrenzt wurde, weil sie tatsächlich zunehmend dezentralisiert autonome Entscheidungen für die Halter*innen ihrer DOT organisiert und bei der Gebarung von Polkadot die Zurverfügungstellung von funktionierender, öffentlich nutzbarer Infrastruktur im Vordergrund steht und diese auch schon genutzt wird.

Literaturverzeichnis

[1] Fischer, Aron, Valiente, Maria-Cruz (2021): Blockchain Governance. In Internet Policy Review. Journal on internet regulation. Governance Volume 10 Issue2. 20.04.2021. https://doi.org/10.14763/2021.2.1554, abgerufen am 17.06.2022

[2] Mini, Tobias, Gregory, Robert Wayne (2021): An Exploration of Governing via IT in Decentralized Autonomous Organizations, Conference Paper, December 2021. https://www.researchgate.net/publication/355483453_An_Exploration_of_Governing_via_IT_in_Decentralized_Autonomous_Organizations, abgerufen am 17.06.2022

[3] Wood, Gavin (2020): A Walkthrough of Polkadot's Governance. Polkadot-Youtube-Kanal. Veröffentlicht 07. Juli 2020. https://www.youtube.com/watch?v=o8sAhDY6IyY, abgerufen am 25. Juni 2022

[4] Wood, Gavin (2022) Governance v2. At: Polkadot Decoded 2022, Buenos Aires, Main Stage. 29. Juni 2022. https://www.youtube.com/watch?v=EF93ZM_P_Oc abgerufen am 3. Juli 2022.

[5] Lange, Guido: Ethereum Mitgründer: Polkadot (DOT) sichert sich durch Private Sale 43,3 Millionen US-Dollar. In: Block-Builders.de. Dein Themenportal für Finanzen und Blockchain. 29. Juli 2022. https://block-builders.de/ethereum-mitgruender-polkadot-dot-sichert-sich-durch-private-sale-433-millionen-us-dollar/, abgerufen am 18. Juli 2022.

[6] Polkadot: Redenomination of DOT. General. https://wiki.polkadot.network/docs/redenomination, abgerufen am 18. Juli 2022.

[7] Cuen, Leigh, Zaho, Wolfie: $1 Billion Valuation May Elude Ethereum Co-Founder's New Blockchain Polkadot. Polkadot's bid for unicorn status has hit a snag, with three Chinese funds buying into the token sale at valuations below $1 billion. In: CoinDesk. 5. Juni 2019. https://www.coindesk.com/markets/2019/06/05/1-billion-valuation-may-elude-ethereum-co-founders-new-blockchain-polkadot/, abgerufen am 18. Juli 2022.

[8] Fundraiso.ch: Web 3.0 Technologies Stiftung. https://www.fundraiso.ch/sponsor/web-3-0-technologies-stiftung, abgerufen am 18. Juli 2022.
[9] Web3 Foundation: Grants Program. https://web3.foundation/grants/, abgerufen am 18. Juli 2022.
[10] Web3 Foundation: Projects. https://web3.foundation/projects/, abgerufen am 18. Juli 2022
[11] Parity: About. https://www.parity.io/about/#about, abgerufen am 3. Juli 2022.
[12] Polkadot Network: About. https://polkadot.network/about/, abgerufen am 3. Juli 2022.
[13] Wikipedia Deutsch: Stiftung (Schweiz). https://de.wikipedia.org/wiki/Stiftung_(Schweiz)#Gr%C3%BCndung_und_Zweck_einer_Stiftung, abgerufen am 18. Juli2022
[14] BWL-Lexikon.de: Aktienarten. https://www.bwl-lexikon.de/wiki/aktienarten/, abgerufen am 9. Juli 2022.
[15] Gründerszene: Aktiengesellschaft. Lexikon. 1. Januar 2019. https://www.businessinsider.de/gruenderszene/lexikon/begriffe/aktiengesellschaft-ag/, abgerufen am 9. Juli 2022.
[16] DGRV - Deutscher Genossenschafts- und Raiffeisenverband e.V.: Was ist eine Genossenschaft? Die Genossenschaften. Ein Gewinn für alle. https://www.genossenschaften.de/was-ist-eine-genossenschaft, abgerufen am 10. Juli 2022.
[17] Polkadot: Governance. Learn. https://wiki.polkadot.network/docs/learn-governance, abgerufen am 26. Juni 2022.
[18] State of Wyoming: SF0038 - Decentralized autonomous organizations. 66th Legislature. Legislation 2021. https://www.wyoleg.gov/Legislation/2021/SF0038, abgerufen am 4. Juli 2022.
[19] Invesdor (2019): Geschichte der Wertpapiere: Vom Pfeffer bis zum digitalen Wertpapier in 2019. 22. November 2019. https://www.invesdor.de/magazin/geschichte-der-wertpapiere-vom-pfeffer-bis-zum-digitalen-wertpapier-in-2019/, abgerufen am 9. Juli 2022.
[20] Elisabeth Nechutnys: Kolonialismus im Widerhall der Geschichte. Postcolonial Potsdam. 5. Januar 2016.https://postcolonialpotsdam.wordpress.com/2016/01/05/kolonialismus-im-widerhall-der-geschichte/, abgerufen am 9. Juli 2022.
[21] ING (2022): Wo kommt die Aktie eigentlich her? Die Geschichte der Aktie. 28.03.2022. https://www.ing.de/wissen/die-geschichte-der-aktie/, abgerufen am 9. Juli 2022.
[22] Wikipedia Deutsch: Genossenschaft. https://de.wikipedia.org/wiki/Genossenschaft, abgerufen am 11.06.2022
[23] Asshauer, Michael (2022): Was ist das Metaverse? Einfach erklärt + Praxis-Beispiele. In: Machen! Magazin für Entscheider. Zuletzt aktualisiert 9. Juni 2022.https://machen.fm/marketing-sales/10516/was-ist-das-metaverse/, abgerufen am 17. Juli 2022.
[24] United States Securities and Exchange Commission (2017): Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO. Release o. 81207. 25. Juli 2017. https://www.sec.gov/litigation/investreport/34-81207.pdf, abgerufen am 16. Juli 2022.
[25] Seewald, Oswald: Allgemeine Staaatslehre. Skript. Uni.skript.passau. Universität Passau. Lehrstuhl für Staats- und Verwaltungsrecht, insbesondere Sozialrecht. 2007. https://www.jura.uni-passau.de/fileadmin/dokumente/fakultaeten/jura/lehrstuehle/dederer/skript_staatslehre_07_seewald.pdf, abgerufen am 15. Juli 2022.
[26] Subscan: Polkadot. Mainnet. https://polkadot.subscan.io/, abgerufen am 26. Juni 2022.
[27] PNS: Polkadot Name System. 2021. https://www.pns.link/, abgerufen am 31. Juli 2022.
[28] Polkadot.Domain: Take Ownership of Your Digital Identity and Assets. https://polkadomain.org/, abgerufen am 31. Juli 2022.
[29] Polkadot: Architecture. Learn. https://wiki.polkadot.network/docs/learn-architecture, abgerufen am 18. Juli 2022.
[30] Wood, Gavin: Polkadot (2016): Vision For a heterogeneous multi-chain Framework. Draft 1. Veröffentlicht in github, letzter Commit am 8. Dezember 2016, Historymarker 10/11/2016: 0.1.0. https://github.com/polkadot-io/polkadot-white-paper/blob/master/PolkaDotPaper.pdf, abgerufen am 25. Juni 2022.
[31] Polkadot.js: Parachains. Overview. Polkadot. https://polkadot.js.org/apps/#/parachains, abgerufen am 19. Juli 2022.
[32] Polkadot.js: Parachains. Overview. Kusama. https://polkadot.js.org/apps/?rpc=wss%3A%2F%2Fkusama-rpc.polkadot.io#/parachains, abgerufen am 19. Juli 2022.
[33] Cointelegraph: What are Parachains: A guide to Polkadot & Kusama Parachains. Guides Menu. https://cointelegraph.com/blockchain-for-beginners/what-are-parachains-a-guide-to-polkadot-and-kusama-parachains, Abgerufen am 19. Juli 2022.
[34] United States Securities and Exchange Commission (2019): Framework for “Investment Contract” Analysis of Digital Assets. In der letzten Version vom 3. April 2019. https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets, abgerufen am 17. Juli 2022.

