HOCHSCHULE MITTWEIDA
University of Applied Sciences

Wissenschaftliche Berichte | Scientific reports

Konferenzband zum Scientific Track der Blockchain Autumn School 2021

Nr. 4, 2021

Konferenzband zum Scientific Track der Blockchain Autumn School 2021
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
Dipl.-Volkswirt Mario Oettler

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.

Titelseite: Foto: 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. 001, 2021
Modelle und Qualifizierungskonzepte zur ressourceneffizienten Teilefertigung - MoQuaRT
Nr. 002, 2021
Ökologische Transformation in Technik, Wirtschaft und Gesellschaft? Tagungsband zur 26. Interdisziplinären Wissenschaftlichen Konferenz Mittweida
Nr. 003, 2021
12. Mittweidaer Lasertagung

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

Review on Blockchain based e-Voting Systems

Nomana Ayesha Majeed
Hochschule Mittweida, Technikumplatz 17, 09648 Mittweida

With the advancement in cryptography and emerging internet technology, electronic voting is gaining popularity since it ensures ballot secrecy, voter security, and integrity. Many commercial startups and e-Voting systems have been proposed, but due to lack of trust, privacy, transparency, and hacking issues, many solutions have been suspended. Blockchain, along with cryptographic primitives, has emerged as a promising solution due to its transparent, immutable, and decentralized nature. In this paper, we summarized the properties that existing solutions should satisfy and explained some cryptographic primitives like ZKP, Ring signatures along with their security limitations. We gave a comprehensive review of some block-chain-based e-Voting systems and discussed their strengths and weaknesses based on the given properties with table of comparison.

1. Introduction

Elections are the cornerstone of leadership selection in any democratic country. For many years, paper-based voting systems have been used for important decisions. This method has many risks related to privacy disclosure, insecurity, and biased voting.

Since 1980, many e-Voting systems have attracted the researchers around the world [22] like in Estonia [40], USA, Australia, and Switzerland to solve the problems faced by traditional voting systems. E-Voting aims to improve security, efficiency, cost-efficiency. Meanwhile, many challenges have been identified in such systems such as corrupt administration, trust in central party, lack of efficient software, secrecy of ballots [41].

Trust is the most complex problem in e-Voting, and blockchain [23] has emerged as a solution to many of the aforementioned problems. In 2009, Nakamoto [21] introduced the blockchain which was preliminary used for cryptocurrencies [31] but now it has become a core component in various other areas of identification, authorization including the smart contracts [30], particularly in e-Voting to solve the issue of trust in the central party. Blockchain is mainly deployed in three forms: smart contract-based e-Voting [3], cryptocurrency-based e-Voting, and as a ballot box [7]. So far, many researched based and commercial-scale voting systems have been deployed, such as Agora [2], Voatz [42], FMV [7].

The rest of the paper is organized as follows: In Section II, we describe the properties that serve as criteria for recently proposed blockchain-based e-voting solutions. In Section III, we discuss ZKP, ring signatures, blind signatures and some other traditional cryptographic algorithms, and their limitations. In section IV, we present a comprehensive review of some blockchain-based e-Voting systems and discuss their strengths and weaknesses based on the given properties. Finally, we illustrate a table ii comparing e-Voting protocol and highlight the areas where improvements can be made.

2. Properties of a robust e-Voting system

We considered thirteen security properties collected from various experimented blockchain-based electronic voting systems. The definitions vary from paper to paper according to their requirements, we provide a refined description of the properties that can serve as an evaluation-criteria for existing protocols.

P1. Privacy: the relationship between the vote and voter should not be revealed and vote must be kept secret.

P2. Anonymity: the protocol should protect the voter´s anonymity while casting the vote.

P3. Robustness: protocol should be capable of tolerating a certain amount of technical failure and participant misbehavior.

P4. Eligibility verification: only registered and authorized voters can participate.

P5. Individual verifiability (E2E): a voter can verify that his vote was casted-as-intended, recorded-as-casted and counted-as-recorded.

P6. Universal verifiability: anyone can download the tallied result, and check the completeness of elections.

P7. Scalability: the e-Voting system should be capable of supporting large-scale elections.

P8. Fairness: protocol should not be capable of providing any partial results before the tallying phase.

P9. Receipt-freeness [19]***:*** the voting system should not generate any receipt to prove whom the voter has voted for. Consequently, a voter cannot provide any proof to third party, this stops vote-buying and selling.

P10. Untraceability [24]***:*** the voter and third party should not be able to trace the vote back to him even after decryption of results.

P11. Coercion resistance *(vote-freely)* [20]***:*** it is the strongest notion of privacy where no voter can prove that he followed the coercer´s instructions. It ensures receipt-freeness but it requires an anonymous channel.

P12. Un-reusability: one vote per eligible voter, it prevents replay attack.

P13. Vote-and-go: a voter can go after casting his ballot.

Furthermore, individual verifiability and receipt-freeness are related. To achieve both properties together, it is required to generate proof that is sufficient for a voter to get verification but insufficient for a coercer to know how the voter has voted. Additionally, verifiability requires linkability and anonymity requires unlinkability of the voter. The voter should know that his vote is included in the tally but he cannot provide a prove for his vote since the vote is not unique [29]. Besides these properties, we have also evaluated the blockchain based e-Voting systems according to the platform, decentralization, voting choice, vote encryption, and cryptographic primitive being used.

Abbreviation	Explanation
ZKP	Zero Knowledge Proof
QAP	Quadratic Arithmetic Program
Zk-SNARKs	Zero knowledge Succinct Non-Interactive Argument of Knowledge
CRS	Common Reference String
DSS	Digital Signature Standard
ECC	Elliptic Curve Cryptography
LRS	Linkable Ring Signature
MAST	Merkelized Abstract Syntax Trees
MPC	Multi Party Computation

Table i: list of Abbreviations

3. Blockchain & Cryptography

3.1. Fundamentals of Blockchain

Blockchain [23] is a decentralized append-only ledger formed by chaining the blocks together. Each connected node has a backup of the entire database, so if someone tries to alter the transaction, it will be immediately detected by all other nodes. Blockchain has become a robust solution for both traditional and e-Voting system due to its characteristics namely: transparency, immutability and decentralization.
Although the blockchain has solved many challenges related to security, such as avoiding the manipulation of votes, fast and transparent voting results without third-party involvement, it is also important to highlight that existing blockchain based solutions have scalability issues, as each transaction need to be verified by the entire network, which reduces speed and increases cost. Moreover, due to the complexity of the computational steps, blockchain requires powerful systems to manage traffic in large elections. Secondly, blockchain is transparent by nature which we don't need in e-Voting systems. Instead, we need privacy and anonymity, and to this end, several traditional cryptographic techniques have been applied to ensure privacy. We have studied most commonly used cryptographic primitives in e-Voting systems and highlighted the limitations. These includes zero knowledge proofs, zk-SNARKs, ring signatures, blind signatures, homomorphic encryption, mix-networks, secret sharing scheme and elliptic curve cryptography [27] [34] [37].

3.2. Zero knowledge proof

ZKP is a cryptographic method invented by [25] in which a prover can prove to the verifier that he knows a certain statement without revealing any information about the statement except the truth. ZKP must satisfy the three properties, namely: completeness, reliability, and zero knowledge. In an e-Voting system, Non-Interactive ZKP is widely used [14], and is obtained by applying the Fiat-Shamir heuristic to prove the validity of a ciphertext, i.e., the voter convinces the third party that his ballot is valid by proving a ZKP without revealing any information about the voter's choice.

The most commonly used ZKPs in electronic voting systems are Schnorr ZKP and zk-SNARKs [32]. zk-SNARKs are very complex proofs and require strong computational power in proofs generation since the arguments are used to prove an NP statement about a QAP without revealing anything about the witness. The main limitation in zk-SNARKs is the generation of CRS which requires the participation of multiple parties, if the parties are compromised then the entire voting system is destroyed. Secondly, ZKP rely on the hardness of the DLOG problem, which is challenging in long run, since as Shor [38] proved that the DLOG can be computed efficiently by quantum computers [12] [16].

3.3. Elliptic curve cryptography

Several digital signatures based on finite fields have been used in e-voting systems for authentication purpose. The recent focus of DSS is on elliptic curve like Schnorr DSS [39]. ECC [34] is an approach to asymmetric cryptography constructed on the algebraic structure of elliptic curves to provide high data security with smaller bit size than RSA. ECC uses elliptic curve point addition and multiplication to generate the keys that acts like a trapdoor. Thus, the difficulty lies in the infeasibility to compute the EC-DLOG problem. Despite the security of EC, side-channel attacks [33] and twist-security attacks make EC unsecure for e-Voting systems as they can overturn the security that ECC aims to provide. Side-channel attacks are more common in the practical implementation of a cryptosystem which often results in leakage of data, thus compromising confidentiality and anonymity.

3.4. Blind Signatures

Blind signature [36] allows a user to select a message, encrypt it and asks and the signer to signs the encrypted message. Hence, it is not the user that is blind but the signer due to the blindness factor involved in encryption! Such signatures are used when the user's privacy is particularly important. Therefore, these signatures are applied extensively in the e-Voting systems that allow an authority to verify the voter's identity. After receiving confirmation, the voter unblinds his encrypted vote and submits it to the tallying authority using an anonymous channel. Thus, ensures eligibility verification.

Although, such signatures are very simple, efficient, but due to the unlinkability of unblinded signature to the voter, it is difficult to find whether the voter cast multiple votes. Furthermore, such systems do not achieve receipt-freeness, since the voter can use the blind factors to link with his ballot to prove later how he voted. On the other hand, the coercer can dictate the voter to use the particular factor to blind his ballot that violates coercion resistance. Lastly, both the voter and the tallying authority must trust the signer. If the signing authority is compromised or refuses to sign, the voting system can stop working [6] [5] [14].

3.5. Ring Signatures

Ring signatures were introduced by [27] in a paper titled "how to leak a secret". It is an anonymized variant of the digital signature and does not require a trusted third party. Ring signatures are constructed in such a way that the ring can only be completed and correctly verified if the signer knows a secret for one of the given public keys in the ring. In e-Voting, the most frequently used ring signatures are linkable ring signatures, [26] where the identity of the signer remains anonymous but with an additional tag that provides linkability feature in case of double submission. The voter generates an LRS to cast his vote which provides anonymity to the vote while linkability helps to detect duplicate voting [9] [15]. Thus, three main advantages of LRS are anonymity, efficiency, and linkability. Many recent developments in e-Voting have used ring signatures [Monero] however, the size of the signature, cost, and time grow linearly with the number of users in many proposed e-Voting systems [11] since the ring contains all public keys that increases automatically with the number of voters, so it should be split into subgroups by using the "image of secret key".

3.6. Secret Sharing Scheme (SSS)

SSS [37] is a method that securely distributes the shares of a secret among a group of participants. Most e-Voting systems used Shamir secret sharing scheme (SSSS); a threshold scheme that uses polynomial interpolation. SSSS first encodes the "secret" into a "polynomial" then divides it into pieces and distributes it. To reconstruct the secret, we need atleast $t\,(threshold)+1$ participants. SSSS is typically used in e-Voting protocols to achieve robustness against corrupted authorities. [5] utilized SSSS to distribute the keys however, the scheme must trust a single dealer for the distribution of the shares. Though, some attacks are possible when shares are revealed asynchronously as long as there is an internal adversary or group of internal adversaries [28].

3.7. Mix-Networks

Mix-nets [35] are mainly used to ensure user anonymity. It consists of a set of mix servers that take encrypted data (votes) as input, re-encrypt it, mix it and pass the output to the next server. The process continues until the last server is reached. In this method, the input (identity of voter) and the final output (vote) remain completely unlinked, providing anonymity to the user. In practice, re-encryption mix-net is commonly used in e-Voting systems compared to decryption mix-net. ZKP is required to verify the honesty of each server which increases the computational complexity. Although, mix-net provide receipt freeness but such systems are less efficient due to the involvement of multiple intermediate steps and exposed to DDoS attacks since all mixers are required during the tally.

3.8. Homomorphic encryption (HE)

Homomorphic Encryption allows to operate on encrypted data without decrypting any information. In practice, additive homomorphic ElGamal encryption [2] [12] and multiplicative homomorphic Paillier encryption [6][8] are mostly used. In e-Voting schemes, the calculation is performed on the ciphertext, so each voter must generate a ZKP to provide the validity of the encrypted ballot. This provides universal verifiability, robustness, and privacy at the same time. However, a threshold of trustworthy tallying authorities is required to decrypt the election result. Such protocols do not require any anonymous channel, but complex strategies and slow computation time makes it inapplicable for large-scale elections. Also, both ElGamal and Paillier cryptosystems are subject to quantum attack.

4. Review of Blockchain based e-Voting systems

4.1. How to vote privately using Bitcoin [1]

Zhao and Chain (2015) proposed an e-Voting system based on Bitcoin using a threshold signature scheme and ZKP. The ballots do not need to be encrypted or decrypted instead random numbers are used to hide the ballot, which are distributed via ZKP. Each voter can fund exactly one of the two candidates, the candidate who is funded more wins the elections. Voting is done via two methods: Claim-or-Refund and Joint transaction. In Claim-or-Refund, if a voter does not reveal his masked vote, all 2n COR instances will expired and the protocol is terminated. In joint transaction, all transactions remain secret and any voter can terminate the entire process without losing any money before the joint transaction appears on the blockchain, it shows that the whole process is in hand of one voter and if the voter is compromised he can destroy the entire voting process. Moreover, the complexity of the protocol mainly lies in the use of *n-n* threshold signature scheme. To create such a signature securely, one needs to add a verification part for their messages to prove good behaviour, which adds new complexity. Likewise, the ZKP setup requires MPC and "yes/no" voting can limit the adoption of this voting system.

4.2. Agora

In 2015, [2] presented a commercial end-to-end verifiable setup called AGORA, which is composed of four layers: a bulletin board, Catena, bitcoin blockchain, and

Votapp. Agora uses ElGamal cryptosystem for vote casting and cast-or-challenge validation to carry out cast-as-intended validations. Neff shuffling technique along with a ZKP is used to obtain a new list of anonymized ballots. Agora's voting system provides the ability to audit election results at any stage of the voting process and allow anyone to observe an election. A final attestation is signed with the auditors' private key once the election is verified. However, it relies on third parties for supervision, who can conspire with the candidate to alter the votes. Furthermore, the platform is not very precise, offering different alternatives for each stage and does not offer coercion resistance, nor it is a robust voting system.

4.3. A smart contract for boardroom voting with maximum voter privacy [3]

McCorry et al. (2017) proposed the first implementation of a decentralized and self-tallying protocol using Ethereum blockchain, and introduced an additional round of commitment to obtain the fairness property. The protocol does not depend on any central party for the privacy of voters, it can only be exposed through a full collusion attack. However, the unsupervised protocol does not provide coercion resistance therefore, it is only suitable for low coercion elections. Furthermore, the efficiency of system is low since it can scale to a maximum of 40 voters due to the gas limit per block and the identities of voters are publically known. Two major scaling issues are: direct storage of all eligible voters on the smart contract, and the utilization of ECC through an external library made it expensive and too large to store on the blockchain.

4.4. Decentralized Voting: A Self-tallying Voting System Using a Smart Contract on the Ethereum Blockchain [4]

Yang et al. (2018) presented a decentralized, ranked-choice, and self-tallying system using a smart contract on Ethereum blockchain. The proposed system ensures voter confidentiality by using ElGamel homomorphic encryption. The content of the vote is encrypted but signature and identification are in plaintext so anyone can verify the identity and helps to avoid double voting. However, it does not offer receipt freeness and ElGamal encryption requires two exponentiations. It also assumes that every registered voter submits their valid vote, if this would not be the case, any voter can destroy the tallying phase without submitting his vote. And, the current protocol does not solve the scaling issue.

4.5. SHARVOT: secret SHARe-based VOTing on the blockchain [5]

Bartolucci et al. (2018) proposed a blockchain based e-voting system called SHARVOT that uses Shamir's secret sharing scheme and bitcoin blockchain, enables on-chain submission of votes and determination of the winning candidate. To improve privacy, the protocol relies on CircleShuffle technology to unlink the voters from their submitted ballots. The protocol has introduced the voting fee to avoid the Sybil attack. However, all stages of the proposed protocol depend on a single dealer; if this dealer is compromised, the entire voting system can be destroyed. Furthermore, the protocol uses a P2SH address during the vote commitment transaction, which leads to a natural limitation on the size of the script allowed to generate P2SH output address. A reduction of the script size might be done with MAST.

4.6. Platform-independent secure blockchain-based voting system [6]

Yu et al. (2018) proposed a platform-independent verifiable and secure voting system deployed on the BFT-blockchain platform using Hyperledger Fabric. The authors have used Paillier encryption, proof of knowledge, and short linkable ring signatures to ensure security, privacy, and scalability. The trustworthiness of blockchain is achieved by using the 4 validation nodes. However, the generation and uploading of encryption of zeros required for receipt freeness consumed most time. Voter registration is done by the smart contract using an email/ ID/ URL along with the desired password which is a very weak method. Therefore, the protocol is not coercion resistant since any coercer can vote instead of the voter by simply hacking their secret key. It is also claimed that the protocol does not depend on the central party, yet the administrator is responsible for generating the keys used to encrypt and decrypt the ballot. This means that the protocol must trust the central party. If the administrator collaborates with one of the candidates, he can make changes to the results before the results are published.

4.7. Follow My Vote (FMV) [7]

FMV proposed a commercial voting platform that uses the BitShares blockchain as a ballot box and ECC to maintain anonymity. A trusted authority verifies the identity of each voter, authorizes only eligible voters to cast their ballots, and provides them with pass-phrases needed in case of changing their vote. It utilizes two key pairs per voter; for identity verification, and to cast a vote that allows individual verification. However, FMV allows the voter to print a receipt of their transaction and ultimately to audit the casted ballots. It does not offer any mechanism that allows observers to verify the accuracy of the final result. Moreover, a trusted party is needed to ensure voter privacy and hide the link between the voter's identity and voting key, and this party has the ability to change votes since it has all voter's pass-phrases. Finally, votes are cast without being encrypted.

4.8. Verify-your-vote: A verifiable blockchain based online voting protocol [8]

Chaieb et al. (2018) proposed an e-voting system called Verify-Your-Vote (VYV) on the Ethereum blockchain using

elliptic curve cryptography, pairings, and identity-based encryption, but the protocol design does not support coercion- resistance. The security of VYV is proven through the use of verification tool "Proverif". The structure of the ballot allows the voter to save the counter value of the corresponding candidate and use it for verification. Though, the system does not resist coercer attack, and the choice of tallying authorities responsible for decryption of votes and counting is not defined. Also, side-channel attacks can undermine the security that ECC is supposed to provide.

In 2020, [18] designed and implemented a verifiable blockchain-based e-voting system (VYV) and evaluates its security properties and performance. The result shows that the time is linear with the number of voters when there is a single server, and it decreases when the number of servers increases. The same pattern holds for the counting phase, so the worst case is when one tallying authority has to count all votes.

4.9. Ring signature based voting on blockchain [9]

Kugusheva and Yanovich (2019) proposed a private blockchain-based voting system that uses LRS to transfer the secret data without compromising voting reliability and voter privacy. The scheme achieves trust and stabilization using the Exonum framework, which is systematically decentralized. However, it is neither user-friendly nor cost-effective. Moreover, it does not achieve receipt freeness and coercion resistance.

4.10. DABSTERS: Distributed Authorities using blind signature To Effect Roust Security in e-Voting [10]

Chaieb et al. (2019) solved some of the weaknesses of VYV namely the centralized registration method and the problem related to Ethereum where any dishonest miner can modify the transaction before it is stored on the blockchain. The proposed decentralized e-Voting system is based on a private blockchain called DABSTERS and uses a blinded signature algorithm to preserve the privacy of the voter. However, the voter has to go to the office physically to register for authentication. Moreover, no coercion resistance is achieved due to the counter values created by the election authorities, and the scalability and performance of protocol are not checked.

4.11. Chaintegrity: blockchain-enabled large-scale e-voting system with robustness and universal verifiability [11]

Zhang et al. (2019) proposed a blockchain-enabled e-voting system called Chaintegrity that satisfies nine properties ranging from scalability, verifiability, robustness, and cost-effectiveness. The authors also proposed a hybrid data structure that combines Bloom filter and Merkle hash tree for fast authentication. Blind signature and Pailler homomorphic encryption are used for large-scale elections to ensure privacy and authenticity. However, the system is proposed for low coercion resistance and three rounds of interaction between the voter and the protocol are required. The selection of election holders to register a voter depends on cryptographic sorting, but it is difficult to generate a random number in a distributed blockchain. Therefore, this feature is not very useful practically. The protocol does not achieve receipt freeness and untraceability, since the voter can use the blind factor in his ballot to prove later how he voted. Finally, the voter has to create two accounts during the registration and casting phase, and also smart contract consumes time in search for a particular transaction, results in a low authentication process.