[35] Hinman, William: Digital Asset Transactions: When Howey Met Gary (Plastic). Remarks at the Yahoo Finance All Markets Summit: Crypto. 14. Juni 2018. https://www.sec.gov/news/speech/speech-hinman-061418, abgerufen am 18. Juli 2022.
[36] gavofyork et al.: Referenda and Conviction Voting pallets #10195. In: GitHub. https://github.com/paritytech/substrate/pull/10195, abgerufen am 26. Juni 2022.
[37] Polkadot.js: Council. Overview. Polakdot. https://polkadot.js.org/apps/#/council, abgerufen am 26. Juni 2022.
[38] @polkadotnetwork. Auf: Twitter. https://twitter.com/polkadotnetwork, abgerufen am 19. Juli 2022.
[39] Youtube: Polkadot. Kanal. https://www.youtube.com/c/polkadotnetwork, abgerufen am 19. Juli 2022.

Self-Sovereign Identities for Smart Devices

Stephan Penner[1], Thomas Wieland[1], Marquart Franz[2]
[1]Hochschule Coburg, Friedrich-Streib-Straße 2, 96450 Coburg, Germany
[2]Siemens AG, Technology, Otto-Hahn-Ring 6, 81739 München, Germany

Abstract: *Current research in identity management is focusing on decentralized trust establishment for distributed identities. One of these decentralized trust models is Self-Sovereign Identities (SSI). With SSI each entity should be able to independently present and manage provable information about itself as well as request and review evidence from other entities. Using a distributed blockchain, information for verifying the authenticity of this evidence can be obtained from any other entity. This concept can be used not only for people, but also for authentication and authorization during the life cycle of devices in the Internet of Things (IoT). This paper presents an SSI-based concept for authentication and authorization of IoT devices among each other, intended to contribute to the change in trust on the internet. The SSI methodology employing a blockchain offers the possibility to establish mutual trust and proof of ownership without relying on any third party. The paper describes the concept, offers a reference implementation, and gives a discussion of the approach.*

1. Introduction

Communication and interaction over digital channels often require that the entities involved are able to authorize themselves mutually before exchanging information or committing transactions. Authenticity and the confirmation of certain abilities become more and more important, for human users as well as for IoT devices.

In the physical world certificates are one example to provide this confirmation for certain information, like an academic degree or the skill to maintain certain machines. In numerous countries, these certificates are also used for the authentication and authorization of an entity, like a driver's license. In this context, trust is established by trusting the author and signatures of the certificates and testing if the certificate is still valid. Then the checking entity can decide to trust this information or not. If the verifier trusts the issuer of the credential, the information stored in the certificate can also be trusted. This model is well known and has been used in various forms for decades in our connected world [1], [2].

In the digital world, a similar model is widely used to establish trust between entities and to check the authenticity of information. For this purpose, a third party is used as an anchor of trust, which stores and manages all relevant information and makes it available to others, for example in the form of digitally signed certificates. This anchor is intended to ensure the integrity and authenticity of this data to establish trust between the entities [2], [3], [4], [5], [6], [7].

What is already economically crucial in e-commerce or financial services systems, is even more important for cyber-physical systems like power plants or trains, where errors could endanger the safety of many people. Especially for the devices in the Internet of Things (IoT) [8] that are becoming more and more popular in these facilities a robust IoT system architecture is required. For this, it is necessary, among other things, that information and attributes of IoT devices can be securely managed, maintained, received and tracked across company boundaries throughout their lifetime [9], [10], [11], [12]. One approach to ensure such a system is to use a life cycle view on IoT devices [3], [4], [5], [11], [12], [13]. During this lifecycle, IoT devices interact with each other. For this interaction a system for authentication and authorization is required. Today most of such systems are using a central trust anchor, holding the data of system participants. Each entity that uses this trust anchor is forced to trust it in order not to leak, misuse or change any sensitive data. Protecting own data from such a misuse is hard because the data is stored in the data processing system with trust anchors [3], [4], [5], and [14].

For solving this trust issue, research and development currently focusses on concepts to eliminate centrally oriented trust anchors for the interaction between entities, including IoT devices. One promising approach utilizes blockchain architectures, leveraging the concept of self-sovereign identities (SSI for short) [3], [9], [15], [16]. With the help of SSI, entities can establish trust between each other on their own using digitally signed certificates, eliminating the need of a central trust anchor. Data can be stored and managed by the entities themselves.

Those previously mentioned certificates could also be used for unequivocal and verifiable proofs of attributes of IoT devices in their life cycle. While stored and managed by the devices, those certificates give a device the possibility to provide evidence for authentication and authorization without involving a third party. Any devices can be programmed in such a way that trust to an entity for particular actions during various scenarios in its lifetime is only given under certain conditions, depending on information in a digital certificate.

In this contribution we present a concept including a reference implementation and evaluation of a system that

can establish an authentication and authorization mechanism for the management and tracking of the life cycle of a cyber-physical system, consisting of several different IoT devices from different manufacturers, using SSI, without the need for a central storage of private data. Other issues of the security of IoT systems, which could theoretically be addressed by SSI, are not discussed here. This paper is structured as follows: First, background is provided about IoT, cyber-physical systems, project context, self-sovereign identities, and the blockchain systems Hyperledger Indy and Aries. Next, the proposed concept will be introduced including a view on related works by other authors. Afterwards an implementation of this concept, using Hyperledger Indy and Hyperledger Aries together with the Python web framework Flask, will be discussed and evaluated. At the end, the main aspects will be summarized, and possible future work will be presented.

2. Background

2.1 Trust Anchors

The Internet of Things, or IoT for short, is a network of devices with embedded microcontrollers collecting information about their physical environment using sensors [8]. Within this network, those devices can communicate with each other or with other systems. A typical property of an IoT device is its limitation of resources like computing capacity, RAM, bandwidth, or available energy.

This work has been conducted in the context of a project focusing on cyber-physical systems in trains [17], [18]. We define a cyber-physical system as an entity consisting of one or several IoT devices as computational units collecting information about its environment and forwarding this information via wired or wireless networks. An example for such a system is a train, consisting of multiple actuators, sensors, and subsystems realized with IoT devices.

Currently a central anchor of trust is often used for authentication and authorization in a cyber-physical system. Humans and devices rely on this anchor to authorize activities during the lifecycle of IoT devices - in manufacturing, in trains as well as in various other scenarios. It is very important in such cyber-physical systems to provide evidence that an information has not been altered.

Such a central instance must be trusted unconditionally. The trust anchor is necessary for the authentication and authorization of all actions in the system holding all necessary information about the connected devices. Technically, authentication is usually realized by asymmetric cryptography, offering public keys in X.509 certificates, signed by a trust authority [19], [13, p. 5]. In many use cases the trust anchor additionally provides signed information for the mutual interaction of the IoT devices, like the affiliation of the owner of a public key. This third party is also necessary for authentication and authorization between the entities. In complex environments like manufacturing sites or trains it is very hard to select the right entity that should hold the role of such a trust anchor. The IoT devices in this system have been manufactured by different vendors. Those are seeking not to reveal anything about their devices. Determining who should provide the trust anchor may easily result in long discussions and strict regulations. Even during operation, no one can be really sure that the trust anchor does not misuse its role.

2.2 Self-Sovereign Identity (SSI)

The goal of SSI is to eliminate the need for a trust anchor and give entities the opportunity to regain control over their data. In addition, entities should be able to decide on their own, if a piece of information should be trusted, whom to show selected information and whom to issue a certificate under certain conditions. In an SSI system the check for authenticity of information provided as a certificate is not carried out by a third party, but by the entities themselves, using information in a distributed, publicly available data storage [3], [5], [20], and [21]. Furthermore, no information associated with the entity should be made publicly available without the permission of the entity in question.

The identification of entities should also take place without a third party. When receiving information as well as when checking and presenting it to other entities, only two parties at most should be involved in these processes [2], [3], [14], and [22]. Attempts to realize SSI systems are using the W3C standards Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs) together with the Blockchain technology [2], [3], [14], and [22].

A DID is a pseudonymized and portable representative of an identity, not disclosing any information about the entity behind it. It is associated with a DID document which provides publicly available information. This information can be used to contact the entity behind the DID. Furthermore, it contains public keys owned by that identity for the establishment of a secure communication channel. This DID with the associated DID document can be securely made persistent on a distributed data storage like a blockchain [3], [20], [23], and [24].

Verifiable Credentials represent the digital counterpart to signed certificates from the physical world. A VC can be used to issue information about a device or a person. Using the issuer's signature, each entity can check by whom a Verifiable Credential was issued and whether its contents are authentic. For this purpose, Verifiable Credentials are signed by the issuer and a corresponding entry is written to a distributed data storage like a blockchain. On this storage the entry itself however contains no information about the contents of the VC or the receiver of it [3], [20], [24], and [25]. So there are three roles involved (according to [24]): the issuer issues the credential and hands it to the holder, often on his request. The holder keeps all his credentials in a wallet.