4.12. Provotum: A blockchain based and end-to-end verifiable Remote Electronic Voting System [12]

Killer et al. (2020) proposed a practical design for a fully decentralized remote electronic voting called Provotum and used public permissioned blockchain as a public bulletin board where only authorized parties can sign the block but anyone can verify it. Therefore, the trust is distributed across different nodes of the blockchain. Provotum is powered by the smart contract, distributed key generation, homomorphic encryption, and cooperative decryption. However, the protocol does not provide coercive security or receipt freeness and support only single voting type. The protocol considers many participants and primitives which leads to an increase in cost and time. Long term privacy cannot be guaranteed as it is based on the security of ElGamal cryptosystem, that is breakable by using the quantum computers in the future. Scalability is not achieved due to the choice of the underlying blockchain and insecure communication channel.

4.13. Scalable Open Vote Network on Ethereum [13]

Seifelnasr et al. (2020) presented an extended version of the work by McCorry et al. and solved scalability problem and universal verifiability by through verifiable off-chain computations using the Merkle tree. The protocol relies on an untrusted administrator to tally the vote off-chain and to publish a Merkle tree of encrypted votes. Its correctness can be publically verified during the dispute phase even if there is only one honest voter, but the amount of gas required in the dispute phase increases linearly with the number of voters, since two Merkle proofs must be performed in addition to two elliptic curve operations. On the other hand, the transaction cost of voter registration includes a Merkle proof of membership, which increases the gas cost. Finally, the total gas needed to run the elections is very low compared to McCorry, but according to the current price, it is still too expensive to be used in large-scale elections.

4.14. Efficient, Coercion-free and Universally Verifiable Blockchain-based Voting [14]

Dimitriou (2020) proposed an electronic voting system based on the Bitcoin blockchain infrastructure. The use

of a token randomizer that acts as a black box during the creation of a ballot ensures receipt-freeness and coercion resistance but, it violates the actual definition of coercion resistance since it does not consider the case when coercer is physically present. Universal verifiability is achieved through the append-only structure of the blockchain. Finally, the proposed system combines the features of blockchain with cryptographic primitives: zk-SNARKs and Pederson commitment to establish the sure elections. It is claimed that the voting system places minimal trust in the election authorities. However, it is assumed that the election authorities who handed the token randomizer to the user are not malicious which involves trust in the election authority. Secondly, the construction of zk-SNARKs again requires a trusted party to generate the CRS. If the election authority responsible for creating CRS is malicious, it can create a CRS that breaks the property of ZK and thus learns the information about the voter's secret parameters. Furthermore, tallying time has linear complexity, and finding shows that proof generation takes under 3 min.

4.15. AMVChain: authority management mechanism on blockchain-based voting systems [15]

Li et al. (2021) presented an e-voting system based on an authority management mechanism. This is a 3-layer access control architecture, where a smart contract is used at each layer for validation and granting permissions. The developed system is based on the hyperledger fabric (consortium blockchain). LRS is used to ensure privacy and encrypt the ballot to disconnect the ballots and voters. The proposed system is suitable for enclosed environment like universities since most of the part relay on the smart contract. There is no method specified for the identity check and registration, and any eligible voter can cast a vote instead of candidate as they have an access to candidate's private key. By using LRS, signing time increases according to the size of ring and tallying time increases with the number of candidates, which increases the risk of result tempering.

4.16. Æternum: A Decentralized Voting System with Unconditional Privacy [16]

Killer et al. (2021) proposed a remote electronic voting system that provides unconditional privacy. Æternum does not need to rely a central party instead unconditional privacy is achieved by using the public permissioned distributed ledger. However, it only allows single voting type and does not prevent a replay attack. Fairness is not achieved by default as the ballots are not encrypted. The method is secure with respect to current and future quantum attacks but if the voting client is compromised, the attacker can link any ballot generated with the client to the owner's device.

4.17. A Manipulation Prevention Model for Blockchain-Based E-Voting System [17]

Tas et al. (2021) proposed a double-layer encryption model to avoid the manipulation of voting results, and utilized a decentralized version that ensures privacy and stores the recorded votes in a distributed manner. However, due to the encryption and distribution, the time to distribute the data increases with the number of nodes. Also, the risk of tampering increases if the lower value is chosen for the threshold. Replay attack, Sybil attack, man-in-the-middle attack, and buying attack is possible. Finally, based on the token used in the transaction, an attacker can coerce the voter to vote for a particular candidate and can verify his vote later.

	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	Platform	Cryptographic primitive	Decentralization	Voting type	Authentication	Tallying protocol
[1]	✓	–	×	–	✓	✓	×	✓	–	–	✓	✓	✓	Bitcoin	ZKP, Threshold signature scheme	No admin	Single	Plain	Blockchain
[2]	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	×	×	✓	Bitcoin	ElGamal cryptosystem	Multi admin	–	–	Any third party
[3]	✓	✓	×	×	✓	✓	×	✓	–	–	×	–	×	Ethereum	Schnorr ZKP, 1-out-of-2 ZKP	No admin	Single	Smart contract administrator	Self-tallying
[4]	✓	×	×	✓	✓	✓	×	✓	×	–	–	✓	×	Ethereum	ElGamal HE, ZKP, distributed encryption	Election admin	Multiple	–	Self-tallying
[5]	✓	✓	×	✓	✓	×	×	✓	–	✓	×	✓	✓	Bitcoin	Secret Sharing, CircleShuffle	Single admin	Multiple	Single dealer	–
[6]	Claimed	✓	×	–	✓	✓	✓	×	✓	✓	Claimed	×	✓	Hyperledger Fabric	PoK, SLRS, Pailler encryption	Single admin	Multiple	SLRS	Administrator
[7]	✓	✓	×	✓	✓	×	✓	×	×	–	×	–	✓	BitShares	ECC	Registrar	Multiple	Trusted dealer	Authority
[8]	✓	✓	–	✓	✓	✓	×	✓	✓	✓	×	✓	✓	Ethereum	ECC, pairings, identity-based encryption, Pailler encryption	Single admin	Multiple	Administrator	Authorities
[9]	✓	✓	✓	×	–	–	×	–	×	–	×	✓	✓	Exonum	LRS	Organizer	Multiple	KYC	–
[10]	✓	✓	✓	✓	✓	✓	×	✓	–	×	×	✓	✓	PBFT blockchain	IBE, Blind signatures	Authorities	Multiple	Digital signature	Authority
[11]	✓	✓	✓	✓	✓	✓	linear	✓	×	×	low	–	×	Platform independent	Blind signature, homomorphic encryption,	Partially	Multiple	Hybrid data structure	Smart contract, election holders
[12]	✓	–	–	✓	✓	✓	×	✓	–	×	×	✓	✓	Public permissioned	ZKP, ElGamal HE, DKG	Authorities	Single	Identity provider	Authorities
[13]	✓	✓	–	✓	✓	×	Claimed	✓	–	–	–	✓	×	Private Ethereum	Schnorr ZKP, OVN, ECC	Untrusted admin	Multiple	Not mentioned	Untrusted admin
[14]	✓	✓	×	✓	✓	✓	×	✓	✓	✓	Claimed	✓	×	Bitcoin	Zk-SNARKs, Pederson Commitment	Registrar	Multiple	Self-authentication	any interested party
[15]	✓	✓	✓	✓	✓	×	×	✓	–	✓	×	✓	✓	Consortium blockchain	LRS	No admin	Multiple	Smart contract	Smart contract
[16]	Claimed	✓	×	✓	–	✓	–	×	–	✓	✓	×	✓	Private permissioned	NIZKP	Voting authority	Single	Voting authority	Anyone
[17]	✓	✓	×	✓	✓	✓	×	✓	×	–	–	✓	✓	Private Ethereum	HE, Secret sharing scheme	Authority	Multiple	Registrar	Network nodes

Table ii: comparison between blockchain based e-Voting schemes

5. Conclusion

e-Voting systems started in 2000, and public blockchains get popularity from 2009-2016. Since 2017, private blockchains have been used more in practice as they are more reliable. Consortium blockchain frameworks like Hyperledger Fabric and Exonum offer more transparency and audibility. By the end of 2019, almost all solutions now rely on permissioned (private) blockchains. We have seen that cryptographic primitives have their limitations concerning privacy and not all blockchain based protocols have succeeded to deliver that level of satisfaction to the voter, which they promised or at least claimed, so the current technologies are not problem-free, there are many unsolved directions like risk of large-scale fraud, strong attack on privacy, and scalability issues, decentralization, quantum attacks that are yet to be addressed. There are some second layer technologies that have been proposed recently such as Sharding, rollups, etc. that could help in one direction and advanced cryptographic primitives on the other.

Reference:

[1] Zhao, Z., & Chan, T. H. H. (2015, December). How to vote privately using bitcoin. In *International Conference on Information and Communications Security* (pp. 82-96). Springer, Cham.

[2] *Agora: Bringing voting systems into the digital age*. Agora. (n.d.). https://www.agora.vote/. Accessed 11 June 2021.

[3] McCorry, P., Shahandashti, S. F., & Hao, F. (2017, April). A smart contract for boardroom voting with maximum voter privacy. In *International Conference on Financial Cryptography and Data Security* (pp. 357-375). Springer, Cham.

[4] Yang, X., Yi, X., Nepal, S., & Han, F. (2018, November). Decentralized voting: a self-tallying voting system using a smart contract on the ethereum blockchain. In *International Conference on Web Information Systems Engineering* (pp. 18-35). Springer, Cham.

[5] Bartolucci, S., Bernat, P., & Joseph, D. (2018, May). SHARVOT: secret SHARe-based VOTing on the blockchain. In *Proceedings of the 1st international workshop on emerging trends in software engineering for blockchain* (pp. 30-34).

[6] Yu, B., Liu, J. K., Sakzad, A., Nepal, S., Steinfeld, R., Rimba, P., & Au, M. H. (2018, September). Platform-independent secure blockchain-based voting system. In *International Conference on Information Security* (pp. 369-386). Springer, Cham.

[7] Long, _ W., & Hourt, _ N. (2021, May 11). *Secure Decentralized Application Development*. Follow My Vote. https://followmyvote.com/.

[8] Chaieb, M., Yousfi, S., Lafourcade, P., & Robbana, R. (2018, October). Verify-your-vote: A verifiable blockchain-based online voting protocol. In *European, Mediterranean, and Middle Eastern Conference on Information Systems* (pp. 16-30). Springer, Cham.

[9] Kugusheva, A., & Yanovich, Y. (2019, December). Ring Signature-Based Voting on Blockchain. In *Proceedings of the 2019 2nd International Conference on Blockchain Technology and Applications* (pp. 70-75).

[10] Chaieb, M., Koscina, M., Yousfi, S., Lafourcade, P., & Robbana, R. (2019, July). DABSTERS: Distributed Authorities using Blind Signature To Effect Robust Security in e-voting. In *International Conference on Security and Cryptography (SECRYPT)*.

[11] Zhang, S., Wang, L., & Xiong, H. (2020). Chaintegrity: blockchain-enabled large-scale e-voting system with robustness and universal verifiability. *International Journal of Information Security*, *19*(3), 323-341.

[12] Killer, C., Rodrigues, B., Scheid, E. J., Franco, M., Eck, M., Zaugg, N., ... & Stiller, B. (2020, November). Provotum: A Blockchain-based and End-to-end Verifiable Remote Electronic Voting System. In *2020 IEEE 45th Conference on Local Computer Networks (LCN)* (pp. 172-183). IEEE.

[13] Seifelnasr, M., Galal, H. S., & Youssef, A. M. (2020, February). Scalable open-vote network on ethereum. In *International Conference on Financial Cryptography and Data Security* (pp. 436-450). Springer, Cham.

[14] Dimitriou, T. (2020). Efficient, coercion-free and universally verifiable blockchain-based voting. *Computer Networks*, *174*, 107234.

[15] Li, C., Xiao, J., Dai, X., & Jin, H. (2021). AMVchain: authority management mechanism on blockchain-based voting systems. *Peer-to-peer Networking and Applications*, 1-12.

[16] Killer, C., Knecht, M., Müller, C., Rodrigues, B., Scheid, E., Franco, M., & Stiller, B. Æternum: A Decentralized Voting System with Unconditional Privacy.

[17] Taş, R., & Tanrıöver, Ö. Ö. (2021). A Manipulation Prevention Model for Blockchain-Based E-Voting Systems. *Security and Communication Networks*, *2021*.

[18 Chaieb, M., Yousfi, S., Lafourcade, P., & Robbana, R. (2021). Design and practical implementation of verify□your□vote protocol. *Concurrency and Computation: Practice and Experience*, *33*(1), e5813.

[19] Delaune, S., Kremer, S., & Ryan, M. D. (2005, September). Receipt-freeness: Formal definition and fault attacks. In *Proceedings of the Workshop Frontiers in Electronic Elections (FEE 2005), Milan, Italy*.

[20] Haines, T., & Smyth, B. SoK: Surveying definitions of coercion resistance.

[21] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*, 21260.

[22] Esteve, J. B., Goldsmith, B., & Turner, J. (2012). International experience with e-voting. *Norwegian E-Vote Project. International Foundation for Electoral Systems. Document disponibil online la adresa http://www. ifes. org/Content/Publications/News-in-Brief/2012/June/% 7E/media/B7FB434187E943C18F4D4992A4EF75DA. pdf*.

[23] Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017, June). An overview of blockchain technology: Architecture, consensus, and future trends. In *2017 IEEE international congress on big data (BigData congress)* (pp. 557-564). IEEE.

[24] Radwin, M. J., & Klein, P. (1995, December). An untraceable, universally verifiable voting scheme. In *Seminar in Cryptology* (pp. 829-834).

[25] Goldwasser, S., Micali, S., & Rackoff, C. (1989). The knowledge complexity of interactive proof systems. *SIAM Journal on computing*, *18*(1), 186-208.

[26] Liu, J. K., & Wong, D. S. (2005, May). Linkable ring signatures: Security models and new schemes. In *International Conference on Computational Science and Its Applications* (pp. 614-623). Springer, Berlin, Heidelberg.

[27] Rivest, R. L., Shamir, A., & Tauman, Y. (2001, December). How to leak a secret. In *International Conference on the Theory and Application of Cryptology and Information Security* (pp. 552-565). Springer, Berlin, Heidelberg.

[28] Tieng, D. G., & Nocon, E. (2016, March). Some Attacks on Shamir's Secret Sharing Scheme by Inside Adversaries. In *Conference Proceedings-The DLSU Research Congress* (pp. 7-9).

[29] Langer, L., Jonker, H., & Pieters, W. (2010, December). Anonymity and verifiability in voting: understanding (un) linkability. In *International Conference on Information and Communications Security* (pp. 296-310). Springer, Berlin, Heidelberg.

[30] Singh, A., Parizi, R. M., Zhang, Q., Choo, K. K. R., & Dehghantanha, A. (2020). Blockchain smart contracts formalization: Approaches and challenges to address vulnerabilities. *Computers & Security*, *88*, 101654.

[31] Klarin, A. (2020). The decade-long cryptocurrencies and the blockchain rollercoaster: Mapping the intellectual structure and charting future directions. *Research in International Business and Finance*, *51*, 101067.

[32] Ben-Sasson, E., Chiesa, A., Tromer, E., & Virza, M. (2014). Succinct non-interactive zero knowledge for a von Neumann architecture. In *23rd {USENIX} Security Symposium ({USENIX} Security 14)* (pp. 781-796).

[33] Danger, J. L., Guilley, S., Hoogvorst, P., Murdica, C., & Naccache, D. (2013). A synthesis of side-channel attacks on elliptic curve cryptography in smartcards. *Journal of Cryptographic Engineering*, *3*(4), 241-265.

[34] Paar, C., & Pelzl, J. (2009). *Understanding cryptography: a textbook for students and practitioners*. Springer Science & Business Media.

[35] De Keyser, T. (2017). Implementation of a verifiable mix network based on the trade-off between resilience, scalability, and performance.

[36] Chaum, D. (1983). Blind signatures for untraceable payments. In *Advances in cryptology* (pp. 199-203). Springer, Boston, MA.

[37] Beimel, A. (2011, May). Secret-sharing schemes: A survey. In *International conference on coding and cryptology* (pp. 11-46). Springer, Berlin, Heidelberg.

[38] Mavroeidis, V., Vishi, K., Zych, M. D., & Jøsang, A. (2018). The impact of quantum computing on present cryptography. *arXiv preprint arXiv:1804.00200*.

[39] Savu, L. (2012). Signcryption scheme based on schnorr digital signature. *arXiv preprint arXiv:1202.1663*.

[40] Heiberg, S., & Willemson, J. (2014, October). Verifiable internet voting in Estonia. In *2014 6th international conference on electronic voting: Verifying the vote (evote)* (pp. 1-8). IEEE.

[41] Fouard, L., Duclos, M., & Lafourcade, P. (2007). Survey on electronic voting schemes. *supported by the ANR project AVOTÉ*.

[42] Specter, M. A., Koppel, J., & Weitzner, D. (2020). The ballot is busted before the blockchain: A security analysis of voatz, the first internet voting application used in us federal elections. In *29th {USENIX} Security Symposium ({USENIX} Security 20)* (pp. 1535-1553).

[43] Noether, S. (2015). Ring SIgnature Confidential Transactions for Monero. *IACR Cryptol. ePrint Arch.*, *2015*, 1098.

Bitcoin's energy consumption and social costs in relation to its capacity as a settlement layer

Lennart Ante[1], Ingo Fiedler[1,2]
[1] Blockchain Research Lab, Max-Brauer-Allee 46, 22765 Hamburg
[2] Concordia University, Faculty of Arts & Science, Montreal, Canada

Bitcoin runs on energy. The decentralized network's amount of energy consumption has resulted in multifaceted discussions about its efficiency and environmental impact. To put Bitcoin's energy consumption into perspective, we propose to relate (a) the energy consumption in TWh and (b) resulting social costs in the form of carbon emissions to the Dollar value settled on the Bitcoin network. Both metrics allow to relate and quantify the capacity of Bitcoin as a settlement layer to the network's energy consumption and resulting carbon emissions, or social costs. We find that in early 2021 Bitcoin (a) settles between $2,333 and $7,555 for each Dollar spent on energy and (b) that, on average, a Dollar settled on the Bitcoin blockchain causes in social costs between 0.007% and 0.01%, depending on the estimated energy consumption converted into the costs of carbon emissions. These results help to assess the efficiency, cost and sustainability of Bitcoin and may allow a comparison of Bitcoin with existing settlement base layers such as Fedwire or gold.

1. Introduction

In early 2021, the market capitalization of all Bitcoins [1] exceeded $1 trillion [2]. Over the course of the year 2020, over $6.3 trillion were moved on the decentralized Bitcoin network, which corresponds to a value of about $17.2 billion per day. In the first two months of 2021 alone, this value amounts to over $80 billion per day and extrapolates to an annual value settled of over $29 trillion [3]. Putting this figure in the context of, e.g., the centralized foreign exchange market, which is estimated at a daily volume of $6.6 trillion [4], the Bitcoin network would represent 0.26% of this market. If compared to a payment service such as VISA, Bitcoin's annually settled value of $29 trillion would represent roughly 2.5-times the annually value settled on the VISA network [5]. However this much-used comparison with VISA that works on top of an existing base-layer settlement system is not particularly apt. In fact, a better comparison is to other base-layer settlement systems like the American clearing house Fedwire, which in 2020 processed about 727 thousand transactions per day with an equivalent value of $3.3 trillion [6].

A key characteristic of the Bitcoin blockchain is that the underlying security of the decentralized network is ensured by the proof-of-work consensus mechanism [7]. In this process, so-called miners expend computing capacity by trying to guess a desired string consisting of numbers and letters before other miners, whereupon a reward, the so-called block reward, is paid out to the miner that successfully guessed the string. This "guessing" process does not follow any clear logic, but works via repetitive trial and error [8]. Accordingly, Bitcoin runs on energy, which in turn led to much discussion and criticism [9].

Various studies have set the goal of quantifying the energy consumption and resulting carbon emissions of the Bitcoin network [10]–[15] and other proof-of-work blockchains [16], [17]. This has even led to public scientific debates on the validity of specific models, assumptions or implications. With the *Cambridge Bitcoin Electricity Consumption Index (CBECI)* [18] and the *Bitcoin Energy Consumption Index (BECI)* [19], two scientifically sound methods have emerged that publish daily estimates of the energy consumption of the Bitcoin network. As of March 2021, the CBECI estimates an annual electricity consumption of 128 terawatt hours (TWh). At 78 TWh, the BECI's consumption estimate is significantly lower. Regardless of which of these two values is closer to the actual power consumption of the network, it can be clearly stated that it is a quantity of international significance, as it would mean that the Bitcoin network accounts for about 0.34-0.57% of the global energy consumption of 22,315 TWh in 2018 [20].

While the energy consumption of the Bitcoin blockchain is undoubtedly "high", it needs to be understood why this energy is expended and what benefit is created from the expenditure. The question of why is easily explained. Miners on the network receive transaction costs and newly issued Bitcoins when they successfully solve the proof-of-work process and validate unconfirmed Bitcoin transactions [21], [22]. Accordingly, the why can be explained via a simple monetary incentive. Miners compare the expected monetary reward with their (electricity) costs and are active as long as it is profitable. To put it simple: If the price of Bitcoin increases and the price of energy remains the same, the amount of energy a miner is willing to spend increases accordingly. The much more complex question of benefits from this energy the topic of this article. The essential use of Bitcoin is to make digital values—irrespective of the fact whether it represents "digital currency" or "digital gold"—secure and transfer-

able without the need of intermediaries. Effectively, intermediaries and their associated costs are replaced by an energy fueled protocol [8].

A first rationale for the significant energy consumption is the secure storage of value. In this paper we focus on the second rationale of Bitcoin: the settlement layer. With a daily settlement equivalent of roughly $80 billion as of 2021, the Bitcoin network represents the first decentralized way to securely transfer value. But how can this added value of the network be assessed and related to its (social) cost to understand whether Bitcoin is an "efficient" or "inefficient" settlement layer?

While an absolute measure of this added value is hardly possible, we tackle this question in a relative way: We put the settled value on the Bitcoin network into perspective to 1) the costs of electricity consumption and 2) the resulting environmental damages caused by the electricity consumption of Bitcoin miners. This yields two running indices that quantify Bitcoin's value as a settlement layer with regard to 1) energy consumed and 2) social costs of carbon emission. These allow to compare the value of Bitcoin with other decentralized (blockchain) settlement layers, such as Ethereum [23], but also to contrast it with centralized settlement layers such as the American FedWire, Clearing House Interbank Payments System (CHIPS) or the European TARGET2 system. These systems which correspond most closely to a centralized equivalent of the Bitcoin network, since they represent base layers with final clearing. On this basis, a relative evaluation can be made as to what extent the Bitcoin network is more or less efficient or inefficient than its centralized counterparties.

This article proceeds as follows. In Section 2, the underlying data, assumptions and methods are listed. In Section 3, metrics and statistics on the Bitcoin network are presented, followed by the above-mentioned metrics for energy consumption and carbon emissions or social costs. Section 4 reflects on the main results and concludes.

2. Data and variables

The metrics developed in this article are based on different data, which in turn come from various sources. Table 1 provides an overview of the variables and respective data sources/references.

Table 1: Overview of variables.

Variable	Description	Source
Blockchain metrics		
USD settled	The amount of successfully transferred Bitcoin transferred on the blockchain multiplied with the price of Bitcoin in USD.	[3]
Transactions	The amount of successful transactions on the Bitcoin blockchain.	[3]
Energy consumption and carbon footprint		
BECI estimate	The annualized estimation of Bitcoin's energy consumption (in TWh).	[18]
BECI minimum	The annualized estimation of Bitcoin's minimal energy consumption (in TWh).	[18]
CBECI estimate	The annualized estimation of Bitcoin's energy consumption (in TWh).	[19]
CBECI lower bound	The annualized estimation of the lower bound of Bitcoin's energy consumption (in TWh).	[19]
CBECI upper bound	The annualized estimation of the upper bound of Bitcoin's energy consumption (in TWh).	[19]

The first type of data (Bitcoin blockchain metrics) are accurately quantifiable metrics of the Bitcoin blockchain, which can be extracted from the blockchain in, e.g., daily, monthly or yearly intervals. The second category of data (Estimation of Bitcoin's energy consumption and carbon footprint) include estimates of energy consumption, energy mix, and carbon intensity of Bitcoin, which are accordingly subject to a certain degree of uncertainty. For this reason, we use two different data bases (the CBECI and BECI), which are likely to be the most frequently cited sources in literature and media.

3. Metrics for evaluating Bitcoin as a settlement layer.

3.1. Bitcoin network characteristics

Figure 1 shows the four key metrics used in this research over time. It can be seen that both metrics used to estimate Bitcoin's energy consumption show a clear increasing trend. In 2017 Bitcoin miners consumed 6.6 TWh in energy and in 2020 already 66 TWh, and for 2021 the CBECI estimates it to be 130 TWh [19]. 130 TWh is equal to 130 billion kilowatt hours (kWh), a unit people are more familiar with. While the number of transactions remains comparatively stable over time, the USD settled per month shows a strong increase from the end of 2020. In early 2021, over 2.7 trillion USD are settled on the Bitcoin blockchain.

3.2. Bitcoin's transactions settled in relation to its energy consumption

We put the sum of Bitcoin transactions ($TX_{i,t}$) in relation to the network's estimated energy consumption (EC_t):

$$TXE_t = \frac{\sum TX_{i,t}}{EC_t}$$

This allows us to quantify the basic efficiency of Bitcoin as a transaction network in relation to energy consumption. This relationship over time is visualized in Figure 2. For example, in January 2017 a transaction has cost 72kWh, in January 2020 already 666 kWh and in January 2021 it increased to 907 kWh (all figures CBECI estimates). This increasing trend implies that the network has become less efficient in terms of energy efficiency for processing individual transactions. Or, as Bitcoin proponents would claim, that the network has become much more secure over time.

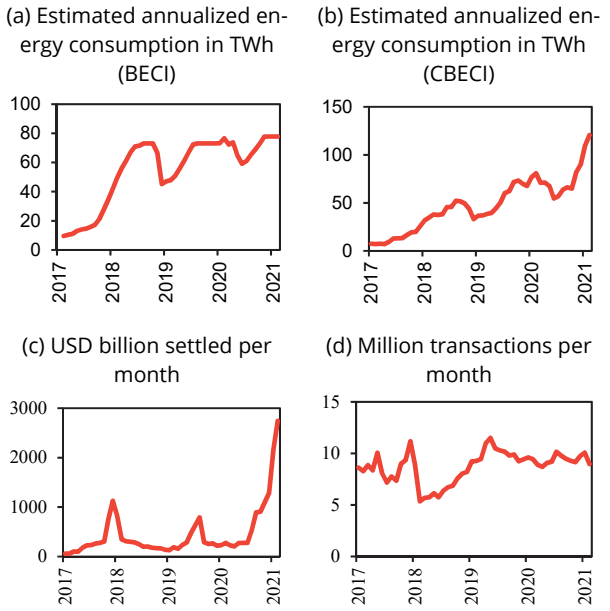

Fig. 1: Bitcoin network characteristics and estimates

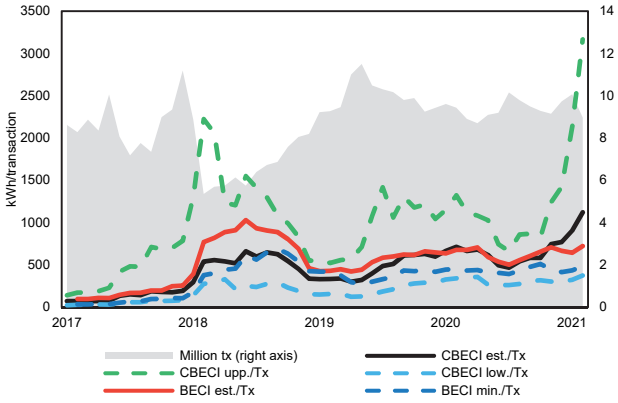

Fig. 2: Number of transactions settled in relation to different estimates of energy consumption of the Bitcoin network per month

However, missing from this consideration is the question of what exactly a transaction implies or means. For example, it makes a significant difference whether a transaction involves an equivalent value of $1 or $1 million. Accordingly, the equivalent value of transactions must be included in the calculation of the ratio to be meaningful.

3.3. Bitcoin's value settled in relation to its energy consumption

In the next step, we calculate the ratio between the transferred equivalent value of all Bitcoins and the estimated energy consumption of the network. We calculate the value as the product of the number of transferred Bitcoins ($BTC_{i,t}$) with the traded Bitcoin price at the time of the transaction ($P(USD)_{i,t}$):

$$VSE_t = \frac{\sum(BTC_{i,t} * P(USD)_{i,t})}{EC_t}$$

This relationship over time is visualized in Figure 3. Bitcoin settled $3,689 billion in 2017, $6,470 billion in January 2020, and interpolated for 2021 will settle $29,138 billion. Per kWh this translates to a settlement of $211 (BECI est.) to $278 (CBECI est.) in 2017, around $92 in 2020, and $252 (CBECI est.) to $378 (BECI est.) in 2021. Assuming a price of $0.05 per kWh as a global average, this translates to a settlement of $4,220-$5,560 in 2017, $1,840 in 2020 and $5,040-$7,560 in 2021 per Dollar spent on energy. To put it differently, the transaction costs for a settled Dollar on the Bitcoin network decreased from 0.018%-0.024% in 2017 to 0.013%-0.020% in 2021.

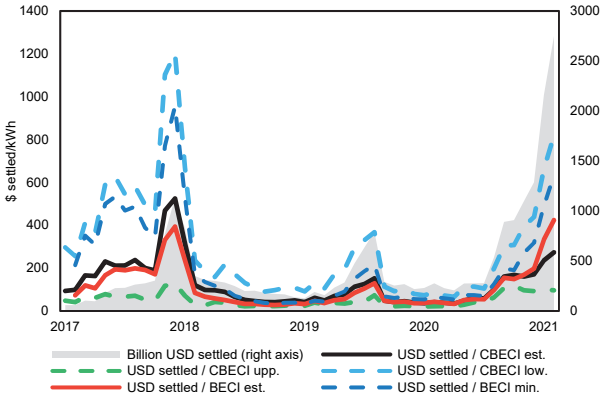

Fig. 3: USD value settled in relation to different estimates of energy consumption of the Bitcoin network per month

More detailed information on specific years as well as upper and lower bounds of energy consumption estimates are shown in Table 2.

3.4. The social costs of Bitcoin's energy consumption

The main argument against Bitcoin is not its energy consumption but rather the social costs caused by this consumption. Applying an estimated weighted average carbon intensity of 490 gCO2eq per kWh [12] allows to calculate the carbon footprint of the Bitcoin network. It yields CO_2 emission of 6.51 (CBECI est.) to 8.56 (BECI est.) million tons in 2017, around 34.5 million tons in 2020 and 38.13-57.17 million tons in 2021. With social costs of one emitted ton of carbon dioxide being estimated at $50 [24], Bitcoin caused social costs of $0.33-0.43 billion in 2017, $1.72 billion in 2021, and will cost in 2021 between $1.91 and $2.86 in 2021.

These increasing social costs can now be put into perspective by comparing them with the Dollar settled (Figure 4). Back in 2017 the ratio of social costs to $ settled is 0.009% to 0.012%, in 2020 nearly 3x higher with 0.027% and in 2021 lower again with 0.0065%-0.0097%.

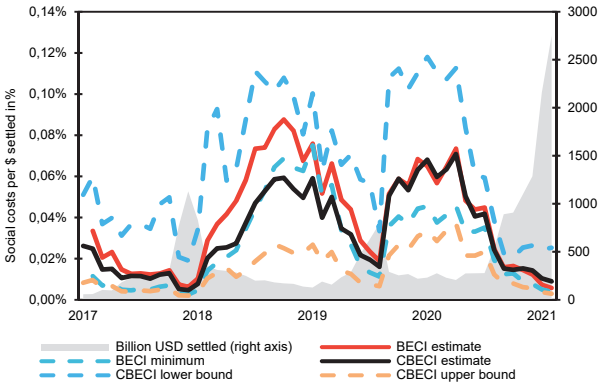

Fig. 4: Social costs per Dollar value settled for different estimates of energy consumption of the Bitcoin network per month.

4. Concluding remarks

The adoption and ownership of Bitcoin, cryptocurrencies and smart contract-based systems, such as decentralized finance (DeFi) or non-fungible tokens (NFTs) are becoming more and more relevant over time [25]–[28]. The increasing relevance of blockchain networks as a basic infrastructure for digital interaction and commerce poses a challenge for society to weigh the costs and benefits of this technology and innovation(s). There is no question that the Bitcoin network consumes a high amount of energy.

In this study, we contribute to the debate about the extent to which this energy consumption and its associated social costs of Bitcoin are "well spent" or "too high".

Table 2. Annual statistics on Dollar value settled in relation to energy consumption estimates of Bitcoin and the resulting social costs.

	2017	2018	2019	2020	2021
Value settled in billion USD	3,689.38	3,369.69	3,922.07	6,470.20	29,398.48i
Bitcoin Energy Consumption Index (BECI)					
Estimate in TWh	17.47i	62.52	63.96	70.29	77.82
Minimum in TWh	7.19i	40.11	44.35	49.13	52.29
USD settled / estimate in kWh	211.17	53.90	61.32	92.05	377.80
USD settled / minimum in kWh	513.16	84.02	88.44	131.68	562.22
Carbon emission (estimate) in million tons CO2	8.56	30.63	31.34	34.44	38.13
Carbon emission (minimum) in million tons CO2	3.52	19.65	21.73	24.07	25.62
Costs of Bitcoin network (estimate) in billion USD	0.43	1.53	1.57	1.72	1.91
Costs of Bitcoin network (minimum) in billion USD	0.18	0.98	1.09	1.20	1.28
Social costs per Dollar settled (estimate)	0.0116%	0.0455%	0.0400%	0.0266%	0.0065%
Social costs per Dollar settled (minimum)	0.0048%	0.0292%	0.0277%	0.0186%	0.0044%
Cambridge Bitcoin Electricity Consumption Index (CBECI)					
Estimate in TWh	13.29	41.82	54.37	70.4	116.67
Lower bound in TWh	5.35	18.93	23.58	34.33	39.71
Upper bound in TWh	45.52	102.32	112.17	115.33	316.08
USD settled / estimate in kWh	277.62	80.58	72.14	91.91	251.99
USD settled / lower bound in kWh	689.10	178.05	166.35	188.46	740.39
USD settled / upper bound in kWh	81.05	32.93	34.96	56.10	93.01
Carbon emission (estimate) in million tons CO2	6.51	20.49	26.64	34.50	57.17
Carbon emission (lower bound) in million tons CO2	2.62	9.28	11.55	16.82	19.46
Carbon emission (upper bound) in million tons CO2	22.30	50.14	54.96	56.51	154.88
Costs of Bitcoin network (estimate) in billion USD	0.33	1.02	1.33	1.72	2.86
Costs of Bitcoin network (lower bound) in billion USD	0.13	0.46	0.58	0.84	0.97
Costs of Bitcoin network (upper bound) in billion USD	1.12	2.51	2.75	2.83	7.74
Social costs per Dollar settled (estimate)	0.0088%	0.0304%	0.0340%	0.0267%	0.0097%
Social costs per Dollar settled (lower bound)	0.0036%	0.0138%	0.0147%	0.0130%	0.0033%
Social costs per Dollar settled (upper bound)	0.0302%	0.0744%	0.0701%	0.0437%	0.0263%

i: interpolated; Carbon emissions are in million tons based on 490 gCO2eq per kWh [12]; the cost per ton of CO2 is estimated at $50 [24].

We argue that a differentiated approach is needed, which puts the resource consumption and the (social) costs of the settlement layer Bitcoin in a comparable context. For this purpose, we set different measures of Bitcoin's estimated energy consumption in relation to a) the settled value in Dollars and b) the social costs in the form of estimated carbon emissions. This allows us to determine key figures that enable comparability with classic settlement layers. The results show that in 2021, a single Dollar of (energy) cost enables a settled value between $5,040 and $7,560. This translates into average transaction costs of 0.013%-0.020%.

This ratio increases with increasing power consumption and decreases with the Dollar amount settled. Since transactions are rather stable, the latter mainly relates to the price of Bitcoin, which is also the main driver of the hash power and thus energy invested into Bitcoin mining. It would thus not surprise, if both effects cancel each other and the social costs per transacted Dollar remains rather stable over time.

As a second metric to measure the relative efficiency of the Bitcoin network from a societal point of view, we suggest to compare the social costs resulting from carbon dioxide emissions of the Bitcoin mining activity to the value it settles every year. For every Dollar settled on the Bitcoin network in early 2021, between $0.000065 to $0.000097 (or 0.065% to 0.0097%) are caused in environmental damages due to CO_2 emissions. This figure gives

an indication that Bitcoin is indeed an expensive settlement layer, but that it is not totally out of line. It needs to be kept in mind that this result depends on the social cost of a carbon emission for which we used $50 per ton. It also depends on the actual CO_2 emission from Bitcoin mining. We simply assumed a global average, although there are good arguments that the ratio is higher for Bitcoin mining, which is often fueled by hydro power and an important contributor to shave peak loads and thus render renewable energies more efficient. However, it could also be argued that such energy is missing elsewhere and causes other energy demand to use non-renewables. Hence, the use of a global average seems adequate.

Potentially an even more informative evaluation of the efficiency of Bitcoin as a settlement layer comes from a comparison to other ways of settling value, for example, a bank wire or a payment in gold. This would need to take into account that the banking system hosts servers, maintains buildings, employs people (who not only need to commute to work, but also cannot engage in a different profession). The gold system comes with storage costs, costs of transportation and a mining process that is damaging to the environment and the workers, especially when quicksilver is used. However, to obtain the social costs of the banking system and the gold system are complex tasks beyond the scope of this paper.

Of course, it must be noted that there are significantly less energy-intensive blockchain networks or consensus mechanisms, which were not considered in more detail in this study [8]. Accordingly, future studies should not only include traditional settlement systems in their considerations and comparisons, but also other blockchains or distributed ledger systems.

References

[1] S. Nakamoto, "Bitcoin: A Peer-to Peer Electronic Cash System," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf. [Accessed: 12-Jun-2019].

[2] Coingecko, "Bitcoin market capitalization," 2021. [Online]. Available: https://www.coingecko.com/en/coins/bitcoin. [Accessed: 10-Mar-2021].

[3] Glassnode, "Glassnode.com," 2020. .

[4] BIS, "Foreign exchange turnover in April 2019 - Triennial Central Bank Survey," 2019.

[5] VISA, "VISA 2019 Corporate Responsibility & Sustainability Report," 2020.

[6] The Federal Reserve, "Fedwire® Funds Service - Annual Statistics," 2021. [Online]. Available: https://www.frbservices.org/resources/financial-services/wires/volume-value-stats/annual-stats.html. [Accessed: 15-Mar-2021].

[7] C. Dwork and M. Naor, "Pricing via processing or combatting junk mail," in Annual International Cryptology Conference, 1992, pp. 139–147.

[8] F. Steinmetz, L. Ante, and I. Fiedler, Blockchain and the Digital Economy: The Socio-Economic Impact of *Blockchain Technology*. Agenda Publishing, 2020.

[9] L. Ante, F. Steinmetz, and I. Fiedler, "Blockchain and energy: A bibliometric analysis and review," *Renew. Sustain. Energy Rev.*, vol. 137, p. 110597, 2021.

[10] A. de Vries, "Bitcoin's Growing Energy Problem," *Joule*, vol. 2, no. 5, pp. 801–805, 2018.

[11] M. J. Krause and T. Tolaymat, "Quantification of energy and carbon costs for mining cryptocurrencies," *Nat. Sustain.*, vol. 1, no. 11, pp. 711–718, 2018.

[12] C. Stoll, L. Klaaßen, and U. Gallersdörfer, "The Carbon Footprint of Bitcoin," Joule, vol. 3, no. 7, pp. 1647–1661, 2019.

[13] A. de Vries, "Bitcoin boom: what rising prices mean for the network's energy consumption," Joule, 2021.

[14] A. de Vries, "Bitcoin's energy consumption is underestimated: A market dynamics approach," Energy Res. Soc. Sci., vol. 70, p. 101721, 2020.

[15] J. Sedlmeir, H. U. Buhl, G. Fridgen, and R. Keller, "The Energy Consumption of Blockchain Technology: Beyond Myth," Bus. Inf. Syst. Eng., vol. 62, no. 6, pp. 599–608, 2020.