The verifier requests proof from the holder, e.g., about authenticity. The holder presents the proof using its signature which the verifier in turn may check. All these actions are based on DIDs that are stored in a public blockchain or another DID network.

2.3 Hyperledger Indy and Hyperledger Aries

A possible option for such a blockchain is a combination of the Hyperledger Indy and Aries [26], [27]. Both are open-source projects founded by the Linux Foundation to establish SSI systems providing the necessary infrastructure. Hyperledger Indy provides tools and libraries to establish the infrastructure for an SSI system. It provides a blockchain solution to store DIDs and information to verify VCs. It also provides an implementation of the W3C standards DID and VCs. It offers a digital identity wallet called Indy-wallet to store those credentials and DIDs [20], [26].

The provided data storage and infrastructure in Hyperledger Indy is a distributed and public permissioned blockchain. Each entity can read its contents, while writing to it is only allowed for entities with the roles trustee, steward, or endorser. In context of this paper, those roles will be summarized as the role “endorser” or “issuer”. The blockchain provided by Indy is not controlled by one entity but distributed across the so-called validator pool. Each member of this pool holds a copy of the blockchain. To write a new entry into the blockchain one member executes a write request from an endorser and broadcasts its result to the other members. After each member has received a certain number of identical answers, related to a write request, the system finds a consensus and this result will be written to each copy of the blockchain [26], [28], and [29].

Only publicly available information will be stored on a Hyperledger Indy blockchain. The blockchain consists of information like DIDs, DID documents and the used public key as well as algorithms etc. to verify an issued digital credential [26], [28], and [29].

Hyperledger Aries emphasis lies on how entities using a Hyperledger Indy SSI system can interact and communicate with each other in a peer-to-peer and secure way. To achieve this, it provides several protocols like *DID Communication*, *Issue Credential, Connection* and *Basic Message* [29], [27]. Other open-source projects, like Aries Cloud Agent Python (ACA-PY), are establishing some kind of framework, implementing the defined protocols in Hyperledger Aries. In particular, Aries Cloud Agent Python (ACA-PY) is recommended to be used by the Aries group [29].

ACA-PY provides a so-called *agent* as a webservice, offering a REST interface to enable the usage of the Aries protocols. The agent needs a *controller* for managing the agent, which must be implemented individually for each use case. The controller tells the agent what to do, for example, to issue a new VC, establish a new DID communication connection using the connection protocol, or to send messages with the basic message protocol. The agent also informs its controller via webhooks about events like receiving a new VC from an issuer.

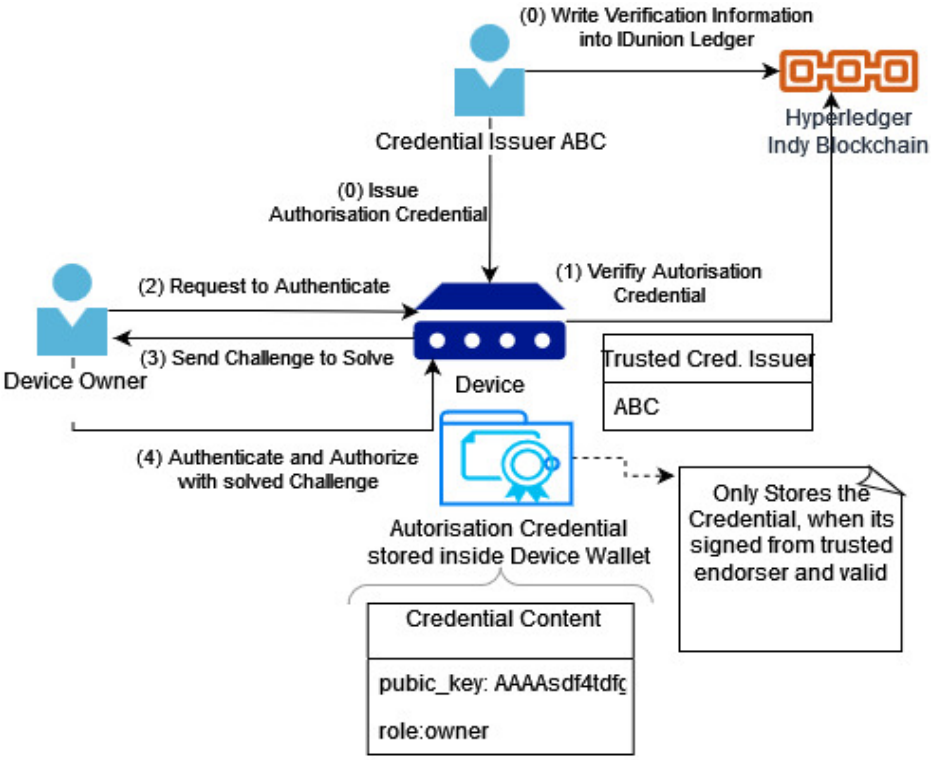

Fig. 1: Overview of the authentication and authorization concept Idea

One major protocol defined by Hyperledger Aries is *DID communication*. With it, two entities can encrypt their messages independent of the used transport protocol like HTTP or MQTT. To ensure this, both entities must exchange their DID and DID document, containing a public key. This can be done by using the connection protocol of Aries. To transmit encrypted messages or verifiable credentials the protocols *basic message* and *issue credential* can be used.

3. Conceptual Approach

We propose to make use of *DID Communication* and basic message to establish an authentication and authorization system using Verifiable Credentials and JSON Web Tokens (JWT). For the communication between entities, we defined message protocol called *Commands*. With this message protocol, entities may transfer tasks or solutions with *basic message* to each other, such as asking for authentication. Before that, a connection between the entities must be established using, for example, the *connection* protocol.

Using *Commands*, entities can transmit asymmetric encrypted requests and answers independent of any message transport protocol like HTTP or MQTT. This is realized by the Aries protocol *DID communication*. In this work, the *Commands* message protocol was used for the message exchange during the authentication and authorization process between two entities. This design was chosen to rely only on the security mechanism provided by *DID Communication*.

To authorize transmitted commands an authentication is needed first. After success, the IoT device can decide whether to execute the command or to decline it. For this, it will check the role of the authenticated entity. Information about which entity has which role is saved by means of a certificate in the IoT device. Therefore, a VC called Authorization Credential, or AuthS-VC for short, was defined. It contains the role and public key of an entity and is stored on an IoT device. Fig. 1 gives an overview of the described concept.

The device will accept this VC if it has originated from a credential issuer it trusts. If the device has an owner configured, it will ask this entity whether to accept or decline the VC instead.

The IoT device has a role-based access system that allows the requested execution of certain commands, like changing the owner, only to entities with certain roles. To authenticate and authorize an entity for such a command, a JWT holding the role of the entity is used combined with a challenge-response mechanism.

To authenticate, the requesting entity presents its public key to the device. The device is then able to check whether the presented key is known or unknown by retrieving VCs. If known, the device can find the corresponding VC with the provided public key, containing the role of the requesting entity. Then, the device uses its own secret key to create a JWT. After the JWT has been created, a challenge is constructed by encrypting the JWT using the public key of the requesting entity found in the VC. If the entity can decrypt this JWT with its secret private key, it has proven its authenticity. By attaching the JWT in future requests, the entity can authorize.

While the public key and role of this entity is saved as a VC, the device can check at any time on its own if this information was somehow altered. Fig. 2 shows the described flow.

Storing information about its owner on a IoT device provides full control over this data by the device itself. Misuse of this information by others is prevented. By holding this information as a Verifiable Credential, the device can even use this information in other domains, because

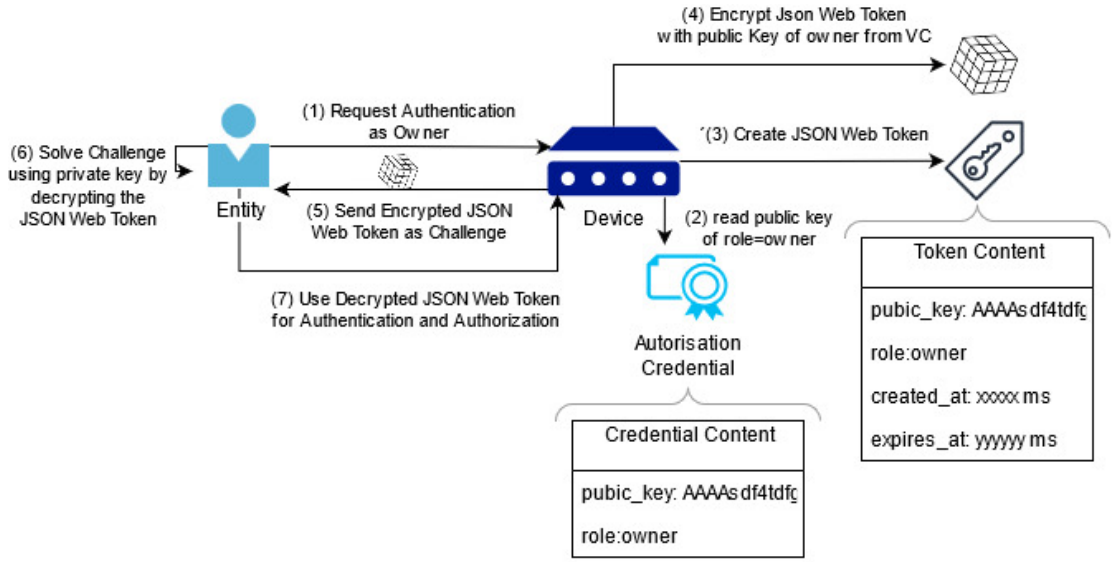

Fig 2: Proposed authentication and authorization system. Messages are delivered using the Aries *basic message* protocol.

there is no dependency to a trust anchor. Only a connection to the Hyperledger Indy blockchain, holding the corresponding verification information to this VC, is needed when the device wants to check its own VCs even in another domain.