[16] U. Gallersdörfer, L. Klaaßen, and C. Stoll, "Energy Consumption of Cryptocurrencies Beyond Bitcoin," Joule, vol. 4, no. 9, pp. 1843–1846, 2020.

[17] J. Li, N. Li, J. Peng, H. Cui, and Z. Wu, "Energy consumption of cryptocurrency mining: A study of electricity consumption in mining cryptocurrencies," Energy, vol. 168, pp. 160–168, 2019.

[18] M. Rauchs, A. Blandin, and A. Dek, "Cambridge Bitcoin Electricity Consumption Index (CBECI)," 2021. .

[19] Digiconomist, "Bitcoin Energy Consumption Index," 2021. [Online]. Available: https://digiconomist.net/bitcoin-energy-consumption/. [Accessed: 05-Mar-2021].

[20] IEA, "Electricity Information: Overview," 2020. [Online]. Available: https://www.iea.org/reports/electricity-information-overview. [Accessed: 10-Mar-2021].

[21] E. Strehle and L. Ante, "Exclusive Mining of Blockchain Transactions," in Scientific Reports 2020 - Conference proceedings of the Scientific Track of the Blockchain Autumn School 2020, 2020, pp. 87–95.

[22] A. Back, "Hashcash - a denial of service countermeasure," 2002.

[23] V. Buterin, "Ethereum white paper - A next gerneration smart contract & decentralized application platform," no. January, pp. 1–36, 2015.

[24] P. Howard and D. Sylvan, "Expert Consensus on the Economics of Climate Change," 2015.

[25] L. Ante, "Non-fungible token (NFT) markets on the Ethereum blockchain: Temporal development, cointegration and interrelations," BRL Work. Pap., vol. 22, 2021.

[26] F. Schär, "Decentralized Finance: On Blockchain- and Smart Contract-based Financial Markets," Fed.

Reserv. Bank St. Louis, 2021.
[27] L. Ante, “Smart Contracts on the Blockchain – A Bibliometric Analysis and Review,” Telemat. Informatics, vol. 57, p. 101519, 2021.
[28] F. Steinmetz, M. von Meduna, L. Ante, and I. Fiedler, “Ownership, uses and perceptions of cryptocurrency: Results from a population survey,” Technol. Forecast. Soc. Change, vol. 173, no. May, p. 121073, 2021.

Development of Identity Solutions for the Internet

Felix Hildebrandt
BC Development Labs GmbH as Blockchains LLC, Markt 16, D-09648 Mittweida

Mapping identities, digital assets, and people's profiles on the internet is getting much traction in the blockchain cosmos lately. The new technology is currently forming architectures that will further pave new ways to reach fundamental mechanisms to interact in a decentralized, user-centered manner. These schemes are often declared as the next generation of the web. Within the article will be shown, how the internet has evolved in managing identities, what problems arose, and how new data architectures help build applications on top of privacy rights. Both technological and ethical perspectives are viewed to answer which guidelines should be considered to fulfill the upcoming branch of decentralized services and what we can learn from historical schemes regarding their privacy, accounting, and user data.

1. Identity within the common Internet

Homepages could be described as windows into a new world as the internet pushed forward and the initial web appeared in the late 80s. They were mainly used to share knowledge from universities around the world and were read-only pages without user management. Within the backend, the network consisted of servers, forming a mesh around the globe. With the TCP and IP protocol, data transfers between machines were focused on transmitting information to a specific device address. All of the webpage data was stored on servers, and regular private computers could connect and load data from or to them. But the purpose of making information accessible for a wide variety of society was fulfilled quickly, and the urge to interact with computers to exchange personal data grew.

At this time, communication was still more or less done via phone or mail, and email use began to grow. Due to the rudimentary technologies and the inefficient computers, for administrators, it was only possible to determine how many devices saw certain pages and at what time they consumed the content. This disadvantage led to new technology to gain more information about the user in front of the device and simplify the communication process.

When the interaction between computers evolved, the internet was generally designated as Web 2 and fundamentally influenced by the previous questions. From today's perspective, it mainly was a front-end revolution with new browser functionalities, leaving server-centered structures and databases as a backend.

IT security and backup mechanisms increased drastically to manage the throughput and safety of the now most valuable goods: user data. Large server centers had to be built and user files secured from unauthored access because frauds rose. On the user side, cookies and APIs were developed to track users' behavior within sessions and store additional traffic- or user information within the browser. Tracking was in total focus, and cart content, areas of interest, or already seen advertising links were essential for business- with it, also identity management. New use cases like social media, e-commerce, or even interactive knowledge platforms proliferated. A vast market of user data emerged to create intricate user data patterns to optimize monetarization and predict behavior. [1] What started as the era of optimizing profits by tracking users emerged into directly gaining profit from personal information from the user. Price and advertisement align with gathered user behavior. Data analysis is a considerable immense amount of how digital products gain value nowadays. [2, 3]

Looking closer at what identity within the web means, it is mostly just tracked down to the device a person uses combined with several accounts created for almost every software product or service in use. Mostly an email plus the login password. Such an account allows the utilization of a particular utility and is set up as a top-to-bottom connection from the manufacturer to the blended-in user.

The manufacturer is the determiner, holding all of the user's information. A user login to this account just represents a device, entering a service and gaining access to a person's specified information. Such access can be created directly from a service provider or by linking to existing logins from others. The second scheme was specially evolved by huge IT giants such as Google, Facebook, and Microsoft, which have billions of users. Within seconds, they can just log in to multiple services using one main account, increasing convenience but also the risk of losing passwords or whole logins and raising problems if the referred account is not valid anymore or some service provider is currently unavailable.

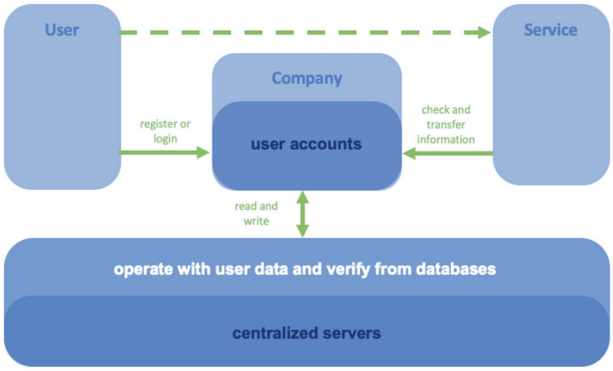

Fig. 1: Regular Web 2 Login Scheme

Many authentication methods evolved to gain authorization from companies or service providers, mainly the OAuth 2.0 protocol. [4] With this scheme, servers can hand out access tokens to users for authentication when using centralized servers on their login. Tokens imply that the user has to put trust in the service provider. However, they can only work with one provider, meaning users need to have accounts for every service in use. Not only do users need to authenticate on multiple token endpoints, but they're also permanently confronted with the man-in-the-middle principle: the intermediate provider can always surveil their relationship activities with the authenticated account to their connected services. Connected logins provide a colossal danger for privacy concerns and attacks that can affect all linked services at once. [5.1]

Another downside: regular schemes just work by transmitting data over device addresses, which can be manipulated or intercepted. The non-existence of a sophisticated identity layer within the internet is one of the primary sources of cybercrime. [5.2]

Further, IBM President Ginni Rometty describes cybersecurity about identity theft as the most splendid profession- and industry-wide threat globally, causing enormous financial and personal damage. [6]

The problem is that the internet was mainly built around machines with their MAC addresses, not for individuals. There is no accurate identity verification- only mechanisms to cover most frauds and give out copies of user rights. With passwords, users gain access to data and services operated and saved on the company's servers. On the other side, documents are digitalized and handed over to third parties, resulting in numerous hoardings of certified copies. It is easy to lose track of who owns, uses, or is up to date on your data because of all the different instances holding parts or duplicates. The scheme quickly shifts control over data to the respective entity, which guarantees its security and legal use. The bureaucracy and needed trust are immense.

Another negative point to mention is that the data is stored on servers operated by the company, meaning it technically belongs to them, even if users own parts of it. [7.1] Even if distortion needs to be done to be compliant with specific laws, if the user gains the right to delete or, more specifically, manage his scraped or purposely put data, it's just a matter of computation power how quickly companies can throughput their data in analytic schemes to get desired advantages. [8] The offset also counts when dodging specific mechanisms to be compliant with rights instantiated from the governments. For the average citizen, it is neither convenient nor user-friendly. At this point, managing all your data and accesses have become a rat-tail of problems.

2. Implementation of Data and Security Laws

The current state also raised issues with informatics ethical perspective, which lends to the General Data Protection Regulation of the European Union in 2018. The GDPR concluded that “everything that helps identify a person, regardless of whether it refers to a natural person's professional, private, or public life”, counts as personal data. [9.1]

The ethical classification is based on this definition and should ensure users full access to their own data management, may it be about critical information or not. User data is collected in any case and is very difficult to be limited. Therefore, the collection of data should not be restricted, but citizens should have full access and transparency regarding the data being collected from and on them.

The General Data Protection Regulation is used to protect the inhabitants of the European Union and their collected data. Data sovereignty must be presented as a fundamental right and guaranteed by all companies in the future. It applies to all citizens, constitutions, and businesses within the European Union. The goals of the GDPR are the protection of natural persons in the processing of personal data and the free movement of such, as well as the safety of fundamental rights, fundamental freedoms, and protection of personal data. Companies need to clearly define what personal data will be stored and which methods are applied to it, in order to be able to protect citizens. [9.2]

In the future, companies will have to continuedly adapt to new regulations. On the way, users will gain more rights to erase data and look up where and when the data was stored. Higher fines and the obligation to notify users in the event of infringements will follow as well. All requirements are always extraterritorial, meaning it is essential from whom the data is and where the data flows, not from where the company operates if servers are located outside the EU. Also, certificates, which verify that certain services and products fulfill the GDPR standards, were discussed. [10] Verification could be an obstacle because the EU has to check up on code and algorithms used within digital services and perform periodic tests. What's already ubiquitous in the food industry could be a lengthy restructuring of digital ecosystems.

Identities can be found in every business, healthcare, government, e-commerce, or future identities in IoT. There is a high relevance in rethinking and changing how data is stored or managed from small companies to big IT giants.

As defined within the GDPR, companies must comply with the data protection rights shown in their checklist. [11] The identity infrastructure is expensive: many companies are still caught up in data ownership lawsuits, ambiguous data sales, and user behavior prediction within gray areas. [3] Because users have the right to manage their data with growing functionality, this will further increase. Users already have the right to prevent the collection of certain data and force its deletion. [12] The wording clearly defines that the data collected is owned by the users, and people can allow access if they wish to do so. Despite the existing Data Protection Regulation, not all companies fully adhere to the established rules or make it nearly impossible due to very cumbersome navigation. If companies provide more transparency, users will gain more possibilities for objection regarding personal data and user profiles. It also discloses the sources and origin of the data. These aspects can limit the quality of Big Data processes if users deny the gathering of specific data streams. However, it is the right step to gain a fair interaction and comply with human rights without changing backside structures. It strengthens customer loyalty and significance of analysis simultaneously.

3. New Approaches on Digital Identities

Within the blockchain space, the adage "not your private key, not your coins" became public. [13] If this would be applied as common sense facing the current web 2, it could be translated into "not your service, not your data." Even with regulations and the right over data, you can never be sure how the data has been used or utilized until you force deletion.

The goal of decentralized identity is to image rights and identifications of identity reliably and give the people back their data's power. For this to happen, it must be defined what an actual online identity means. As individuals in the real world, persons share relationships. Both are individual operators, and the relationship doesn't belong to anyone, as it's the connection between them. Looking at the current Web 2, it is the opposite: companies and services operate identifiers of user's identities and manage the personal data they are giving away. As the previous chapter told, users never have their own identity or sovereignty. Citizens just gain more rights to access certain functionalities of their instantiated datasets at most. It's a very high workload for every party involved to comply with or check up on personal data. Web 3 concepts will make it much more efficient to comply with regulations because they are built on privacy rights and offer digital identities which have relationships like in the offline world, where nobody relies on each other. Users can just verify other participant's datasets by proving their verifiable credentials when asked.

The term Web 3 is already common sense when looking into the future, defining a more decentralized way how the internet works by using decentralized blockchain networks that act as the enablers but also processors behind. The new generation of web develops a bit more gradient than the previous, because for the first time, the fundamental backend technology of the internet is tackled. The unbeatable factor here: For the first time in history, actual digitally values can be signed, transmitted, verified, and used between global instances. Private and public keys are used to secure the connection between such parties. The cryptography within such networks has the power to abandon previous centralized server approaches for safer user-centric technology, without the need to trust intermediaries.

New concepts rely on decentralized peer-to-peer networks forming unified ledgers. This approach not only introduces more resilient and secure blockchain networks: the governance of software systems will also fully depend on protocol consensus from the blockchain itself, instead of large instances bearing power. Such networks also drastically lower system administration and IT security costs for companies because users hold their identity data independently. On top of that, transparency is a significant aspect.

When running decentralized applications, there is a huge trend to make source code public so everyone can adopt and build with it. Transparency comes from raising the level of trust participants have in the network or application and forming the governance of such. [14]

Not only are future identity solutions transparent, but they will also store most data on devices within wallet applications, pushing self-sovereignty even further. Sensitive Data will likely be stored off-chain, just releasing hashes as verifiable credentials onto the blockchain itself. Actions on the ledger can be executed by referring back to an actual address of an account, not only commands transmitted by a particular device as we used to know from Web 2. Within such an approach, multiple software systems can request the verification of one piece of public data or hashes from offline information. Publicly available encrypted files also solve data duplication. [7.2]

All features bring a lot of responsibility back to the user. Therefore, more user-friendly concepts need to develop over time for a seamless transition. As Alex Preukschat and Drummond Reed describe, the concept of Self-Sovereign Identity, SSI in short, is "the best overall analogy because it's how we prove our identity in the real world: by getting out our wallet and showing the credentials we have obtained from other trusted parties. The difference is that with decentralized digital identity, we are doing this with digital wallets, digital credentials, and digital connections." [5.3]

As already mentioned, blockchain technology offers the exchange of digital values by using digital signatures from one wallet to another. This value can be anything from fungible cryptocurrency to non-fungible credentials, artworks, documents, and so on.

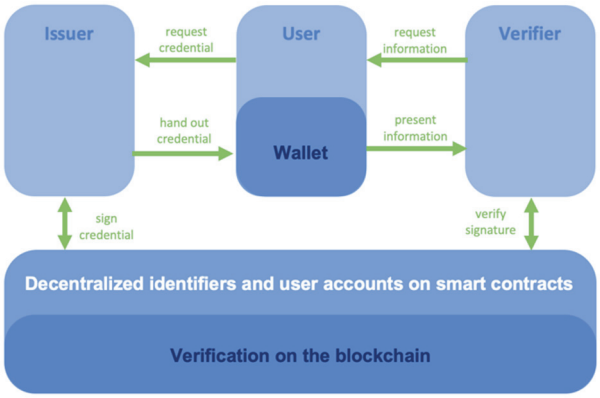

Fig. 2: Web 3 Identity

There are three main roles within the network: a issuer, a verifier, and the user itself. As in the real world, the user has the owned wallet and requests a credential from the issuer. The individual, therefore, may need to give additional data to him. After the request is fulfilled, the issuer signs a credential on the blockchain, referred to the user's address, and issues the new credential to the user's wallet. With the issuers signature and proof that he holds the identity-related data in his wallet, the holder can now use services that need those certificates. For instance, he could use a passport handed out before an exchange. The verifier, in this case, the exchange provider, will request the newly acquired value and verify its signature, before the exchange is transacted. For this to happen, the user needs to present the credential to him. [15, 16]

Some examples of use cases can further help understand its potential on top of it. For e-Commerce, registration and payment could be made directly through the SSI, evading passwords and accounts. All receipts could be handed out as credentials and are written into the blockchain. For finance, citizens could demand any bank service on the fly, eliminating bureaucracy and submission of the same forms. If both parties support SSI interfaces, they can exchange their required credentials and even use multi-signature for essential documents and high value transactions. Health documents could also be shared instantaneously with clients, friends, or nurses within healthcare, providing consent for medical procedures. Because of the blockchain, there could also be lifetime histories of vaccinations, which can be verified or shared with other instances.

For traveling, boarding passes and checkpoints of trips can be documented to verify places visited in the past, and calculate hazard potentials. Even tickets for airlines, hotels, trains or music could be automatically connected to someone's wallet. [5.3]

As the last example, different interpretations of SSI could be used to fully digitalize grade certificates, file transfers, and cross-university or even transnational IDs within the education field. Currently, one colossal driver is Educhain. [17]

Like in the real world, both sides will always show their verifiable credentials to ensure instances are the ones they claim to be. As expected, every example could be managed directly from the smartphone, fully self-sovereign, if all participants accept one ledger system. Decentralized solutions are always tied to network effects. If only a minority of services uses SSI, it could be an obstacle. The needed network effect is an enabler for cross-chain solutions like Polkadot to connect transactions of wallets and contracts to fit into one huge SSI ecosystem. [18] An obvious downside also is that data cannot be verified offline. This could be solved by making the internet accessible to every corner of the world from satellite meshes. Such a principle is currently in an early release from Starlink. [19] The final problem could be seen as the management of keys for wallets, which are needed to operate the SSI software. One solution to this topic will be solved within the next section.

4. Contract-Based Accounting

Within the future, users could freely manage a lot of digital information about themselves. For people, there needs to be proper accounting and ordering of all glimpses of verifiable credentials. That's why even user profiles on the blockchain are in transition. Regularly, users just have wallets to interact within the blockchain for simple transactions. But there are also smart contracts, which can add a lot more functionality: scripts running on decentralized virtual machines from blockchain networks, that act like regular applications. Such smart contracts can be referred to as a decentralized "world computer" where blockchain nodes collectively provide the machine's power. [20] They can execute programs, and map user accounts or profiles as known today. More complexity mostly comes with additional functionality and defines a huge step to get closer to the initial defined goal of Web 3 identities.

By using this computation power, which is triggered when certain network transactions were sent, complex business logic can be mapped on top of it, starting chains of smart contract code execution. With the help of such, even multiple wallets from different devices can be combined to user accounts on fully manageable identity ecosystems. All devices or wallets connected to one account can then speak as one combined identity, enabling role- and right- as well as separated key-management.

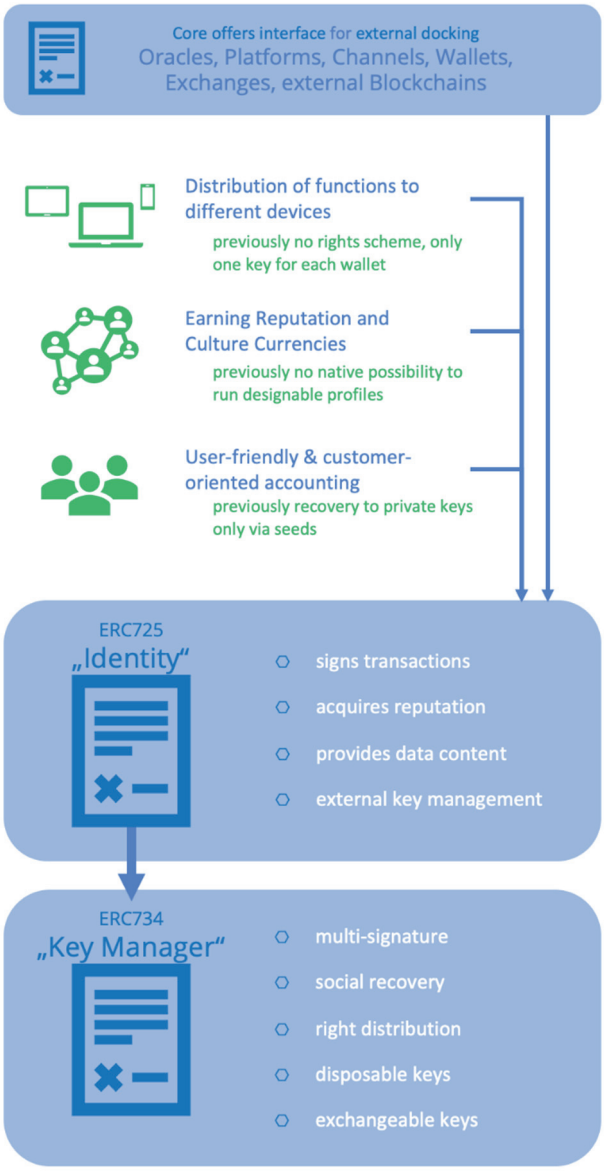

Fig. 3: Contract-Based Accounting

This single contract account can then manage all kinds of digital assets, currencies, etc. Even security contracts could be interposed to reverse accidental transactions back to the initial situation. The clue here is that actual data can always be hashed and written into smart contracts, acting like profiles. As for the identity controller, the owner can encode the attached secret information with all its keys in the value store of the contract. This way is more user-friendly than regular blockchain solutions, because of the more accessible backup and recovery schemes with such key management. The initial idea of contract-based accounting was already discussed within the early days of Ethereum in 2014. However, it was dropped because of the early smart contract functionality's complexity, key security, time-limits and black swan potentials. [21]

In 2017 identity was first standardized as ERC725 on the Ethereum blockchain and further developed afterwards, as seen in figure 3. [22]

Because of the utilization of the Ethereum blockchain, mainly coming from the DeFi space [23], it would be too expensive to realize contract-based accounting nowadays. Complex contracts have to include lots of transactions and all of them need to be covered with expensive fees. Even grand scaling schemes like the rollup technology [24] or sharding [25] won't solve that much throughput if every human being or device's identity is managed within one blockchain system.