New roles are easily defined. An entity with the role *maintainer* for example could be configured by issuing a corresponding VC to the device. By defining a public key to the role, the VC would identify an entity with the role maintainer. Corresponding access rights to certain commands for this role would be defined in the device itself. Because the VC is verifiable, this information can even stay valid if the device changes its domain or is transferred to a new owner. Therefore, the same authentication and authorization system is appliable over the entire lifecycle of an IoT device across company boundaries.

4. Related Work

4.1 RBAC-SC

Cruz et al. propose a distributed role based access control system called RBAC-SC using blockchain technology [16]. The goal is to use a role of an entity, like a student at University X, across company boundaries.

An instance that wants to assign roles to entities defines a smart contract on the Ethereum blockchain. For example, if a university wants to assign its students the role of X student, the smart contract is used and assigns this role to an address on the blockchain. This address is owned by an entity.

Later, this address will be used to check whether the entity has the role of X student. Before that, the smart contract is checked. Next, a challenge is used to evaluate whether the entity has access to the address in question to which the student role of university X has been assigned. To do this, the entity must sign information from the public address block with its private key. The associated public key is also stored on the Ethereum blockchain.

4.2 SSIBAC

The core idea of SSIBAC from Belchior et al. in [15] is to map Verifiable Credentials presented by entities to access rules. To use a resource, an entity first sends a request to the system. The system checks the defined rules for the requested access, in which the necessary attributes or roles are specified. On this basis, the requesting entity is checked by means of a challenge, by using verifiable credentials to generate a verifiable presentation (VP) that proves the required attributes or role of the requesting entity in a VC. If the entity responds with a VP, this is first validated and passed on to an access control engine, if the VP is valid. The engine then uses the information from the VP to calculate whether the access request is to be granted or denied. The authors used Hyperledger Indy for the necessary infrastructure of their system.

5. Reference Implementation

To implement the system proposed above, we used Hyperledger Indy as SSI infrastructure and Hyperledger Aries framework to implement our process. As mentioned before, we defined a message protocol called *Commands* to exchange commands like an authentication and authorization request. Also, we defined a Verifiable Credential called AuthS-VC. Its schema is written to a blockchain based on Hyperledger Indy. To exchange messages with *basic message,* structured using the *Commands* protocol, a controller was implemented with Python web framework Flask [30]. The controller receives notifications as webhooks from the agent. The agent informs the controller, when, for example, a new basic message has been received. The controller also contains an implementation of the *Commands* protocol to send and interpret messages using it. It also possesses the logic to get an AuthS-VC using a public key and to create and send a JWT challenge over the *Commands* protocol. To achieve this, the controller uses the ACA-PY agents REST interface to send basic messages.

The system consists of two major components: a web portal that sends a request with the *Commands* message protocol and a device that receives and processes such a request. To be able to authenticate, the device holds an AuthS-VC about the owner in its wallet. Fig. 3 shows the issued AuthS-VC with role owner in the wallet of the device. The *cred_def_id* field provides the information who has signed this VC and where to look at in the blockchain to verify the authenticity of this VC.


```
"referent": "51e3aad8-e227-4c5e-8040-ba7831226a78",
"attrs": {
  "endpoint": "http://localhost:9803",
  "public_key": "AAAAC3NzaC1lZDI1NTE5AAAAIFE9xj2JxMJDyzk0
  "role": "owner"
},
"schema_id": "PfUQbbAm8mSp2zvGoquabn:2:Autorisation:0.1",
"cred_def_id": "Y5q6MYZrDnZ6Q3BnoYZduk:3:CL:2294:0.157719
```


Fig. 3: Owner stored as VC in the wallet of the device

Using the basic message protocol, the web portal sends a *Commands* formed request to authenticate to the device with its public key. Fig. 4 shows the authentication request sent by the web portal to a device using basic message and *Commands.*

```
BEGIN;
AUTH:public_key-= AAAAC3NzaC1lZDI1NTE5AAAAI
FE9xj2JxMJDyzk0yW9rbMEmWyRvdNos6xjA/Y2XYBqy;
END
```

Fig. 4. Authentication request from the web portal, sent to the device. This request is transmitted using the Aries basic message protocol and formatted using the Commands protocol. This string is the content of the basic message to be sent using ACA-PY.

The device checks if the presented public key is saved as an AuthS-VC. If so, a JWT is created using the information public key and role inside the VC. Subsequently, the JWT

is encrypted using the public key and sent back to the web portal as challenge. This is shown in Fig. 5.

```
BEGIN;
RESP_AUTH:
     challenge-= <string with encrypted JWT>,
     role-= <role of the requester found in the VC>
END
```

Fig. 5: Response from the device, after it receives an AUTH request with a known public key.

With the JWT, the web portal can authenticate itself to the device, in this case as its owner. The JWT is also used as a proof of authorization for certain actions. In case the presented public key is not saved in an AuthS-VC, the device responds with an error message shown in Fig. 6.

```
BEGIN;
ERROR:msg-= Auth Rejected. Public key
AAAAC3NzaC1lZDI1NTE5AAAAIFE9xj2JxMJDyzk0yW9rbMEmWyRvd-
Nos6xjA/Y2XYBqy is unknown!;
END
```

Fig. 6: Error response when the provided public key is unknown.

6. Evaluation

For evaluation, we defined a function called *Change Owner* that changes the owner of a device. If an entity could authenticate as the owner, this function can be executed. To be able to transfer the ownership to a new entity, the device holds two AuthS-VCs. They represent the current owner and the new owner.

During the change owner process, the device will connect to the new owner and test if he is able to authenticate and authorize. After all steps have succeeded, the device deletes the VC corresponding to the current owner, leaving only the new owner's VC in the wallet. After that, the previous owner is not able to gain access anymore. All previous JWTs, which are still valid, become automatically useless, because the device always checks if the public key in the JWT corresponds to a public key stored as a VC.

To execute *Change Owner,* the owner has first to obtain a JWT. This is done by setting up a connection to the device using the connection protocol of Hyperledger Aries. After a connection has been established, a connection ID is returned. This can then be used to send an authentication request as basic message with the *Commands* protocol to the device.

For this, we implemented a function called *Ask for new Access Token* shown in Fig. 7 for the web portal.

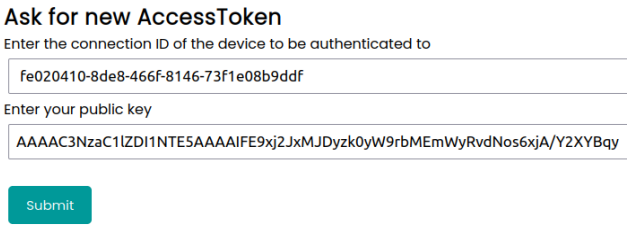

Fig. 7: Ask for new access token function on the web portal

By presenting the connection ID and the own public key, the request to a specific device can be constructed by the application. After clicking the submit button, the software prepares an authentication request to the device. The request received from the device is shown in Fig. 8.

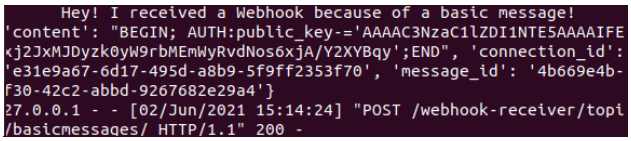

Fig. 2. The device controller receives an Auth request.

After the request, the device checks if the provided public key is known. If the key is stored in an AuthS-VC, it responds with an encrypted JWT. The web portal receives this challenge and tries to solve it by using its own private key. This is shown in Fig. 9.

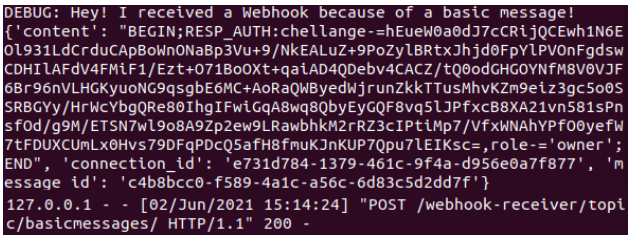

Fig. 9. Console output of the web portal controller, after receiving a challenge as a response to the previous AUTH request.

After the challenge has been mastered, the web portal obtains a new JWT and stores it. The user of the web portal will see this on his screen as shown in Fig. 10.

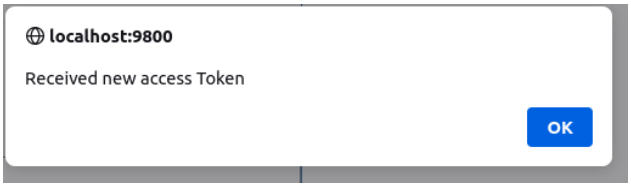

Fig. 10: Response of the web portal after successful authentication

Now, with the newly obtained JWT, the entity can authorize to let the device execute the process of changing its owner. For this, the user calls the "change owner" function and provides all necessary information for this process as shown in Fig. 11.

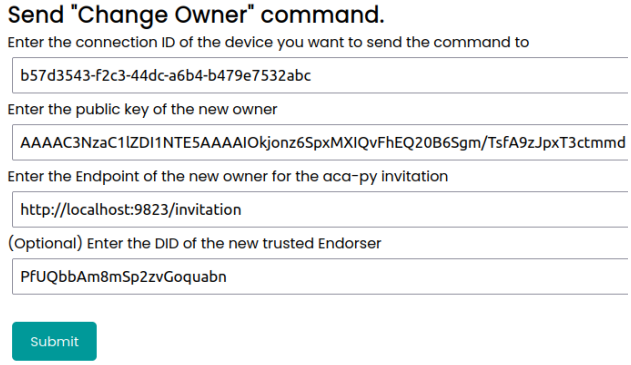

Fig. 11: Change Owner function on the web portal.

The controller of the web portal constructs a *Command* representation of this request by adding the obtained JWT for authentication and authorization.

If the owner could authenticate and authorize correctly, the device responds to the WebPortal with the message that the *Change Owner* process has been completed. After that, the entity sending the *Change Owner* command is not able to receive a new JWT or use its old JWT to authenticate and authorize. Attempting to do this will result in an error message, informing that the provided public key is unknown.

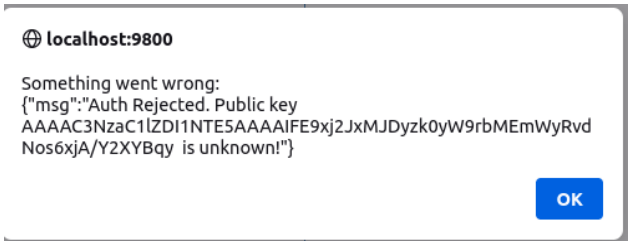

Fig. 12: Response, when old owner tries to authenticate itself to the device after Change Owner completed successfully

7. Conclusion

In this paper a possible solution has been introduced how to design and implement an authentication and authorization system, needed for the tracking and management of the lifecycle of IoT devices, using Verifiable Credentials and DIDs. A concept and an implementation of it could be provided and presented in a demonstration. The proposed system responds with an encrypted JWT as a challenge to an authentication request. The challenge will be constructed by only using public information from an entity stored as a VC on the device itself. The entity requesting an authentication can only solve the challenge when it possesses the right private key to the public key of an entity with a certain role.

Using a message format on top of Hyperledger Aries basic message protocol, the partners can communicate securely using asymmetric encryption for their messages. This is handled via DID communication. The only requirement is the ability to send and receive DID communication based basic messages. This can be achieved by using an ACA-PY agent.

Using Verifiable Credentials to store information, the proposed system becomes easily portable into other environments. In those, the VCs can be verified, when a connection to the corresponding Hyperledger Indy blockchain can be established. Those VCs can be used to configure any entity to a certain role even across company boundaries.

Future work is still necessary to analyze how to check if a trusted endorser or any credential issuer can be trusted to be allowed to issue certain credentials. For example, there should be research about how to verify that entity A is allowed to issue certificates of type X. One solution could be to ask for signed VCs proving this ability. Then of course the question pops up recursively, how to verify that the issuer of those VC is also allowed to do that. There should be research about this topic, concerning how to break this circle.

Acknowledgements

This work was supported by funding of German Federal Ministry for Digital and Transport (BMDV) and Federal Ministry for Economic Affairs and Climate Actions (BMWK) in the projects “RailChain” and “IDunion”.

References

[1] *IDunion - A Public Utility for Verification of Identity Data in Finance*. [Online Video]. Available: https://www.youtube.com/watch?v=CT0MrxRJXno

[2] Linux Foundation, “Introducing the Trust Over IP Foundation.” Accessed: Dec. 07, 2021. [Online]. Available: https://trustoverip.org/wp-content/uploads/2020/05/toip_introduction_050520.pdf

[3] G. Fedrecheski, J. M. Rabaey, L. C. P. Costa, P. C. Calcina Ccori, W. T. Pereira, and M. K. Zuffo, “Self-Sovereign Identity for IoT environments: A Perspective,” in *2020 Global Internet of Things Summit (GIoTS)*, Jun. 2020, pp. 1–6. doi: 10.1109/GIOTS49054.2020.9119664.

[4] B. Singhal, G. Dhameja, and P. S. Panda, *Beginning Blockchain: A Beginner’s guide to building Blockchain solutions*. Springer, 2018.

[5] Q. Stokkink and J. Pouwelse, “Deployment of a Blockchain-Based Self-Sovereign Identity,” *ArXiv180601926 Cs*, Jun. 2018, Accessed: Dec. 07, 2021. [Online]. Available: http://arxiv.org/abs/1806.01926

[6] N. Naik and P. Jenkins, “Self-Sovereign Identity Specifications: Govern Your Identity Through Your Digital Wallet using Blockchain Technology,” in *2020 8th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud)*, Aug. 2020, pp. 90–95. doi: 10.1109/MobileCloud48802.2020.00021.

[7] A. S. Wazan, R. Laborde, D. W. Chadwick, F. Barrere, and A. Benzekri, “How Can I Trust an X.509 Certificate? An Analysis of the Existing Trust Approaches,” in *2016 IEEE 41st Conference on Local Computer Networks (LCN)*, Dubai, Nov. 2016, pp. 531–534. doi: 10.1109/LCN.2016.85.

[8] F. Wortmann and K. Flüchter, “Internet of Things: Technology and Value Added,” *Bus. Inf. Syst. Eng.*, vol. 57, no. 3, pp. 221–224, Jun. 2015, doi: 10.1007/s12599-015-0383-3.

[9] S. Dramé-Maigné, M. Laurent, L. Castillo, and H. Ganem, “Augmented Chain of Ownership: Configuring IoT Devices with the Help of the Blockchain,” Singapore, Aug. 2018, vol. Part I, pp. 53–68. doi: 10.1007/978-3-030-01701-9_4.

[10] M. A. Khan and K. Salah, “IoT security: Review, blockchain solutions, and open challenges,” *Future Gener. Comput. Syst.*, vol. 82, pp. 395–411, May 2018, doi: 10.1016/j.future.2017.11.022.

[11] L. F. Rahman, T. Ozcelebi, and J. Lukkien, “Understanding IoT Systems: A Life Cycle Approach,” *Procedia Comput. Sci.*, vol. 130, pp. 1057–1062, 2018, doi: 10.1016/j.procs.2018.04.148.

[12] N. Yousefnezhad, A. Malhi, and K. Främling, “Security in product lifecycle of IoT devices: A survey,” *J. Netw. Comput. Appl.*, vol. 171, p. 102779, Dec. 2020, doi: 10.1016/j.jnca.2020.102779.

[13] S. Fatima, S. Ahmad, and S. Siddiqui, “X. 509 and PGP Public Key Infrastructure methods: A critical review,” *IJCSNS Int. J. Comput. Sci. Netw. Secur.*, vol. Vol. 15, no. 5, pp. 55–59, 2015.

[14] G. Goodell and T. Aste, “A Decentralised Digital Identity Architecture,” *Front. Blockchain*, vol. 2, p. 17, Nov. 2019, doi: 10.3389/fbloc.2019.00017.