Scalability issues are why the term "blockchain of blockchains" evolved. The scheme describes a network where blockchains can connect with each other. Those connections could be similar to the internet, which grew larger with more and more connected servers. Within the Web 3, branches likely will need to split apart in different networks.

With this idea in mind, Lukso was founded in 2018. [26] Creating an ecosystem for new smart contract standards and revealing the possibilities of user accounts and their identity for the creative economy are the project's primary goal. The network will be tackled by using universal profile structures known from social media. It differs from personal identities, often meant in SSI development, and creates public personas with the same functionality, holding any kind of digital art or unique NFTs. While shifting around smart contracts behind the scenes, users can add credentials, links to other networks, or functionalities for different apps. This could be perceived as a light identity management system and a new era of self-sovereign social media platforms. The system could also be used for decentralized login mechanisms for software services. [27]

In comparison to the regular servers used to log in, data loss or downtime can be eliminated with blockchain networks, if their nodes are decentralized around the world. Even personal identities could, at some point, be linked to universal public profiles as hybrid SSI solutions, while only gaining access to personal off-chain data via on-chain logins. With the ERC 1056 standard, the Ethereum ecosystem already has its solution for personal off-chain SSI data, linking public keys from users to them to utilize identity references. [28]

5. Guidelines for Decentralized Development

The famous question is how to define ethics and principles by which we can assess software services operating with user data, e.g., their identities. The GI, an IT representative in Germany, offers prefabricated guidelines by which standard software should develop and evaluated. The GI is the largest German non-profit professional society that has set itself the goal to promote computer technology. It has 20,000 members and counts as a member of the Council of the European Societies for computer science. The guidelines have been designed so that professional ethics or moral conflicts are objects of joint reflection. The instructions are intended to provide guidance to design, create, operate, or use IT systems.

Because of the user data-related topic, the guidelines are linked to the SSI context.

The programmed software should be designed and legally verified by people that possess current and comprehensive expertise. Within the blockchain space, programmers should have deep knowledge about the network and governance they build on, as well as their smart contracts. At the same time, constructive criticism is needed, which is amplified through the high transparency within Web 3. For the exchange of information, good communication skills are necessary to evaluate solutions, communicate them to other people, and simplify them to an abstract level. In this topic, permanent training in the subject should be necessary, especially on new approaches and news on decentralized identifiers and verifiable credentials. Developers also need legal competence when working with tokens or user data within the blockchain space.

Companies bear social responsibility and impact because identities will work and live within new blockchain accounting systems. In this regard, users and builders will contribute to socially acceptable and sustainable solutions. [29]

Developers have to adhere to the principles of ethics about data protection. They should ideally also build their applications on them, not with them. When collecting large datasets with unique content, as "big data" applications do, the National IT Summit has designed its own guidelines. These principles can be summarized in the following sections and transferred directly to the development of SSI software. [30]

Consumers and users must be aware of the purpose or benefit of the application, its processing, and the amount of data collected. They must also be notified when data is transferred to third parties.

The transparency of this information is needed to ensure self-determined actions. Secondly, users have to approve the usage of data, need to see their collected data as well as resulting evaluations. They must also explicitly agree with the linking of data and transfer of information.

The software only has to gather the minimal required data, which is indispensable to reach the solutions target. On this topic, anonymous or pseudonymous data has to be preferred. It also has to be regularly checked for responsible handling of the personal data and that no violation of rights and interests has happened. If so, users also need to be transparently informed about it. The data should never be processed for ethically or morally dishonest purposes and evaluations, links, or data transfers must not harm users nor their possibilities. [30] To summarize, there are many ways to collect data, but a clear line is drawn when the user shows dislike or harms the user instead of adding value. [9.3]

Ethics also cover how the software is instantiated and brought to the user base. As already told in the last chapter, total transparency, e.g., open-source code, is mandatory when identifying solutions that claim to be self-sovereign. Users must have the right to prove and modify their digital identity software. As this right is given, the identity owner's use case possibilities further increase. The analogy can be drawn to the real world of social behavior.Within a modern democratic government, citizens as individual human beings can rely or demand on their rights and human dignity. Anyone can express freely, and the political opinions of the majority are taken into the main focus when developing future governmental plans. To relish everyone's rights and eliminate upcoming problems, citizens must work as a union to provide and establish bright, reflected futures. This approach also reduces the risk of exploitation from corporations, so that individuals can move on in life with fewer boundaries. We should build fair digital systems like we do in the real world: empower individuals, and form strong relationships while remaining fully independent. Therefore, it is necessary to promote the open-source development of self-sovereign identity. [5.4]

6. Current State of SSI and Outlook

The significant advantage of Web 3 with its user-centered approach is that it represents human interaction-like relation between digital software services. When connected to blockchain networks SSI's, it can unfold their true potential. The network is fail-safe, decentralized, executes actions on its store of value all in one. On the negative side, accurate SSI accounting is in its early age and not as fast and scalable as centralized services. Creating complex schemes on SSI-based components requires a lot of transactions when instantiating. On top of that, even identity standards have not found significant adoption by now. In 2018, Nick Poulden first released a fully functional prototype on the first version of the ERC 725 identity standard on Ethereum. [31] It was a huge success, seeing the technical concepts being brought to life. Ethereum is currently trying to create its standalone login functionality, and so it is expected from multiple other blockchains.

For the development industry, SSI is understood as the new hype. There are plenty projects directing into different areas: may it be strictly private identifiers, public profiling or hybrid variants. Many research facilities are working out various concepts and protocols for citizenships, student organization, financing-, travel- or new social media, etc. The key will be interoperability, which is difficult to determine, because of the rough standartisation being done by now. [15, 16]

Mass adoption will most likely be gradual because existing solutions are convenient and currently functional to use. An additional downside is that the technology needs to be brought to the issuers across all industries, mainly governmental or old established instances. Both, issuers and users need to accept the same ledger so that

verifying instances can prove their verified credentials. It has to be said, that it will require great products to change the industry. Overall, SSI is just facing the start of a new century of how digital relationships are managed.

Acknowledgements

Special thanks to BC Development Labs GmbH as Blockchains LLC which supports my research, and practical work as well as giving me the opportunity to build meaningful and up to date software which will be used in future development.

References

[1] Kaushik, A. (2010): Web analytics 2.0. The art of online accountability & science of customer centricity. Hoboken, N.J.: John Wiley (Sybex serious skills).

[2] Patel, N. (2019). The future of AT&T is an ad-tracking nightmare hellworld. The Verge. Retrieved August 31, 2021, from https://www.theverge.com/2019/5/22/18635674/att-location-ad-tracking-data-collection-privacy-nightmare

[3] Bernet, D. (Director). (2015). Democracy [Documentary]. INDI FILM.

[4] Parecki, A. (2021). OAuth 2.0 — OAuth. OAuth.Net. Retrieved August 31, 2021, from https://oauth.net/2/

[5] Preukschat & Reed, A. & D. (2021). Self-Sovereign Identity: Decentralized Digital Identity and Verifiable Credentials. Manning Publications Co. 1) p. 9; 2) p. 4; 3) p. 10; 4) p. 285

[6] Morgan, S. M. (2015, November 24). IBM's CEO On Hackers: "Cyber Crime Is The Greatest Threat To Every Company In The World." Forbes. Retrieved August 31, 2021, from https://www.forbes.com/sites/stevemorgan/2015/11/24/ibms-ceo-on-hackers-cyber-crime-is-the-greatest-threat-to-every-company-in-the-world/

[7] Voshmgir, S. (2020). Token Economy: How the Web3 reinvents the internet. Shermin Voshmgir. 1) p. 32; 2) p 27 ff., p 95 ff.

[8] Mitchell, J. (2019). The Evolution of the Internet, Identity, Privacy and Tracking – How Cookies and Tracking Exploded, and Why We Need New Standards for Consumer Privacy – IAB Tech Lab. IABTechLab. Retrieved August 31, 2021, from https://iabtechlab.com/blog/evolution-of-internet-identity-privacy-tracking/

[9] GDPR-Info.eu. (2021). Datenschutz-Grundverordnung: DSGVO als übersichtliche Seite. Datenschutz-Grundverordnung (DSGVO). Retrieved August 31, 2021, from https://dsgvo-gesetz.de/. 1) ch. 1 art. 4; 2) ch. 1 art. 1-3; 3) ch. 2

[10] Keithahn & Conway. (2020). DSGVO: Zusammenfassung und Ausblick. Mailjet. Retrieved August 31, 2021, from https://www.mailjet.de/dsgvo/?gclid=EAIaIQobChMIx9nyhb7S5QIVgrTtCh3y9g2VEAAYAiAAEgLdIPD_BwE#was-ist-dsgvo

[11] GDPR.eu. (2019). GDPR compliance checklist. Retrieved August 31, 2021, from https://gdpr.eu/checklist/

[12] Wolford, B. (2020). Everything you need to know about the "Right to be forgotten." GDPR.Eu. Retrieved August 31, 2021, from https://gdpr.eu/right-to-be-forgotten/

[13] Ledger Academy. (2020). Not Your Keys, Not Your Coins: Why It Matters. Retrieved August 31, 2021, from https://www.ledger.com/academy/not-your-keys-not-your-coins-why-it-matters

[14] Simon, A. (2018). Blockchain evolution: A quick guide and why open source is at the heart of it. Opensource.Com. Retrieved August 31, 2021, from https://opensource.com/article/18/6/blockchain-guide-next-generation

[15] W3.org. (2019). Verifiable Credentials Data Model 1.0. Retrieved August 31, 2021, from https://www.w3.org/TR/vc-data-model/

[16] W3.org. (2021). Decentralized Identifiers (DIDs) v1.0. Retrieved August 31, 2021, from https://www.w3.org/TR/did-core/

[17] Educhain. (2021). The issue, Share and Verify Any Academic Record Digitally. Educhain.io. Retrieved August 31, 2021, from https://educhain.io

[18] Wood, G. (2016). Polkadot Whitepaper. Polkadot. Retrieved August 31, 2021, from https://polkadot.network/PolkaDotPaper.pdf

[19] Crist, R. (2021). Starlink explained: Everything you should know about Elon Musk's satellite internet venture. CNET. Retrieved August 31, 2021, from https://www.cnet.com/home/internet/starlink-satellite-internet-explained/

[20] Buterin, V. (2014). Ethereum whitepaper - whitepaper.io. Ethereum. Retrieved August 31, 2021, from https://whitepaper.io/document/5/ethereum-whitepaper

[21] Recksiek, M. (2021). Fabian Vogelsteller über NFTs, LUKSO, Krypto & die Zukunft. YouTube. Retrieved August 31, 2021, from https://www.youtube.com/watch?v=KYoBJq9lA3w&ab_channel=Bitcoin2Go

[22] Vogelsteller, F. (2017). ERC: Proxy Account · Issue #725 · ethereum/EIPs. GitHub. Retrieved August 31, 2021, from https://github.com/ethereum/EIPs/issues/725

[23] Varshney, A. (2021). Ethereum and DeFi are forcing smart contract platforms to evolve. Cointelegraph. Retrieved August 31, 2021, from https://cointelegraph.com/news/ethereum-and-defi-are-forcing-smart-contract-platforms-to-evolve

[24] Interdax. (2020). Scaling Ethereum on L2: Optimistic and ZK-Rollups | Interdax Blog. Medium. Retrieved August 31, 2021, from https://medium.com/interdax/ethereum-l2-

optimistic-and-zk-rollups-dffa58870c93
[25] Ethereum. (2021). Shard chains. Ethereum.Org. Retrieved August 31, 2021, from https://ethereum.org/en/eth2/shard-chains/
[26] Vogelsteller, F. (2018). Lukso Whitepaper. Lukso Network. Retrieved August 31, 2021, from https://lukso.network/assets/LUKSO_Whitepaper.pdf
[27] Patel & Sahoo & Mohanta. (2019). DAuth: A Decentralised Web Authentication System using Ethereum. Reseachgate. Retrieved August 31, 2021, from https://www.researchgate.net/publication/337513916_DAuth_A_Decentralized_Web_Authentication_System_using_Ethereum_based_Blockchain
[28] Thorstensson, J. (2018). ERC: Lightweight Identity · Issue #1056 · ethereum/EIPs. GitHub. Retrieved August 31, 2021, from https://github.com/ethereum/EIPs/issues/1056
[29] GI. (2021). Unsere Ethischen Leitlinien - Gesellschaft für Informatik e.V. Gesellschaft für Informatik e.V. (GI). Retrieved August 31, 2021, from https://gi.de/ueber-uns/organisation/unsere-ethischen-leitlinien/
[30] Nationaler IT Gipfel. (2015). Leitlinien für den Big-Data-Einsatz im Überblick. Digitale Technolo-gien. Retrieved August 31, 2021, from https://www.digitale-technolo-gien.de/DT/Redaktion/DE/Downloads/Publikation/Smart_Data_Positionspapier_BigData_Leitlinien.pdf?__blob=publicationFile&v=7
[31] Origin Protocol. (2018). ERC 725 Demonstration. YouTube. Retrieved August 31, 2021, from https://www.youtube.com/watch?v=jjUKWRK8H2g&feature=youtu.be

Autradix – Self-optimizing, Decentralized, Non-custodial Trading DeFi Protocol

Steffen Kux
autradix.io, Chemnitzer Straße 49e, 09648 Mittweida

*Cryptocurrencies are characterized by high volatility, both in the short and long term. Experienced traders exploit this to make profits from price fluctuations by swing trading. However, this requires closely observing and analyzing the prices and trading positions at the right time. Only a few specialists, who spend time focusing on this, or optimized trading bots are able to actually make continuously profits. The **autradix protocol** is a self-optimizing and self-learning parametric trading algorithm that analyzes price actions in real-time and adaptively optimizes the algorithm's parameters to realize the user's investment objective. Embedded in an adaptive genetic algorithm, possible parameterizations are simulated and the optimal for the investigated trading pairs are calculated. The generic trading protocol API enables coupling with various crypto exchanges and decentralized protocols. A smart contract based decentralized, trustless, and tokenized fund, controlled by a DAO, enables users to invest, operate trading agents, and to participate in the profits generated according to their share.*

1. Introduction

The aim of the **autradix protocol and ecosystem** is to establish a decentralized and trustless DeFi protocol Instrumentalizing the chances of a very volatile market by implementing an automated and self-optimizing trading strategy, powered by adaptive parameter optimization and supported by artificial intelligence methods analyzing social media and other sources.

The autradix protocol opens these possibilities also for investors who have neither the necessary knowledge nor time to apply a good trading strategy. The target groups are smaller investors who also want to profit from the movements of the crypto market or want to stabilize the value of their asset collection as well as investors looking for a stable and automized trading bot.

1.1 Trading Objectives

There are two fundamentally different objectives for automated trading:

1. Trading to realize maximum gains (increase in value).
2. Trading to maintain the value of the investment despite price fluctuations (value preservation).

The autradix protocol can be configured and optimized for both approaches, allowing users to define their trading strategy and thus their chances of winning, but also the risk.

1.1.1 Increase in Value

If the goal is to achieve maximum profits, the attempt is made to take the best possible advantage of every price movement in order to increase the overall value of the portfolio. In particular, short-term price changes are of interest. Gains against the long-term trend can be realized as well. However, this focus on short-term gains also entails a significantly higher risk, since the relatively small short-term price fluctuations also quickly entail the risk of realizing negative trades. This is additionally limited by the fees since a trade can only be successful if it realizes more than the required fees.

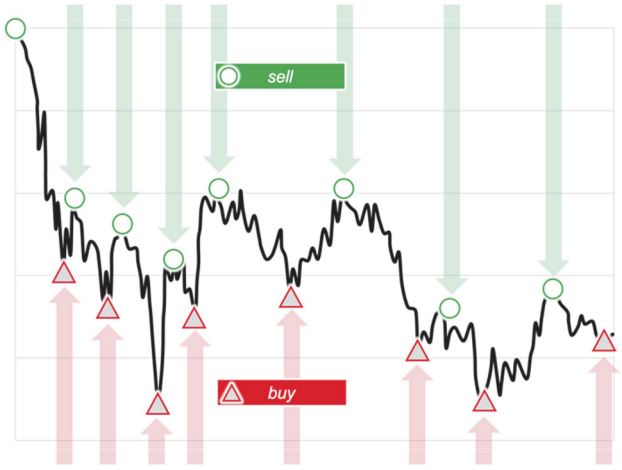

Figure 1: Short-term trading (principle)

1.1.2 Value Preservation

In contrast, the focus of value preservation is not on short-term fluctuations, but on compensating for long-term negative price changes and the associated loss in value of the portfolio by rebalancing the weighting of the assets in the portfolio in such a way that the value of the portfolio has a higher overall value compared with the original composition (simple "hodl"). The aim of this strategy is to achieve the most stable value within the specified portfolio limits. The risk of the strategy is lower than with short-term trading.

However, there is still the risk that the adjusted portfolio is less favorable and thus loses more value than the original one. Likewise, price fluctuations with very strong gradients may not be recognized in time, which can lead

to the fact that such price jumps or price falls cannot be reacted to in time.

Especially in this approach, the support of appropriate artificial intelligence methods can be very useful to combine the investment strategy and the need for fast action.

Figure 2: Long-term trading (principle)

2 Trading Model

2.1 Overview

Price developments of shares and cryptocurrencies in particular are characterized by a stochastic pattern. Therefore, future developments cannot be predicted from past data. Market influences, the illogical behavior of market participants (fear of missing out behavior or panic selling), the link to local and global events (catastrophes, wars, crises, economic and social events), the impact of influencers (e.g., when an influencer sends a positive or negative tweet about a cryptocurrency), and last but not least the very different expectations and forecasts can have quite unpredictable effects.

On the other hand, the impact of regulatory efforts (promotion or hindrance of market activities, regulation of mining or other crypto activities, or restrictions of DeFi activities, ...) but also the occurrence of common trading strategies (such as triggering stop-losses or other trading triggers) can also influence at least the probability of a certain market behavior within certain limits.

2.2 Mathematical Model

Many automated trading strategies are based on applying mostly heuristic methods of price analysis or AI approaches and giving the trading bot an advantage due to its 24/7/365 availability and quick response capabilities. The basic algorithm of autradix is a purely mathematical approach that derives trigger events for trading currency pairs from the analysis of real-time data.

2.2.1 Numerical Curve Analysis

For this purpose, the data of the price are suitably smoothed. The price data $[t_i, y_i]$ are obtained as pairs of discrete values of the time t_i and the price at this time y_i with an average sampling rate of 1 second from a price oracle. This can be the price information of a custodial exchange on which trading is to take place or a decentralized price oracle.

The data is mathematically smoothed so that the resulting curve can then be further processed. The smoothed value $\hat{y}_i$ at index i with the length l for the smoothing interval is calculated by a weighted averaging using the weighting function $\omega_i(k)$

$$\hat{y}_i = \sum_{k=i-l}^{i} \omega_i^o(k) y_i \quad with \quad \sum_k \omega_i^o(k) = 1.$$

For an assumed simple weighting function

$$\omega_i^o(k) = \begin{cases} \frac{1}{l} & i-l \le k \le i \\ 0 & else \end{cases}$$

the smoothing function is

$$\hat{y}_i = \frac{1}{l} \sum_{k=i-l}^{i} y_i \ .$$

The length l of the smoothing interval determines whether the long-term or short-term behavior of the price trend is more interesting. A more risky but maximum performance-oriented strategy will tend to work with a short smoothing interval (e.g., of a few seconds or minutes) while a strategy to hedge against loss of value will work with much longer intervals, since here the longer-term trend and less the short-term fluctuations are of interest.