[15] R. Belchior, B. Putz, G. Pernul, M. Correia, A. Vasconcelos, and S. Guerreiro, “SSIBAC: Self-Sovereign Identity Based Access Control,” in *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, Dec. 2020, pp. 1935–1943. doi: 10.1109/TrustCom50675.2020.00264.

[16] J. P. Cruz, Y. Kaji, and N. Yanai, “RBAC-SC: Role-Based Access Control Using Smart Contract,” *IEEE Access*, vol. 6, pp. 12240–12251, 2018, doi: 10.1109/ACCESS.2018.2812844.

[17] J. Lee, B. Bagheri, and H.-A. Kao, “A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems,” *SME Manuf. Lett.*, vol. 3, Dec. 2014, doi: 10.1016/j.mfglet.2014.12.001.

[18] L. Monostori *et al.*, “Cyber-physical systems in manufacturing,” *CIRP Ann.*, vol. 65, no. 2, pp. 621–641, 2016, doi: 10.1016/j.cirp.2016.06.005.

[19] ITU-T Recommendation, “X.509 Information Technology - Open Systems Interconnection - The Directory: Authentication Framework.” ITU, Jun. 1997. [Online]. Available: https://www.itu.int/rec/T-REC-X.509

[20] P. C. Bartolomeu, E. Vieira, S. M. Hosseini, and J. Ferreira, “Self-Sovereign Identity: Use-cases, Technologies, and Challenges for Industrial IoT,” in *2019 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, Sep. 2019, pp. 1173–1180. doi: 10.1109/ETFA.2019.8869262.

[21] Y. Liu, Q. Lu, H.-Y. Paik, X. Xu, S. Chen, and L. Zhu, “Design Pattern as a Service for Blockchain-Based Self-Sovereign Identity,” *IEEE Softw.*, vol. 37, no. 5, pp. 30–36, Sep. 2020, doi: 10.1109/MS.2020.2992783.

[22] M. S. Ferdous, F. Chowdhury, and M. O. Alassafi, “In Search of Self-Sovereign Identity Leveraging Blockchain Technology,” *IEEE Access*, vol. 7, pp. 103059–103079, 2019, doi: 10.1109/ACCESS.2019.2931173.

[23] Sporny, Manu, Longley, Dave, Sabadello, Markus, Reed, Drummond, Steele, Orie, and Allen, Christopher, “Decentralized Identifiers (DIDs) v1.0 - Core architecture, data model, and representations,” W3C Proposed Recommendation, Aug. 2021. [Online]. Available: https://www.w3.org/TR/did-core/

[24] A. Preukschat and D. Reed, Self-sovereign identity: decentralized digital identity and verifiable credentials. Shelter Island: Manning, 2021.

[25] M. Sporny, D. Longley, and D. Chadwick, “Verifiable Credentials Data Model v1.1 - Expressing verifiable information on the Web,” Nov. 2021. [Online]. Available: https://www.w3.org/TR/vc-data-model/

[26] Hyperledger Revision, “Hyperledger Indy SDK.” [Online]. Available: https://hyperledger-indy.readthedocs.io/projects/sdk/en/latest/docs/

[27] “Hyperledger Aries.” [Online]. Available: https://github.com/hyperledger/aries

[28] “Hyperledger Indy Node.” [Online]. Available: https://github.com/hyperledger/indy-node

[29] “Hyperledger Aries Cloudagent Python.” [Online]. Available: https://github.com/hyperledger/aries-cloudagent-pythonrabak

[30] “Flask documentation.” [Online]. Available: https://flask.palletsprojects.com/en/2.0.x/

Blockchain für die Supply Chain des grünen Wasserstoffmarktes – Eine innovative Lösung?

Volker Wannack
Blockchain Competence Center Mittweida (BCCM)/Hochschule Mittweida,
Technikumplatz 17, 09648 Mittweida

Bisher gibt es keine einwandfreie manipulationssichere Nachweisführung für klimafreundlichen „grünen" Wasserstoff und der damit möglichen Nachverfolgung der Herkunft vom Erzeuger erneuerbarer Energien bis zum Endverbraucher, sodass die gesamte Supply Chain des „grünen" Wasserstoffs nicht im Sinne einer ökonomischen, ökologischen und sozialen Nachhaltigkeit dargestellt und in einem sicheren und transparenten Markt abgebildet werden kann. Mit einer geeigneten Blockchain kann dieses Problem gelöst werden, die darüber hinaus weitere noch nie dagewesene Mehrwerte für die Supply Chain des „grünen" Wasserstoffmarktes und für den nachhaltigen Strukturwandel insgesamt bietet und deren Entwicklung demnächst im Rahmen des Förderaufrufs „Technologieoffensive Wasserstoff" innerhalb der Forschungsförderung des Bundesministeriums für Wirtschaft und Klimaschutz im 7. Energieforschungsprogramm der Bundesregierung startet.

1. Einleitung

Durch die regionalen, nationalen und internationalen Wasserstoff (H_2)- und Blockchain-Strategien [1,2,3,4,5] wird dem Wasserstoff und der Blockchain-Technologie auf Landes-, Bundes-, europäischer und weltweiter Ebene zum Durchbruch verholfen und somit die politische und gesellschaftliche Grundlage für das bespiellose Projektvorhaben "Blockchain Basierter Wasserstoffmarkt (BBH_2)" gelegt, das im Rahmen des Förderaufrufs „Technologieoffensive Wasserstoff" innerhalb der Forschungsförderung des Bundesministeriums für Wirtschaft und Klimaschutz im 7. Energieforschungsprogramm der Bundesregierung gefördert wird. Die Projektidee ist die Entwicklung eines funktionierenden Blockchain-Minimum Viable Product (B-MVP), also einer geeigneten Blockchain als Basistechnologie mit einer gemeinsamen Datenbank & Plattform (sowie die dazugehörige Implementierung von automatisch abwickelnden Smart Contracts), für die gesamte Supply Chain des („grünen") Wasserstoffmarktes. Der Betrieb dieser Blockchain stellt eine paradigmenwechselnde, innovative Lösung für einen klimafreundlichen und nachhaltigen Strukturwandel dar, weil er noch nie dagewesene Alleinstellungsmerkmale, Vorteile und Mehrwerte im Rahmen einer ökonomischen, ökologischen und sozialen Nachhaltigkeit bietet, die in Kapitel 3 dargestellt werden.

2. Stand der Wissenschaft und Technik

Durch die Blockchain-Technologie können Daten in Unternehmen und Behörden dezentral, schnell, (fälschungs)sicher, transparent, nachverfolgbar, automatisiert und deutlich kostensparender weitergegeben werden. [6] Aufgrund dieser Vorteile wurden bereits im Bereich Medizin, Logistik, Finanzwesen, Immobilien, Identitätsmanagement, Verwaltung und Energie verschiedene Anwendungsfälle dieser Technologie identifiziert [7, 8, 9, 10, 11] und bereits teilweise umgesetzt. [9, 10, 12, 13] Im Bereich der Energiewirtschaft gibt es beispielsweise verschiedene Regionalstrommodelle, welche auf der Blockchain-Technologie basieren. Blockchain-Handelsplätze für lokal erzeugten Ökostrom werden zum Beispiel von den Stadtwerken Wuppertal mit Tal.Markt [14], im Landkreis Biberach mit BiberEnergie [15] und von enviaM in Kooperation mit Elblox [16] angeboten. Darüber hinaus wird von der Bundesregierung die Entwicklung & Implementierung Blockchain-basierter Herkunftsnachweisprozesse für (Öko)Strom und (Bio)Gas empfohlen [11], die in den nächsten Jahren im Kontext des Schaufensterprogramms „Sichere digitale Identitäten" [13] umgesetzt werden. Denn für Strom- und Gasabnehmer ist heute die tatsächliche Herkunft der Energie nur schwer nachvollziehbar. Ein Nachweis erfolgt lediglich über unscharfe Zertifikate im Nachhinein. Zudem ist für (Öko)Strom und (Bio)Gas in Deutschland jeweils eine zentrale Stelle geschaffen worden (das Umweltbundesamt für Ökostrom [17] und die Deutsche Energie-Agentur GmbH für Biogas [18]), die aufwendig in den teilweise manuellen Prozess eingebunden ist. Der mögliche Einsatz der Blockchain-Technologie für Nachweise über Ausgabe, Handel, Verfolgung und Einzug von Strom oder Gas erlaubt dann erstmals eine Ende-zu-Ende-Zertifizierung und damit einen „anlagenscharfen" Nachweis. Nachdem eine Anlage registriert ist, wird mit einem Verbraucher ein Energiebezug vereinbart. Nach Eintragen des Handelsabschlusses auf einer Blockchain werden die erzeugten und verbrauchten Mengen von den verantwortlichen Messstellenbetreibern in einen Smart Contract übertragen. Auf diese Weise werden für die erzeugten Einheiten auf der registrierten Anlage Herkunfts-Tokens erzeugt und anschließend dem Verbraucher übermittelt. Die Vorteile, die eine Blockchain für diesen beispielhaften Prozess für Herkunftsnachweise hat, bietet sie natürlich auch für Wasserstoff, um z.B. den automatischen einwandfreien manipulationssicheren Nachweis von „grünem" anstatt z.B. von „grauem"

Wasserstoff (ohne ein hier bereits existierendes, suboptimales Nachweisregister zu berücksichtigen) zu erbringen. Darüber hinaus bietet sie weitere noch nie dagewesene Mehrwerte für die Supply Chain des („grünen“) Wasserstoffmarktes und für den damit verbundenen nachhaltigen Strukturwandel insgesamt (wie im nächsten Kapitel dargestellt), sodass ihre Entwicklung durch das Projekt BBH_2 notwendig ist.