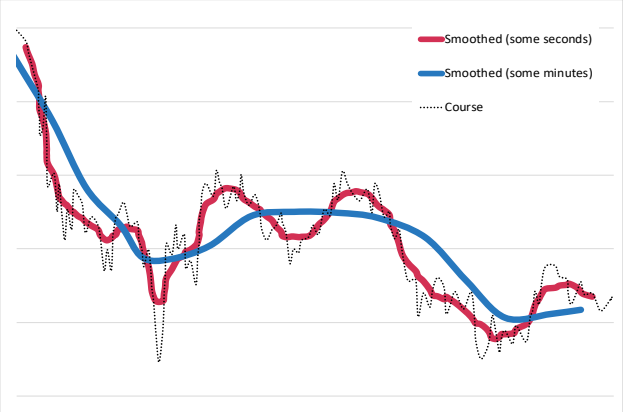

Figure 3: Price curve and different smoothing intervals

Short smoothing intervals lead to smoothed functions following fast the course of the stochastic course, while long intervals representing the long-term trend of the course, react however accordingly sluggishly to short term changes. With the weighting function the characteristic of the smoothing can be tuned. With suitable weighting functions (other than the simple approach

above), it can thus be achieved that movements at current time are better recognized even with longer smoothing intervals.

An indicator that a potential local maximum or minimum of the price has passed is a minimum or maximum on the smoothed price curve. For this purpose, the smoothed curve is derived numerically. The difference quotient is calculated for all positions of the smoothed curve. Except at the edges of the curve, the central difference quotient is used

$$\dot{y}_i = \frac{\Delta \hat{y}}{\Delta t} = \frac{\hat{y}_{i+1} + \hat{y}_{i-1}}{t_{i+1} - t_{i-1}}$$

This is possible because the smoothed curve is sufficiently smooth and at least once differentiable. For the decision whether it is a minimum or a maximum, the second derivation is needed also. To make this numerical stable, the curve of the first derivative is smoothed again appropriately

$$\hat{\dot{y}}_i = \sum_{k=i-l}^{i} \omega_i^1(k)\dot{y}_i \quad with \sum_k \omega_i^1(k) = 1 \ .$$

Then the second derivation is calculated by once again calculating the difference quotient, now from the smoothed derivation curve

$$\ddot{y}_i = \frac{\Delta \hat{\dot{y}}}{\Delta t} = \frac{\hat{\dot{y}}_{i+1} + \hat{\dot{y}}_{i-1}}{t_{i+1} - t_{i-1}} \ .$$

A potential high point at i_{sell} which signifies a selling signal, is present when applies

$$\dot{y}_{i_{sell}} = 0$$
$$\ddot{y}_{i_{sell}} < 0$$

and a potential low point at i_{buy} signalling a buy chance is expected at

$$\dot{y}_{i_{buy}} = 0$$
$$\ddot{y}_{i_{buy}} > 0$$

The curve is always analyzed backwards from its most current position, since only the last local extreme points are relevant for a potential decision.

2.2.2 Thresholds

The identification of an extreme point is only a trigger for a potential trading chance. An event must not be triggered immediately, as this would lead to many wrong decisions due to the partly strong stochastic price fluctuations, since a valid trading signal requires a trend that allows a value gain to be achieved through a suitable trade.

For this reason, thresholds θ_{buy} and θ_{sell} are defined that must then be exceeded or undershot in the predicted direction to trigger an actual event. These threshold values must not be too large, as this would lead to a trading event being triggered very late (and perhaps too late) in a trend progression. If the threshold value is too small, it may happen that short-term stochastic fluctuations already trigger an event, which may lead to a trading action that moves against the trend and thus realizes losses.

The determination of appropriate thresholds depends strongly on the characteristics of the price trend (e.g., how strong the usual stochastic fluctuations are) and also on the trading strategy. Optimal values differ for different currency pairs and do not remain the same for the same pair over time.

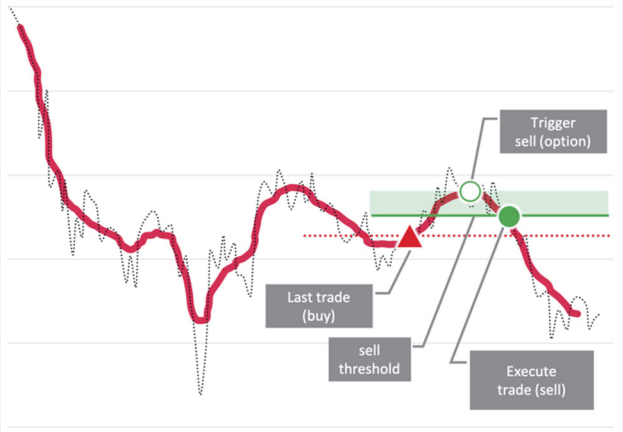

Figure 4: Trading mechanism (trigger, threshold, trade)

2.2.3 Impact Analysis

Furthermore, a portfolio impact analysis is performed before a trading event is triggered. This means that it is analyzed whether the trade actually has a positive impact on the total value of the portfolio or would cause a negative performance due to the local development. Also trading to another token may be more promising.

The impact analysis must be weakened over time, because otherwise the trading could be completely prevented if the price trend runs in the wrong direction and no positive trade is possible anymore (e.g., a purchase was made and before a sale could be triggered, the price turned and has fallen since then, so that the short-term fluctuations could be used, but no sale is possible due to the negative impact). Then a negative trade may be necessary to get back into business.

The impact analysis has also parameters I_{buy} and I_{sell} to control its behavior.

2.3 Parametric Model

The model described has a number of parameters that can be used to adapt the model to the requirements. All relevant parameters that determine the characteristics of the model can be controlled externally and are available as optimization variables.

In section 2.2, parameters for the mathematical model are already introduced:

- l ... length of the smoothing interval
- l_{der} ... length of the smoothing interval of the first derivation

- ϕ ... form parameter of the weight function for the smoothing algorithm (not described in this paper)
- θ_{buy} ... threshold to trigger a potential trade
- θ_{sell} ... threshold to trigger a potential trade
- r_{trade} ... maximum relative amount of an asset that may be used for a trade
- I_{buy} ... Impact analysis form factor (not further described in this paper)
- I_{sell} ... Impact analysis form factor

Other parameters (like additional chart analysis criteria) are not described here and may be introduced later.

2.4 Investment and Portfolio Strategy

When putting together a balanced portfolio, care should be taken to ensure that the assets that belong to it have appropriate weightings. When trading takes place, this weighting will be shifted. If everything is allowed, each token can be swapped partly or completely into other tokens without restrictions.

Since the selection of trading opportunities is done by the algorithm based on mathematical indicators, it does not take into account the risk attached to these tokens and so on. If the composition of the portfolio is to be actively influenced, it is possible to specify how large the minimum and maximum share of a token may be.

Based on these specifications, the trading algorithm can optimize its strategy to meet the portfolio composition and take these constraints into account when triggering a trading event.

2.5 Adaptive Parameter Optimization

With the parametric model, it is now possible to formulate a mathematical optimization task[1] to determine the optimal parameter configurations. The aim is to tune the model so that the best possible decisions can be made with this model for a currency pair or some combined currency pairs.

2.5.1 Objective function

Assume that there are potentially j assets α_j in the portfolio and each asset α_j has a value $\psi(\alpha_j) \geq 0$. The total value of the portfolio is

$$\Psi = \sum_j \psi(\alpha_j)$$

For the calculation of the potential asset value, starting from an initial value, trades are simulated on real data from the past to the present. The simulation interval Δt must be large enough that sufficient potential trades can be executed, but should also not be too large in order to keep the computational effort as low as possible, and also to be able to react to changes in the characteristics of the price trend.

The objective is to maximize the total value Ψ of the assets under the given constraints, simulated in the interval $[t_{now-\Delta t}, t_{now}]$:

$$\Psi_{[t_{now-\Delta t}, t_{now}]} \rightarrow max$$

Although the behavior of each currency pair can be viewed as independent by itself with respect to the behavior of other pairs with the value function $\psi(\alpha_j)$, these are not intependend if the portfolio strategy is considered as well as it is done in the portfolio value function Ψ. This means that the parameters for all currency pairs need to be optimized together to find the optimal parameter configuration for the whole portfolio.

2.5.2 Optimization variables

The already described parameters of the model and, if necessary, additional variables from chart analysis methods are used as optimization variables. Each variable is constrained by a suitable interval.

These parameters must be set for each currency pair.

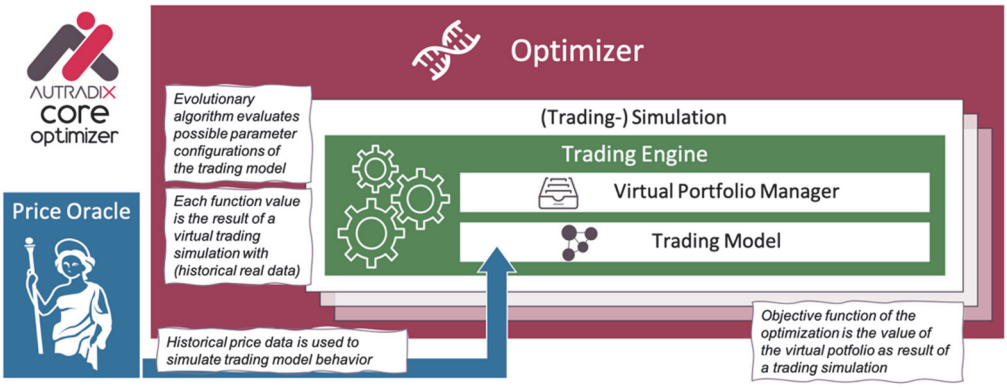

Figure 5: Optimization principle to find optimal parameter configuration for trading model

[1] see figure 5

2.5.3 Constraints

The specifications of the portfolio composition are formulated as constraints. This means that the ratio of the individual cryptocurrencies can already be taken into account when optimizing the parameters.

2.5.4 Optimization Algorithms

The optimization task is a highly dimensional, nonlinear blackbox problem.

The function value $\Psi_{[t_{now-\triangle t}, t_{now}]}$ is the result of a number of numerical simulations based on real price trends from the past.

No statement can be made about continuity and differentiability. Gradient information is not available. These could be calculated by numerical differentiation, but this would be very computationally expensive due to the many optimization variables. Furthermore, no information regarding the smoothness of the function can be predicted. In particular, discontinuities and jump points cannot be excluded.

The optimization method must therefore be an algorithm that does not require gradient information, works globally, and can also cope with non-continuous objective functions and constraints.

Genetic/Evolutionary Algorithms

Genetic or evolutionary algorithms are nature-inspired optimization methods[2] that apply the laws of heredity (e.g., Mendel's laws) to mathematical problems. Through repeated operations such as

- crossover (exchange of properties) and
- mutation (random changes),
- selection (sorting out good and bad solutions)

these methods tend to convert towards the optimum.

In addition, these algorithms do not impose any requirements on the smoothness, continuity, and differentiability of the objective functions and constraints, and no gradient information is needed. Thus, they are well suited for the described optimization problem. The fact that these algorithms require relatively many function evaluations for the optimization is not a serious problem, since the optimization does not have to be performed in real time.

2.6 Artificial Intelligence Support

Secondary information can give very good indications of whether a trading event is imminent or in which direction a price trend is highly likely to move. This information can come, for example, from social media, relevant forums, and communication platforms. Very different information could be considered.

2.6.1 Influencer

Influencers are people who have a significant impression on other people due to their strong presence in social media or their high visibility due to their celebrity. Beyond this flow of information, influencers can have a very strong impact on the decisions of their followers. Statements made by such people quickly go viral and are spread very quickly through their network of followers.

For example, Elon Musk has significantly moved the price of cryptocurrencies like Doge and Bitcoin up or down with a few tweets. Analogous actions are also not unknown from stock market trading. So, a statement on the interest rate level of the European Central Bank by the head of the Central Bank can have an influence on buying or selling decisions of bonds.

The AI model is trained to filter and recognize those messages from the flood of social media postings that come from key influencers and have the potential to go viral and drive others to more or less predictable trading behavior.

However, if a potential influencing event is detected by the AI, this is not immediately acted upon (i.e., immediately translated into a trade), but this information is used to tune the parametric trading model so that it will react faster and more actively to a resulting price change.

This is done, for example, by changing the parameters of the smoothed curve l and ϕ and the limit values θ_{buy} or θ_{sell} in order to be able to react more quickly to an imminent price rise or fall. The trading ratios r_{trade} can be adjusted, too, to optimize the volume in order to achieve a higher profit.

Especially the impact analysis needs to be tuned if predictable behavior is expected to prepare the algorithm to be ready to act.

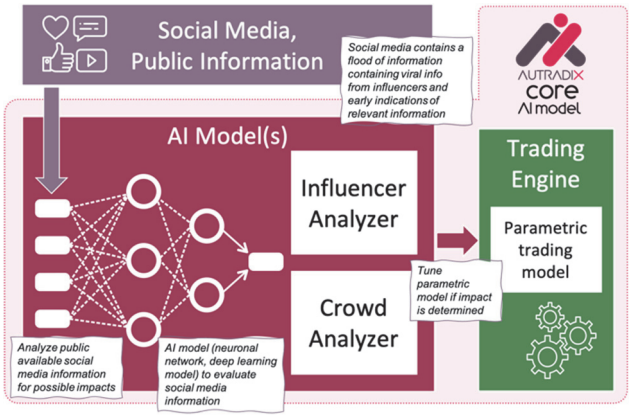

Figure 6: AI models to evaluate social media information

[2] for more information, see [1]

2.6.2 Crowd behavior

Social media and relevant discussion forums can provide even more helpful information. For example, if many people discuss that a cryptocurrency (or the project behind it) has run into difficulties (e.g., due to a software hack), the expectation can also be derived from this that a price drop is to be expected with a certain probability. Conversely, positive news (such as the achievement of a financing round or the release of a new version) are also indicators of a possible price increase.

Of course, this information is no guarantee for such a price movement, because often the market does not act logically, but can be an important indication that such a movement is being expected.

The AI model used for this purpose is trained to recognize that positive or negative information related to a cryptocurrency is accumulating. Similar to influencer analysis, these trigger signals are used to adapt the parametric model so that it can react more effectively to such behavior.

3 Technology

3.1 Generic Trading Interface (GTI)

The trading strategy of the autradix algorithm is by itself completely independent of the underlying trading platform. This means that centralized exchanges such as Crypto.com, Coinbase, Kraken, Binance, etc. can be used, as well as decentralized exchanges such as Uniswap and others.

Many of the centralized exchanges provide APIs for managing accounts and executing trades. The autradix protocol embeds these APIs in a generic interface so that users can choose self-determined which exchanges they want to use. The generic interface also allows decentralized exchanges to be integrated in the same way. In this way, it is possible to integrate and use the whole variety of crypto ecosystems according to the requirements and wishes of the users.

The generic trading interface (GTI) provides the following functions:

- Query of price information on the selected currency pairs.
- Manage the wallet/account.
- Set and stop trades.

3.1.1 Centralized Exchange APIs

Centralized marketplaces allow their users to trade coins and tokens. In addition to spot trading, leveraged products are often offered (margin trading). Even though the autradix protocol is very generic, leveraged trading is currently not supported.

In addition to direct buying and selling at the current market price, exchanges offer more complex trading rules such as limits, stop loss, stop limit, ... These are also not supported at present.

The fee model for bid/ask trades of central exchanges is mostly volume dependent. For each trade a fee is charged, which depends on the value of the transaction. This means that a small transaction will cost less than a large one. For the autradix protocol results that a transaction is only profitable if the relative profit is higher than the relative fees.

For trading, relative profit must always be maximized on centralized exchanges, not the absolute profit. On the other hand, it is possible to trade small volumes without incurring excessive fees, as long as the relative profit is sufficient.

Since the trade is only one transaction in the exchange's system database and does not require any transaction

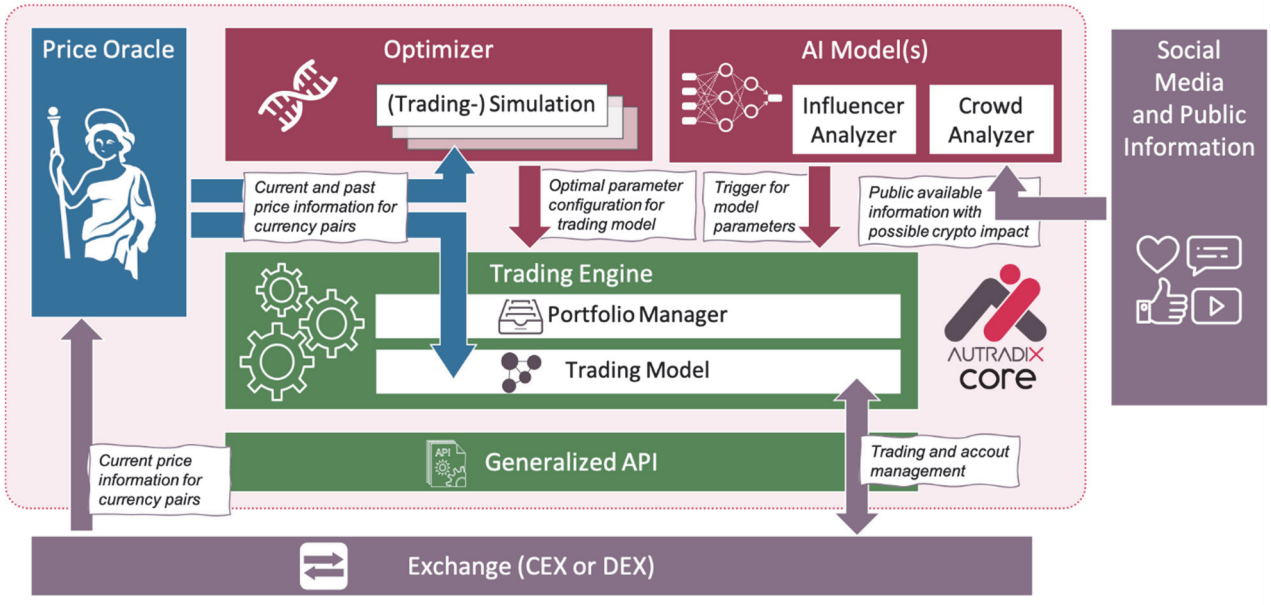

Figure 7: autradix core components

on the blockchain, the execution time is usually very short. That is, the transaction is final almost in real time.

The tradable volume and the resulting price depend heavily on the liquidity and the available supply or demand of the exchange.

3.1.2 Decentralized Exchange APIs

In decentralized exchanges, a trade means a transaction on the blockchain. The fee which is the blockchain's transaction fee is independent of the volume of the transaction. Instead, it depends on the current gas price and how much gas is required for the interaction with the smart contract of the exchange.

If the usable gas for the transaction is set too low, it is possible that the transaction of the trade will take a very long time to be executed or even will not be executed at all. The offered gas has to be high enough to ensure that the transaction is executed quickly. This is necessary to reduce the risk that the price has changed too much between triggering the trade event and the actual trade which could lead to a negative trade if the price moves into the wrong direction in between.

Compared to trades at a central exchange, DEX transactions take significantly longer to become final, as the same rules apply as for any other transaction on the blockchain.

The fees for such a transaction are independent of the volume which means that even large transactions do not incur higher fees. Conversely, however, this also means that high transaction costs can be incurred for small volumes, which makes this transaction less effective or even negative.

When trading on DEX, it is therefore not the relative profit but the absolute profit of the transaction that is relevant for executing a successful trade.

As many DeFi products are currently working on processing transactions in Layer 2 (e.g., rollups), this will also bring essential advantages for this application, as it will drastically reduce transaction costs.

However, this also cannot be scaled arbitrarily. With increasing volume and depending on the liquidity of the pool of the currency pair, a trade has increasing influence on the price. This means that a potential sale of a large volume can cause the price to drop. The same is true in the other direction as well.

For that reason, the autradix protocol is considering this as well when a trade is going to be created.

3.2 Price Oracle Service

For the simulation described above which is among others the basis for the calculation of the objective function value of the optimization task, historical price trends of the currency pairs under consideration are required.

Both centralized and decentralized exchanges offer APIs or oracles to read price data. Depending on the API, access to historical data may also be possible to a certain extent. Depending on the simulation used, more extensive data sets are required than can't be retrieved directly from the APIs.