3. Nutzen von BBH_2

Der wesentliche Nutzen von BBH_2 ist der folgende: Erstens verbessert das in Abbildung 1 dargestellte B-MVP erstmalig die Logistik-, Handels- und Transaktionsprozesse innerhalb der gesamten Wasserstoffmarkt-Akteursprozesskette (Erzeuger erneuerbarer Energien, die Überschussenergie nutzenden Wasserstoffproduzenten, Wasserstofftransport- und Verteilnetzbetreiber und die Wasserstoffverbraucher) dergestalt, dass diese nun gemeinsamen geschützten Zugriff gewähren, kosteneffizienter sind und transparent & nachvollziehbar, flexibel standardisiert & automatisiert abgewickelt, revisions- & fälschungssicher gespeichert, geteilt und ausgewertet werden können. Der Schwerpunkt der Blockchain liegt somit in der einwandfreien manipulationssicheren Nachweisführung des klimafreundlichen “grünen” anstatt des z.B. klimaschädlichen “grauen” Wasserstoffs und der damit möglichen Nachverfolgung der Herkunft vom Erzeuger erneuerbarer Energien bis zum Endverbraucher, sodass die gesamte Supply Chain des „grünen“ Wasserstoffs im Sinne der ökonomischen, ökologischen und sozialen Nachhaltigkeit dargestellt und in einem sicheren und transparenten Markt abgebildet wird. Zweitens könnte das B-MVP länderübergreifend gültig sein und bedarf demnach keiner länderspezifischen Datenhaltung. Drittens schafft das B-MVP über eine damit einhergehende mögliche Gründung einer Blockchain-Betreibergesellschaft langfristig Arbeitsplätze und dient der Fachkräftegewinnung sowie Qualifizierung und Ausbildung. Viertens lässt das B-MVP neue tragfähige Geschäftsmodelle entstehen, die Grundlage für weitere Unternehmensansiedlungen bzw. Neugründungen sind und wiederum mit einer zusätzlichen langfristigen Schaffung von Arbeitsplätzen einhergeht. So können z.B. Produzenten und Transportnetzbetreiber durch Datenauswertung individuelle Tarife entwickeln sowie bedarfsgerechte Netzkapazitäten bereitstellen. Weiterverteiler und Endkunden würden von bedarfsgerechten Tarifen und fälschungssicheren Nachweisen profitieren. Fünftens trägt das B-MVP zu einer Steigerung der Wertschöpfung durch technologischen und wirtschaftlich nutzbaren Vorsprung bei und zu einer damit verbundenen besseren, nationalen und internationalen Standards-setzende Sichtbarkeit im Sinne einer klimafreundlichen, nachhaltigen, zukunftsfähigen und -weisenden Vorzeigeregion, die sich als Vorreiter mit überregionaler Strahlkraft manifestieren wird. Sechstens schaffen die

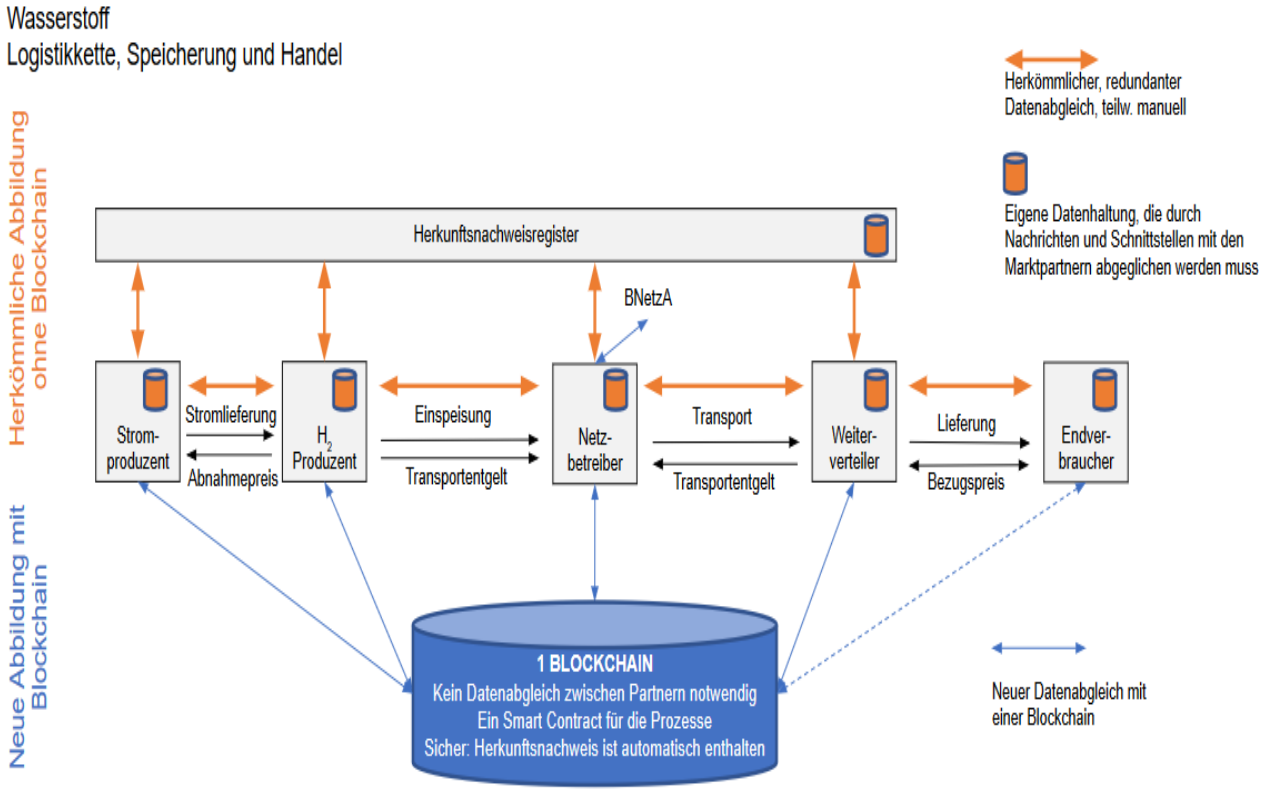

Abbildung 1: Design & Vorteile des Blockchain-Minimum Viable Product (B-MVP) für den Wasserstoffmarkt (Eigene Darstellung)

vorherigen genannten Punkte zusätzliche Anreize für Forschung und Entwicklung und tragen zur Verbesserung & Bündelung des Wissenstransfers von Hochschulen und Unternehmen, zur Steigerung der wissenschaftlichen Leistungsfähigkeit und somit zu einer Entsprechung des Verständnisses von strategischem Innovationsmanagement und Innovationskultur bei, weil damit in übergeordneter Weise zwei zukunftsweisende Technologien im innovativen Mantel der Sektorkopplung gebündelt werden.