The autradix Price Oracle Service provides a service that uses the APIs to one or more exchanges to retrieve price data at the required sampling rate and stores it in its own database, and then in turn provides a REST API through which this data can be retrieved from the autradix protocol.

For a system to be tamper-proof, it must be ensured that this data is correct and available. This can be done by a trusted node or better by a decentralized trustless network of oracle providers.

3.3 Solutions

The autradix core software, consists of

- The price oracle which collects price data and provide historic data for the simulation,
- The trading engine with the parametric trading model and the portfolio manager,
- The optimizer for the trading model parameters,
- The simulation engine to simulate trading with historic data,
- The AI model to analyze and evaluate social media and other information to tune the mathematical model, and
- The interface to the exchanges.

The goal of the software architecture is to enable a system that can meet the different requirements of the users in terms of convenience, self-sovereignty and compliance.

In figure 7 is visualized, how these core components work together and interact with exchanges and information sources.

3.3.1 Software-as-a-Service

Many applications are offered to the user as software-as-a-service (SaaS). The actual software service is hosted on a server (see figure 8). Users can then create an account and use the service offered within this framework.

In terms of user-friendliness, this is very simple. The software, which is offered as a web application or mobile or desktop app, is accessed via the user's account which is defined and secured by user name and password and, if appropriate, 2FA for greater security.

The backend is operated by the service provider, without the end user coming into contact with it, except through configuration via the application interface, if that is required.

This software application is operated as a central cloud service. The end user must trust the operator – regarding the running software components, the IT infrastructure, and the account and key management to access the service. The service provider may also charge a fee (e.g., share of profits, setup fee, ...).

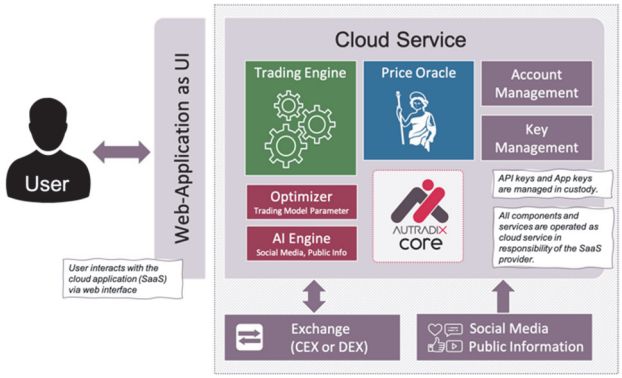

Figure 8: SaaS Architecture

The user has no influence on which software version is used or which exchanges are connected and does not have to worry about it and the operation of the IT infrastructure. If the assets are managed on a central exchange, the user remains in full control of them (or correctly, the exchange which acts as custodian for the user), as the autradix SaaS service can only trade via an API key and this key can be restricted in terms of permissions (only read and manage trades, but no withdrawals or transfers not approved for trading).

As far as self-sovereignty is concerned, since the assets are held in custody at the exchange, the user retains control and the autradix service cannot access the assets directly.

The situation is somewhat different for decentralized exchanges. The assets are held in a wallet in which the user has full control over the private keys. Transactions are signed with these key(s). In order for a central service in the form of a SaaS to trade on a DEX, the service needs access to these keys to sign the required transactions.

This means that the end user must make the private key(s) available to the autradix service. The service would then have full control over the assets and thus the service would have to be trusted to handle the key correctly and not misappropriate the assets.

This problem is solved by using a smart contract multisig wallet with special app keys which have restricted permissions only. The multisig wallet has keys that only the owner can control and with which all transactions can be executed.

Furthermore, the wallet has a special application key that can only execute transactions that are required to execute trades on the corresponding DEX, although the recipient of the returned tokens must be the wallet itself. This application key can then be made available to the service and it can be used for trading activities without gaining control over the assets beyond the granted permissions.

From a compliance[3] point of view, it will be necessary for the users who have an account with the service (centralized exchange) to go through an appropriate KYC process. As the autradix service has no control over the assets at any time, no additional compliance actions are needed.

If a DEX is used and the user gives the autradix service only an app key with limited rights, the control remains with the user and no additional KYC is required.

3.3.2 Local Node

Truly self-sovereign operation of the autradix system is possible by the users running their own autradix node. The backend software is largely the same as in the SaaS approach, but there is no central service operator of the platform. Instead, the user runs the service locally on a node. This node is configured to connect to the user's trading venues and trades there with the user's accounts (central exchanges) or the user's wallet (decentralized exchanges)[4].

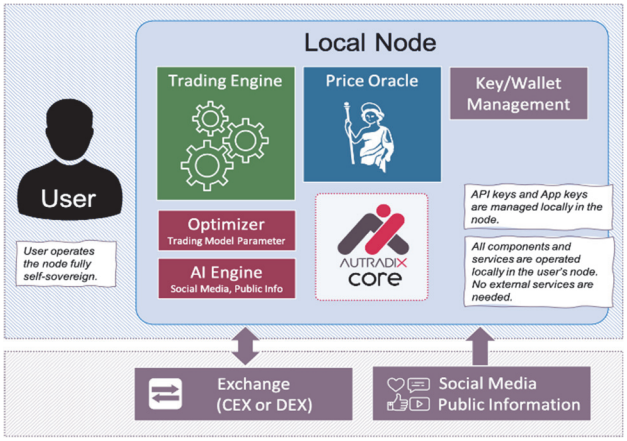

Figure 9: Local Node Architecture

Since the node is in full control of the user, he/she is always in full control of his/her assets[5]. For security reasons, API keys should nevertheless be limited in permissions to what is necessary to trade. Similarly, for use with DEX, it makes sense that the wallet is also implemented as a multisig wallet with app keys restricted to perform only the needed trading transaction to grant the trading algorithm only the minimum necessary rights.

Compliance requires no restrictions. The provisions for any central exchange and non-custodial wallets used apply. Beyond that, there are no further restrictions, as the

[3] Compliance requirements still need to be evaluated in detail

[4] see figure 9

[5] With the restrictions on central exchanges

entire system is always in full control and operation of the user without any custodian services.

3.3.2.1 System Requirements

The following components run on an autradix node:

1. Price oracle (or a remote oracle is used for this).
2. Trading engine
3. Parameter optimizer (including trading simulators for each traded currency pair)
4. AI engine
5. Wallet / Account manager

In terms of memory requirements, the database of the price oracle and the database of the trading engine require the most space. Also, the AI models require some space. Depending on the number of actively used currency pairs and how far into the past the data is kept (as needed for the simulation), memory is required. However, data for one day and one currency pair requires only a few MB. The trained AI models may require some hundred MB.

Fast SSDs are advantageous to speed up read performance and shorten the simulation time. Alternatively, in-memory databases are well feasible at this size and advantageous for performance reasons.

The parameter optimizers are by far the most computationally intensive components, since these adaptively calculate the optimal parameterization of the trading algorithm and must calculate some hundred or thousand simulations for each objective function value.

Since this optimization does not have to be performed in real time, it does not require very high computing power. A multi-core environment is beneficial, since the function evaluations can be parallelized well.

In order to operate a node effectively, it must have a permanent internet connection to retrieve information (price oracle, account information) and execute trades.

The aim is to optimize the software for use on a single-board computer (e.g., Raspberry Pi 4) or other small computers in order to be able to implement cost-effective nodes.

Also, the implementation as module for the DAppNode[6] is a possible approach. Then the user can operate his autradix node as subtask at this node.

Alternatively, an autradix node can be set up on a cloud server. In contrast to an own hardware node, it is very easy to secure a 24/7 operation and performance requirements are easily met even with small configuration packages.

3.3.3 DeFi Fund

Another way to make the autradix system accessible and thus usable to users is a decentralized fund into which users can invest and then participate in the gains of the fund according to their shares.

In contrast to the approaches described as centralized service or as decentralized independent node, in which in both cases only the user's assets are managed and traded, this approach manages a portfolio that contains and controls the assets of all users.

In figure 10 the architecture of the decentralized DeFi fund is visualized.

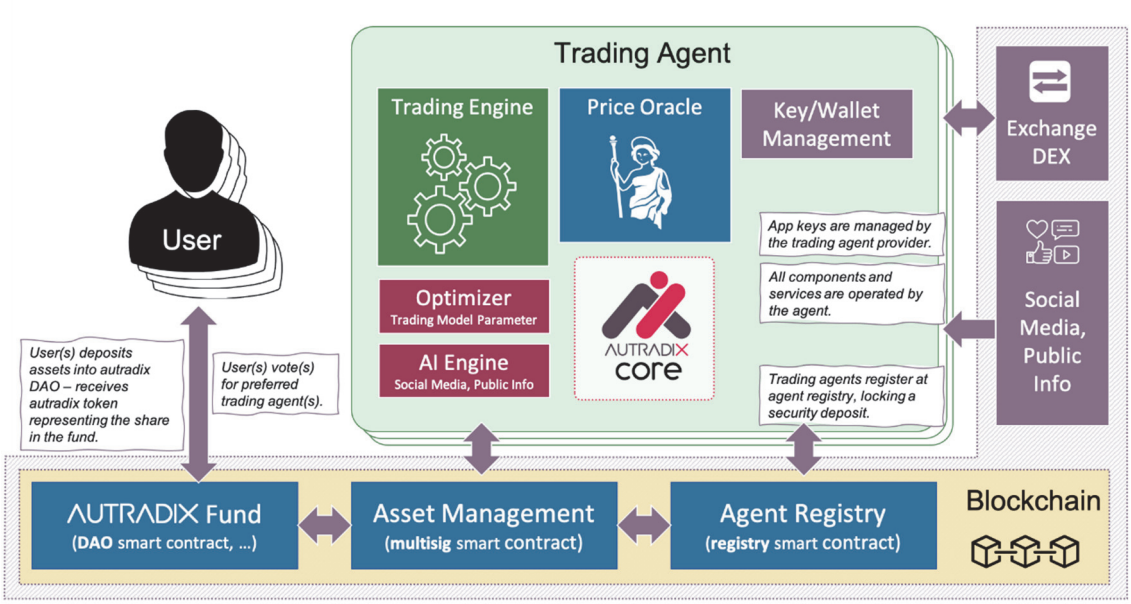

Figure 10: Decentralized Fund Architecture

[6] see https://dappnode.io/

3.3.3.1 Asset Management

The assets are managed in a smart contract. Users deposit their assets in the smart contract and release them for trading. Upon deposit, the user's share in the value of the overall portfolio is determined and allocated to the user in the form of tokenized shares (share tokens are mined upon deposit).

If a user wishes to withdraw his share of the portfolio, the share tokens are burned and the equivalent value of the share is transferred back to the user.

A suitable oracle must be used to determine the total value of the portfolio, as other ERC20 tokens are also part of the portfolio in addition to Ether and their value cannot otherwise be determined on-chain.

Suitable waiting periods until the deposited assets are traded or until withdrawn assets can be released must be defined and transparently disclosed so that oracle manipulations, attacks such as frontrunning, etc. can be prevented.

3.3.3.2 Trading

Only decentralized exchanges can be used for trading the assets from the fund, since otherwise an account would have to be used for trading on a centralized exchange, in which the assets are held in custody. However, since the entire protocol is to be designed as trustless as possible, this will not be an option.

The assets are managed in a multisig with special app keys, which only allows the trading agents the necessary permissions to swap the assets, but not to withdraw or perform other transfers.

3.3.3.3 Ecosystem and Incentives

The autradix fund ecosystem recognizes the following roles:

Investors – these are the users who pay assets into the fund in order to achieve a good return.

Shareholders – by investing in the fund, the users get voting rights to participate in the strategic decisions of the DAO, especially the selection of trading agents.

Trading agents – these are the operators of the trading bots who want to get a good return for providing the IT service to the fund.

The entire system operates in a fully decentralized manner and does not require any central instance, operator, or coordinator. The system is also trustless[7] which means that individual users (regardless of their role) do not have to trust other users.

Each role has an economic incentive to behave honest and according to the rules of the ecosystem. Fraud or misbehavior is already prevented at the protocol level or it is strongly motivated by crypto-economic incentives to behave correctly, since otherwise it would lose its security deposit or not receive revenue, for example.

3.3.3.4 Trading Agents

A trading agent is an off-chain software that can manage and trade assets similar to a SaaS bot or local node. A centralized service could be implemented for this, but would in turn make the whole system no longer trustless, not to mention that the operation of such a custodian trader is complicated from a compliance point of view (requires appropriate regulation for crypto trusteeship) and would be a single point of failure as well. The approach also works fully decentralized and trustless through algorithmic and crypto-economic protection.

The decentralized system allows trading agents to register on the platform at the agent registry. For security, a deposit must be made, which will be slashed if the agent can be proven to be acting maliciously. A newly registered agent cannot trade for the time being, but must first be elected by the token holders. This is done at regular intervals (epochs).

Elected traders will then receive an asset volume to work with. This volume must be large enough to realize meaningful trades, but still small enough for multiple trading agents to work with.

Each agent can specify how high his maximum trading volume should be and it will be allocated the actual volume depending on its reputation in the election process. As an incentive for operating an agent, the agent receives a percentage of the profits it generates as tokens.

3.3.3.5 Autradix DAO

The investors which have contributed assets to the fund will receive tokens according to their share of the fund balance, which at the same time gives them the corresponding voting weight in decisions, for instance

- Selection and volume approval of trading agents,
- Blocking or exclusion of malicious trading agents, etc.
- Fund strategy

3.3.3.6 Autradix Token

The autradix token is a central element of the DeFi fund. It has the following tasks and properties:

- Fungible token, following the ERC20 or ERC777 standard.
- It represents the countervalue of the assets managed in the DeFi fund. The number of issued tokens always correlates to the value of the fund.

[7] Trust is established by the software protocol only

- It can be redeemed at any time for the corresponding share of the deposit.
- It gives voting rights in decisions of the DAO.
- All payments (e.g., compensation of trading agents) are made in the token.
- A community or development fund can be realized as a percentage of the epoch profit, too. This fund can be used to finance future developments at the decision and permission of the DAO.
- The token is stable to the value of the portfolio. It can be traded on exchanges, but will always have the equivalent value of the share of the fund portfolio. This stability can be hedged algorithmically.
- The token does not represent a share of a company or organization, but it is a utility and governance token that is used exclusively to operate the autradix fund. A legal classification has yet to be made.

3.3.3.7 Compliance and Regulation

The autradix DeFi fund is decentralized and is not operated by a service provider. It is a smart contract running on the public Ethereum blockchain. The investors (users who deposit assets into the smart contract) receive tokens in exchange for their deposit, representing the value of their share in the total fund. The trading agents or other users do not have full control over the assets at any time. The portfolio is managed in a smart contract without a trustee. All relevant decisions are made and approved by the token holders in the form of a DAO.

Even though the token is designed as a utility and governance token, it still represents a store of value with profit expectation. Therefore, it is necessary to examine to what extent it might be subject to trading restrictions.

Necessary regulatory obligations are from a current point of view not different from other already existing DeFi solutions. However, a detailed legal examination is still necessary.

4 Summary and Outlook

With autradix, a trading protocol is presented that makes it possible to automate trading with volatile cryptocurrencies on the basis of an adaptive self-optimizing model and make it accessible to a larger group of users. An adaptive evolutionary optimization algorithm is used to set the parameters and thus the properties of the trading model to best match the user's goals.

With the targeted use of tuned AI models, it is possible to support the mathematical models and to react triggered to predictable events. Information from social media and other public information sources is evaluated and used to identify possible events with an impact on the crypto market in order to adjust the trading strategy accordingly.

With a generalized API, the protocol is not bound to a specific exchange or decentralized protocol, but can be ported and optimized to the trading platforms the user needs.

The protocol can be realized as a cloud service, as a fully self-sovereign node under the user's own responsibility, but also as a decentralized, trustless, and tokenized DeFi protocol. This makes trading as easy as simply buying a token. Investors and operators of trading agents thus come together and can share in the profits without the need for an intermediary, trustee, or coordinator and without having to trust the other participants in the ecosystem.

4.1 Prototypes and possible Roadmap

The parametric model is the basis of the autradix protocol. In PoC-1 the trading model, the price oracle service and the generic interface is implemented.

Based on this, the optimizer with the trading simulators is realized in PoC-2.

With the generic interface and the implementation for one or more exchanges PoC-3 can be achieved.

The continuation of this prototype allows the Local Node to be realized and used practically (release 1). Building on this, the cloud service can be developed (release 2).

In parallel or as the next development step, the decentralized DeFi fund can be implemented in release 3.

References

[1] S. Kux: Hybride Optimierungsstrategien für komplexe technische Aufgabenstellungen. University of Applied Sciences Mittweida, Master Thesis, Mittweida, 2011.

Design disclosure for Blockchain-based Application used in public education certificates with electronic hashes

Arno Pfefferling, Patrick Kehling
Hochschule Mittweida, Technikumplatz 17, 09648 Mittweida

Abstract: Blockchain Technology has become an innovative, mature tool for digital transformation, disrupting more and more application areas in their business processes, values, or even economic models. This paper leverages more than 30 academic publications on prototypes and their Blockchain-based use cases to transact certificates in the context of public education. The conceptual design and guiding ideas are reflected in the practical application development for the Federal Ministry of Education and Research ECHT! project within the showcase region WIR! in Mittweida and are used for the research design. During this approach we applied agile methods and the current certificate process to propose a comprehensive disclosure of a new software prototype including a three-layered architecture with multi-stakeholder components. The artefact instantiation contributes to the practical knowledge base within Information System Research and specifically in digital certificate processes starting from creation, searching, and proofing up to revoking by consideration of an existing IT landscape as well as organizational hierarchy.

1. Introduction

The last months and the following years are under tremendous changes worldwide due to the forced use of new digital tools in organizations or in remote home-offices up to fully virtual institutions. This digitalization can go hand in hand with adaption of disruptive technology to stimulate culture of innovation [1]. Gurhaxani and Dunkle propose the following dimensions: risk-taking, diverse perspectives, failure to be learned from and rewards for innovators by removed cultural resistance. The ECHT! project grasp to manifest these dimensions by designing a prototype for digital certificates created inside the University of Applied Sciences Mittweida (HSMW).

Blockchain Technology (BT) in its core offers and is demonstrating those values. Especially the application field data management is a realistic use-case far from hype [2]. Furthermore, academic literature has shown that through BT innovation is accelerated, just to cite a highlight “we have the chance to experiment with secure, decentralized systems, which could enable new social models that go well beyond the economy.” [3]. According to Beck and Müller-Bloch the innovation process fades boundaries by BT with discovery / conceptualization phase, incubation / experimentation loop and acceleration / commercialization stage [4]. For the WIR! showcase region Mittweida the statement we see describing us as best: “initiatives already moved beyond discovery, are fully immersed in incubation”. The main consequence is that with such decentralized approaches a complex way of managing and processing within governance becomes a critical success factor, so that we consider selected questions raised by [5]:

How is accountability determined and how is identity engrained in Blockchain economy?

How are disputed transactions resolved and how is then trust affected in the Blockchain economy?

What is the role of institutions in this economy?

Our practical solutions by prototyping are additionally under the scope of usability to ensure market readiness and maximized business values for the ECHT! project partners as well as be a lead example for the whole WIR! showcase region Mittweida. To govern the complex development of our minimal viable product we adapt aspects from Zavolokina et al. specifically “activities concerned with designing the system itself and identifying its business value for consortium members” [6] by permissioned BT to tackle governance tensions as trade-offs namely design openness versus competitiveness and hierarchical effectiveness versus democratic efficiency.

To consider the right decisions of the mentioned trade-offs we ultimately needed to evaluate BT impacts on a task level: “Routine tasks are explicit and codifiable. They include the calculations involved in bookkeeping; the retrieving, sorting, and storing of structured information in association with clerical work; and the precise execution of repetitive physical operations in a stable environment.” [7]. Whereby we define our use case of Certificates created in public education. The next crucial topic we considered is the General Data Protection Regulation (GDPR) in Europe. Rieger et al. proposed three potential approaches: “central authority, pseudonymization and shared responsibility.” [8]. Furthermore, current problems of centralized regulatory are found in data lineage “caused by data aggregations that occur at increasing distances from the source continue to grow.” [9]. Regulatory is helping us furthermore to understand consumer views of information privacy and future research in position to GDPR [10].

The cited chances and already demonstrated success in academic publications with BT make us strongly agree on what Altketbi et al. wrote: "huge potential in the use of Blockchain for government services since it can deliver government services in a cheaper, distributed and voluntary way." [11]. For our practical instantiation we supplementary tackle the recent question: "How to increase interoperability of existing information systems?" [12] and see this as central technical development research gap.