4. Umsetzungsmethode

Die geplante Methode der Umsetzung ist die folgende:

a) Evaluierung & Abbildung einer geeigneten Blockchaintechnologie und -architektur: Hierzu gehört die Anforderungsaufnahme, das evaluierende Anforderungsmanagement, die Entwicklung von Erhebungs- und Erarbeitungsmethoden, die Evaluierung des deutschen & europäischen Marktes hinsichtlich der Regulierung, das Festlegen der prozessualen Abbildungsmöglichkeiten des deutschen und des europäischen Marktes für den B-MVP, die Evaluierung der Konformität mit der Datenschutzgrundverordnung, die Erstellung eines Datenschutzkonzeptes, das Herstellen von Marktkonformität/Marktstandards/Akzeptanzforschung, die Konzeptionierung zur Erfassung und Auswertung der gesammelten Daten, die Erstellung eines UX/UI-Konzeptes, die Erstellung der Systemarchitektur unter Einbezug der Bestandssysteme, die Analyse von Verbundsystemen, deren Datenhaltung sowie Prozessintegration, die Bestimmung der technischen Parameter für die Blockchain und der notwendigen Infrastruktur, sowie die Erstellung eines Hosting- und Sicherheitskonzeptes.

b) Entwicklung & Implementierung der Blockchain, der Smart Contracts und der Hinterlegung von Herkunftsnachweisen: Hierzu gehört die Aufnahme konkreter Prozesse für die Abbildung von Smart Contracts, die Konkretisierung und Auswahl der umzusetzenden Smart Contracts, deren fachliche, inhaltliche, prozessuale Ausgestaltung und konkrete technische Beschreibung, die Definition der Auslösepunkte für Aktionen im Kontext des physikalischen Lieferprozesses, die juristische Prüfung und Legitimation, die Entwicklung von Smart Contracts, die Prüfung von KI-Anwendungen zur automatisierten Entscheidungsfindung, die Anforderungsaufnahme zur fachlichen Ausgestaltung der Herkunftsnachweise, deren Konzeptionierung zur technischen Umsetzung und die Definition der Auslösepunkte für die Weitergabe von diesen, die Verknüpfung mit externen Handelspunkten (Börsen/OTC-Märkte), die Entwicklung von digitalen Herkunftsnachweisen, die Analyse, das Festlegen und das Aufsetzen einer geeigneten Blockchain, der Aufbau einer realen Demoumgebung, die Anbindung der erfassten Systeme und der analysierten und standardisierten Daten, die Implementierung der Smart Contracts auf die Blockchain, die Umsetzung der Herkunftsnachweise innerhalb des B-MVP, die Frondend- und Backendentwicklung, die Umsetzung sicherer Identifizierung mittels selbstsouveräner Identitäten, die Verknüpfung der Smart Contracts mit dem Smart Contract-Register und der Security Check des B-MVP.

c) Entwicklung geeigneter Schnittstellen zu bestehenden Systemen der Nutzer: Hierzu gehört die Anforderungsaufnahme zur Schnittstellenanalyse im Wasserstoffprozess, die Definition von benötigten Datenschnittstellen, die Schnittstellenarchitektur zu Nominierungs-, Portfoliomanagement-, Trading- und Abrechnungssystemen und die Schnittstellenentwicklung in Abhängigkeit der B-MVP-Entwicklung.

d) Entwicklung geeigneter Datenformate für den Austausch der prozessrelevanten Daten: Hierzu gehört die Anforderungsaufnahme für prozessrelevante Daten und Datenformate, deren Beschreibung und Harmonisierung, die Abbildung technischer relevanter Prozesse, die Gegenüberstellung mit dem zu beschreibenden Workflow und die technische Beschreibung der Automatisierungsschritte als Vorbereitung für die B-MVP-Entwicklung.

e) Durchführung von Feldstudien zur Verprobung des B-MVP und Prüfung der Skalierung des B-MVP auf anderen Märkten und Nutzergruppen: Hierzu gehört: die Auswahl geeigneter Testuser, die Erstellung des Testdurchführungskonzeptes, die Formulierung und Erstellung der Testfälle, die Verprobung des B-MVP im Markt, ein Review der Testergebnisse innerhalb der Feldstudie, eine iterative Teststellung, die Evaluation der Ergebnisse, die Vorbereitung zu Markteinführung, die Anpassungen und Dokumentationen und die Kommunikation der Ergebnisse mit Politik, Wirtschaft und der Bevölkerung.

5. Fazit

Das Projekt Blockchain Basierter Wasserstoffmarkt (BBH_2) schafft eine paradigmenwechselnde, innovative Lösung für einen klimafreundlichen und nachhaltigen Strukturwandel, weil sie noch nie dagewesene in Kapitel 3 beschriebene Alleinstellungsmerkmale, Vorteile und Mehrwerte im Rahmen einer ökonomischen, ökologischen und sozialen Nachhaltigkeit bietet. Deren aktive Umsetzung, die im Rahmen des Förderaufrufs „Technologieoffensive Wasserstoff" innerhalb der Forschungsförderung des Bundesministeriums für Wirtschaft und Klimaschutz im 7. Energieforschungsprogramm der Bundesregierung gefördert wird, ist nicht nur im besonderen Interesse der zahlreichen sich am Projekt engagierenden beteiligten Partner aus der Wirtschaft, sondern wird auch durch politische Partner unterstützt, sodass BBH_2 überregionale Aufmerksamkeit und eine exponierte nationale und internationale Stellung erhält und sich somit im Sinne einer zukunftsfähigen und -weisenden Frontrunner-Lösung mit überregionaler Strahlkraft manifestieren wird.

Literaturverzeichnis

[1] EC (2021): Europaen Blockchain Strategy, unter: https://digital-strategy.ec.europa.eu/en/library/european-blockchain-strategy-brochure (abgerufen am 05.08.2022)

[2] BMWi (2020): Die nationale Wasserstoffstrategie, unter: https://www.bmwi.de/Redaktion/DE/Publikationen/Energie/die-nationale-wasserstoffstrategie.pdf?__blob=publicationFile&v=16 (abgerufen am 05.08.2022)

[3] BMWi (2019): Blockchain-Strategie der Bundesregierung, unter: https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/blockchain-strategie.pdf?__blob=publicationFile&v=8 (abgerufen am 05.08.2022)

[4] SMWA (2020): Innovationsstrategie des Freistaates Sachsen, unter: https://publikationen.sachsen.de/bdb/artikel/35302 (abgerufen am 05.08.2022)

[5] SMWA (2019): Sachsen Digital - Digitalisierungsstrategie des Freistaates Sachsen, unter: https://publikationen.sachsen.de/bdb/artikel/33501 (abgerufen am 05.08.2022)

[6] Joos (2019): 5 Vorteile und 5 Nachteile der Blockchain-Technologie, unter: https://www.blockchain-insider.de/5-vorteile-und-5-nachteile-der-blockchain-technologie-a-881712/ (abgerufen am 27.05.2022)

[7] VDI (2018): Blockchain- Eine Technologie mit disruptivem_Charakter, unter: https://gi.de/fileadmin/GI/Hauptseite/Aktuelles/Meldungen/2018/Blockchain_-_Eine_Technologie_mit_disruptivem_Charakter.pdf (abgerufen am 05.08.2022)

[8] Talin (2021): 28 Blockchain Use Cases – Mögliche Anwendungen der Distributed Ledger Technology (DLT), unter: https://morethandigital.info/blockchain-moeglichkeiten-und-anwendungen-der-technologie/ (abgerufen am 05.08.2022)

[9] BCCM (2022): Forschung & Entwicklung, unter: https://blockchain.hs-mittweida.de/forschung-entwicklung/ (abgerufen am 05.08.2022)

[10] BSRM (2022): Aktuelle WIR!-Projekte, unter: https://blockchain-mittweida.com/projekte/ (abgerufen am 05.08.2022)

[11] dena (2019): dena-MULTI-STAKEHOLDER-STUDIE: Blockchain in der integrierten Energiewende, unter: https://www.dena.de/fileadmin/user_upload/dena-Studie_Blockchain_Integrierte_Energiewende_DE4.pdf (abgerufen am 05.08.2022)

[12] HSMW (2022): Verteilte Informationssysteme, unter: https://www.cb.hs-mittweida.de/webs/verteilte-informationssysteme.html (abgerufen am 05.08.2022)

[13] ID-Ideal (2022): ID-Ideal-sicheres Management Digitaler Identitäten, unter https://id-ideal.hs-mittweida.de/ (abgerufen am 05.08.2022)

[14] WSW (2022): WSW TAL.MARKT - Die Energierevolution, unter: https://www.wsw.info/ausgabe-172/energie/wsw-talmarkt/ (abgerufen am 05.08.2022)

[15] Biber Energie (2022): BiberEnergie - Strom für Dich und mich – regional und bürgernah, unter: https://www.biberenergie.de/ (abgerufen am 05.08.2022)

[16] enviaM (2019) https://www.enviam-gruppe.de/presse/presse-mitteilungen/2019/enviam-und-elblox-er%C3%B6ffnen-online-marktplatz-f%C3%BCr-regionale-erzeuger-und-verbraucher-von-strom-aus-erneuerbaren-energien-in-ostdeutschland (abgerufen am 05.08.2022)

[17] UBA (2022): Herkunftsnachweisregister (HKNR), unter: https://www.umweltbundesamt.de/themen/klima-energie/erneuerbare-energien/herkunftsnachweisregister-hknr (abgerufen am 05.08.2022)

[18] dena (2022): Biogasregister, unter: https://www.biogasregister.de/startseite/ (abgerufen am 05.08.2022)

ISSN 1437-7624