To answer this motivated situation this paper builds first the Fundamentals of BT and Trust. Followed by explaining the research approach using Literature review as foundation for agile prototyping. Final Insights of our prototype design represents the main findings and are rounded up in the last chapter as conclusion.

2. Fundamentals

For better understanding of the scope of Blockchain-based applications this section is structured in two parts first a more technical description and the second part with frameworks to describe social-economic relations.

2.1. Technology behind Blockchain

BT can be described as a distributed database build up by interconnected Transactions (Tx) that are protected by cryptographic private and public key mechanisms which can be seen as digital signatures. The distribution can be realized over a peer-to-peer network whereby participants act via nodes to ensure consensus about status of the data at a certain time. Nodes can have a full copy of the distributed database or depend on another node by lightweight blockchain data. Tx are put together in blocks (data packages) which uses protocol-specific fields and a defined block header. For most BT the hash of the previous block, a timestamp, the Merkle root and additional Tx data is stored for the whole network to create a chain where the consensus is built in. The Merkel root represents a single hash of the included Tx with consideration of order and single data status. In other words, the Merkle root is the last hash value of the Merkle tree constructed from hashes of up to thousand Tx. So called hash or hashing stands for mathematical one-way functions that transform input data to a defined alphanumeric string depending on a standardized algorithm. Important is that the same input always hashes to the same value [13].

Over time these basic technical mechanisms got developed in very different ways and directions to solve problems in new application areas so that up to now a very wide and heterogenous variety of BT is created. According to Sanka et. al the following features, benefits and importance of BT include distributed/decentralized nature, data integrity and security, anonymity, transparency and traceability, cost saving, increased speed, efficiency, interoperability, verifiability and right to be forgotten [14]. These factors strongly depend on the chosen Blockchain type (public, private, consortium/federated) as well as the used technology. Casino et al. define the following property for BT with consensus mechanism, identity anonymity, protocol efficiency and consumption, immutability, ownership, management and transaction approval [15]. To choose the right BT Labazova et. al proposed a configuration process model with the attributes 1) Governance 2) properties and 3) deployment depending on the application area [16]. In short researchers and practitioners evoked a wide space of Blockchain-based applications for mass adaption.

2.2. Frameworks for Trust and Governance

Besides the technical part we see the success of applications only if they are user-centric (UC). Specifically for BT Fleischmann et al. differentiates between functional and emotional benefits which are brought together of the emerging codes of security with trust and states "shifting the research discussion from a predominantly technology-oriented design angle to a UC perspective, present research reminds researchers and practitioners alike that for the acceptance and sustainable success of blockchain applications, it is critical to develop the underlying technology against the backdrop of UC needs, as it is those UCs that finally decide on the success or failure of any application" [17]. User in the public deal with lack of Trust and reputation or incomplete information where central trusted party such as an insurance company, a central bank, or the government are the problem solver [18]. The conclusion for us is that the BT is not a standalone solution instead it is designed to support the whole Certificate process in public education meaning our work contributes to the digital transformation of government starting by finishing a single module exam up to reaching the final degree at a university. Treiblmaier et al. mention for this transformation already BT for digital identity as the unique identity assigned to an individual under a particular digital identity scheme, typically a government-backed scheme [19]. We see BT as enabler for collaborative governance, which is stated as "the processes and structures of public policy decision making and management that engage people constructively across the boundaries of public agencies, levels of government, and/or the public, private and civic spheres in order to carry out a public purpose that could not otherwise be accomplished" [20]. If collaboration with Trust is enabled we expect that "Firms can gain many benefits from inter-firm cooperation, such as activities with a broader scale and scope, shared costs and risks, improved ability to deal with complexity, enhanced learning effects that lead to improved returns on research and development (R&D) investments, and enhanced flexibility and efficiencies and a shorter time to market" [21].

In Summery digital Certificates in public education play a major role for Trust and Security in Governments. Requirements for public sector are generally described by

the Confidentiality-Integrity-Accessibility (CIA) triad [22] which can be fully applied on our proposed prototype.

3. Research Approach

The hermeneutic framework for literature review by Boell et al is used in this paper. Whereby the following two circles could be fulfilled – (1) search and acquisition, (2) analysis and interpretation [23] to guide the artefact creation by deriving knowledge from existing prototypes within applied sciences. Circle (1) included grouping by a Process- and System-view since we wanted to differentiate between more practical and theoretical work. In (2) we categorized the paper content by Assets, Conditions and Capabilities to find easier decision making for our own prototype. The full summary is given in Table 1. Literature was gathered by the following keyword combinations: "blockchain-based certificate" + "application" and "blockchain-based application" + "education" with a careful forward and backward examination in four bibliographic databases: Google Scholar, Scopus, IEEE Xplore and AIS Library.

We used agile software development for instantiation included evaluation by feedback of stakeholders from the current certification process. This way we tried to maximize research output and keep the project work efficient driven as well as follow an approach to contribute to the knowledge base in the emerging field of BT.

Ref.	Process-view (Use Case)			System-view (Architecture)			Month Year
	Asset	**Condition**	**Capability**	**Asset**	**Condition**	**Capability**	
[24]	issuer, recipient, verifier and blockchain in between	enable cross-university student records and achievements	request for BT Tx a/o verification of Tx	EduCTX platform, 2-2 multisig addresses	DPOS (delegated proof of stake) consensus in permissioned Ethereum	ECTX tokens as equivalent for ECTS, issuing and revoking Certificates	Jun-21
[25]	issuers, recipient, consumers	online environment as an alternative for paper-based certificates	give a/o maintain a/o tracking of academic transcripts	QR-code	hash values for certificate stored on-chain with proof of work consensus	generation tamper-proof record	Apr-21
[26]	university, accreditation body, employer	user input of encryption and private key needed	responsibilities verify a/o creating a/o signing a/o issuing a/o revoking	verification app, university and accrediting interface	Truffle suite of Ethereum in testnet Rinkeby	automation and immutability	Apr-21
[27]	client, provider, authority and auditor	eHealth composite service	continuous monitoring and coordinated activities	Ethereum with evidence generation and workflow coordination	public cloud interface for blockchain	authentication, management, storage of Certificates for services	Nov-20
[28]	recipient, owner, authorities	gateway with defined policy	register personal data, grant a/o revoke access, access a/o verify a/o delete data, request logs	hybrid model with off-chain data and linked tokens	GDPR compliance of data (content)	control and audit network with untransparent (private) transactions	Oct-20
[29]	creator, verifier, content, user	controllable reward for intellectual property, unique password and documents with keys	issuing a/o access a/o authenticate a/o verification records	Ethereum Blockchain	remove intermediaries, obtain transparency, immutable information	Navigator Web3.JS with metamask and React including Truffle and Ganache	Oct-20
[30]	admin, owner, user	digital Certificates if paper-based document gets lost	request for secret a/o file download, view a/o control request and files	Name, Course, Date of Issue, Institution, Document Hash, IPFS	Hyperledger fabric with JSON-files in IPFS via URL	user and access management	Sep-20
[31]	issuer, owner, verifier technical system	review of existing blockchain-based solutions	assign a/o verify user, crossmatch data and de-encryption with on-chain hash	Hyperledger Fabric storage and identification framework	previously Certificate solution is open to vulnerability and data security is inadequate	verification in the blockchain are authentication, authorization, privacy, confidentiality, ownership	Jul-20
[32]	certificate authority, MSChain user	secure transparent Certificates	issuance, querying and revocation	wrapper to server layer	Hyperledger Fabric Blockchain network	microservices	Jul-20

Ref.	Process-view (Use Case)			System-view (Architecture)			Month Year
	Asset	Condition	Capability	Asset	Condition	Capability	
[33]	employe(e)rs and trust (as third party)	online survey and semi-structured interviews	authenticate and record Certificates	specify nothing more	specify nothing more	digitalization of key learning activities / achievements	Jul-20
[34]	Issuer (students), verifier (employers) and institutions	Education sector in India	store a/o request a/o view Certificates	Ethereum blockchain in Securecert platform	hash values for Certificate stored on-chain	smart contract with IPFS connection	Jul-20
[35]	Institution, registrar, employer	storing of digital Certificates	verification and validation	Three interfaces and Blockchain	chaotic algorithm for hashing	specify nothing more	Jul-20
[36]	certification authority and issuer	agencies with database	management, issuing, verification and revocation	Certificate template and receiver	smart contracts (Ethereum)	Web3.JS compatibility	Jun-20
[37]	specify nothing more	design needs to be close to R3 Corda Blockchain	specify nothing more	agents and DAG Tx tree as communication layer	pointer with hash value in the block description to constructed Tx	only every participant grows and maintains their own chain of Tx	Jun-20
[38]	education dept. with teacher and student, Certificate authority	Vietnam education system	writing a/o finding of Certificates	Hyperledger on public cloud infrastructure with off-chain 2-layer architecture	testing a/o evaluating platform and performance and operations measurement	input a/o write a/o validate a/o seal	Mar-20
[39]	issuer, recipient, credential issuer a/o verification and 3rd party	Thailand education system	match making for credentials controlled by owner	data models build in Merkel trees	Blockcerts infrastructure	manifest and credential files for privacy granted verification	Dec-19
[40]	university, student, employer, Certificate, observer and accreditation body	Pakistan education system	issue a/o share a/o verify a/o revoke Certificates and single records	Cerberus PoA (proof of authority) implementation of Ethereum	data models build in Merkel Trees	Parity and JSON compatibility with batch processing	Dec-19
[41]	user group students, teachers, academic staff, external	data aggregation in Minister of Education and Research	creation, verification a/o simulation, ordering a/o endorsement, adding by Blockchain Tx	application layer (each user group app), virtual state machine / data / network layer	smart contracts as bridge for Apps and Ledger entries	data models with dlock, Tx, Blockchain with world state for academic record and Certificate	Nov-19
[42]	issuer, recipient, verifier and Blockchain in between	Compliance with the EU eIDAS regulation	signing a/o check of validity of Certification authentication	Ethereum implementation	Blockcerts with open badges standard	Additional format validation	Oct-19
[43]	student, coordinator	scalable exchange of academic records in different formats between academic institutions	automated reliable request, upload, transfer and validate records	web browser based front-end and Hyperledger Middleware-Backend	accuracy and integrity not checked of academic records and no payment system	access control, Transcript request a/o process, Validation	Jun-19
[44]	review of existing blockchain-based solutions	Slovenia education system	record keeping a/o sharing	EduCTX platform	student-centric or institution-centric design	central Platform to combine investigated project solutions	May-19
[45]	student, institution, ledger, organization and validating entity	3rd party portal to validate certificates	validation request with institution private key signing of Certificate hashes	WAMP Server as bridge for PHP, HTML front-end and mySQL, Blockchain back-end	Multi-sig for every user authentication	combined structure to alter Certificates	Mar-19
[46]	student, coordinator	register a/o initiate a/o validate transaction, get a/o operate information, create certificate	decentralized distribution	web browser-based front-end and Hyperledger backend	separate configuration and operation components	selective visibility of Educational records	Mar-19

Ref.	Process-view (Use Case)			System-view (Architecture)			Month Year
	Asset	Condition	Capability	Asset	Condition	Capability	
[47]	examination of Blockchain initiatives	Blockchain used in eGoverment	adoption brings openness and transparency for services	specify nothing more	specify nothing more	specify nothing more	Jan-19
[48]	user, data purchaser a/o validators	GDPR compliance	service provider for "handling" data with monetization	platform	smart contracts, access and identity Blockchain	view a/o verify a/o governing datasets	Jan-19
[49]	issuer, Certificate authority	digital signatures on documents	create, use and check certificates	smart contracts	Pyethereum (Python Ethereum implementation)	gen-keys, issue, get-cert, sign, check-sig, revoke-cert	Oct-18
[50]	institution, registrar, employer	aim to further extend solution with medical recording system	register and populate student cohort, issuing a/o verify certificates	off-chain storage system and blockchain smart contract structure (holders a/o Certificate ID)	scalability not solved	database json export and Blockchain as bridge for interface	Jul-18
[51]	school, student, company with electronic Certificate system and Blockchain	QR-code and certificate serial number	mobile app and direct print on Paper-based certificates	Ethereum with smart contract interactions	service provider for maintaining blockchain system	Certification unit w/o generation, logout, query and student or company w/o inquiry	Apr-18
[52]	external companies, institution and educational organizations	ECTS harmonization within Europe and equal verification of Certificates			INFURA Ethereum node including solidity smart contracts	multi-step signing process scheme	Jan-18

Table 1: Overview of references (ordered by Month-Year) for Blockchain-based Certificates in public education.

4. Final design disclosure

The first (core) layer of our design is the Certificate as an object itself. It can be digital, analogue and is bound to one single person handed out from an institution at a fixed date to represent entirely accountability. This issued Certificates as objects are for students or attendants of seminars and lectures from public education of one certified institution. This unique relationship (object <-> person <-> institution) builds a trust anker as single identities from an offline network which can be verified as combination online by users with inbuild electronic hashes of documents and signatures. With this definition we are close to the new age of digital twins enhanced by BT [53].

Verification of objects include the proof attributes: authenticity, immutability and ownership. Different situations verify selectively on those attributes e.g., if the object is lost a re-creation process for all three attributes needs to be done. In case of job applications only authentic prove is needed. This business logics are programmed in the second (application) layer with user interfaces (human person interacts with data) and machine interfaces (automatic algorithms processing data). This logic space is in continuous growth to be able to solve disputed Tx by being under the overarching Governance of all users.

Our prototype is using a combination of Java and RESTful APIs within the HSMW network and a separate sandbox IT-infrastructure with docker to allow cloud-compatibility and have increased platform flexibility. The implemented system components are called modules which can interact via different communication protocols. Main driver for us is the https protocol with TLS encryption. Functions and actions from modules are declared as capabilities. The third (Trust) layer is based on a USB card reader device in combination with unique signature card to comply with the EU eIDAS regulation. This way the trust anker is built by qualified electronic signature stored directly on the digital Certificates e.g., as PDF files. The BT is placed as the overarching interface for public connection and outside networks (see Figure 1). The used BT for our prototype was in the beginning a cloud-based Hyperledger Fabric and shifted to a permissioned Ethereum-hybrid environment to get more user and first public institutions on board.

Following the definition of trust ankers a characterization between assets and conditions describes the functionality of Trust for granted valid or faked certificates. The data model for BT interaction is a simple JSON object with strings of electronic hashes. In detail it is a SHA256 hash for the PDF file itself and additional hash of three variable data fields e.g., last name, birthday and student ID plus a random generate string as pointer used in the verification process of the Certificate itself.

5. Conclusion and Outlook

From the last four years more than thirty peer-reviewed publications about Blockchain-based applications for Certificates in public education could be found and analyzed. A trend towards one single BT could not be found.

Conditions (Trust and Security) and capabilities (create/revoke and verify Certificates) are following the same problem space only the used assets vary in on- and off-chain solutions for data storage. We tried to use high citied and top ranked references but might missed more insightful ones. This lack of practitioners we covered by our own prototyping and development experience during creation of the shown design disclosure. BT singled out and endorsed as an interface for Trust in public open networks but strongly needs additional technology like the underlying USB reader device to manifest real-life states to digital objects.

Further research can follow on one hand the theoretical construction and modelling as well as comparing of our proposed work to existing solutions or on the other hand a practical testing how compatible our conceptual design is to include other innovative technology for digital Certificates.

Our prototype itself is going in continues development by two-week sprints parallel to a GO-live state.

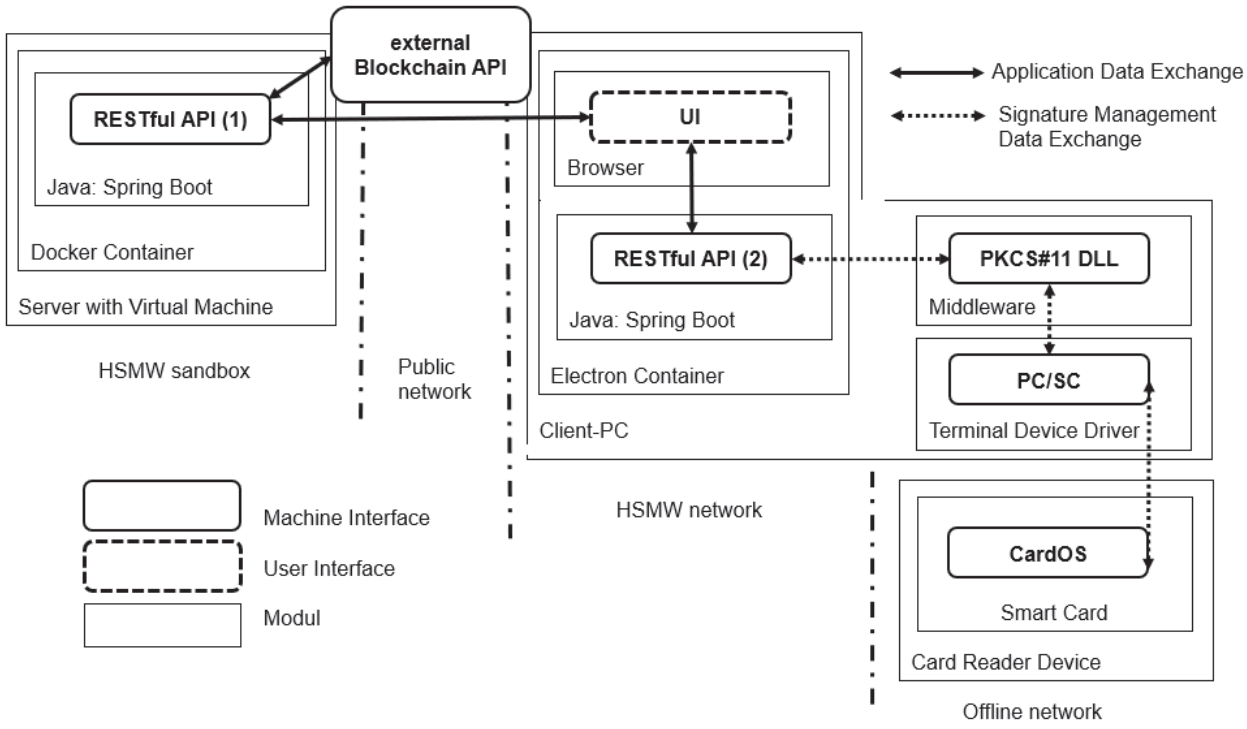

Figure 1: Design disclosure of our prototype with external USB card reader, HSMW sandbox and a secured software client including web User Interface (UI) for Microsoft Windows environment - arrows show communication routes.

Acknowledgements

Special thanks to the German Research Foundation who supplied financial the WIR! showcase region Mittweida and us as the ECHT! sub-project (FKZ 03WIR1311B).
Furthermore, we are grateful for our industry partner QuadriO GmbH.

References

[1] V. Gurbaxani and D. Dunkle, “Gearing Up For Successful Digital Transformation,” *MISQE*, vol. 18, no. 3, pp. 209–220, Sep. 2019, doi: 10.17705/2msqe.00017.

[2] O. Labazova, T. Dehling, and A. Sunyaev, “From Hype to Reality: A Taxonomy of Blockchain Applications,” in *Proceedings of the 52nd Hawaii International Conference on System Sciences*, Grand Wailea, Hawaii, p. 10.

[3] R. Beck, “Beyond Bitcoin: The Rise of Blockchain World,” *Computer*, vol. 51, no. 2, pp. 54–58, Feb. 2018, doi: 10.1109/MC.2018.1451660.

[4] R. Beck and C. Müller-Bloch, “Blockchain as Radical Innovation: A Framework for Engaging with Distributed Ledgers,” in *Hawaii International Conference on System Sciences 2017 (HICSS-50)*, Jan. 2017, p. 10.

[5] M. Rossi, Mueller-Bloch, Christoph, J. B. Thatcher, and R. Beck, “Blockchain Research in Information Systems: Current Trends and an Inclusive Future Research Agenda,” *JAIS*, pp. 1388–1403, 2019.

[6] L. Zavolokina, R. Ziolkowski, and I. Bauer, “Management, Governance, and Value Creation in a Blockchain Consortium,” *MISQE*, vol. 19, no. 1, pp. 1–17, Mar. 2020, doi: 10.17705/2msqe.00022.

[7] J. Mendling, G. Decker, R. Hull, H. A. Reijers, and I. Weber, “How do Machine Learning, Robotic Process Automation, and Blockchains Affect the Human Factor in Business Process Management?,” *CAIS*, pp. 297–320, 2018, doi:

10.17705/1CAIS.04319.
[8] A. Rieger, F. Guggenmos, J. Lockl, G. Fridgen, and N. Urbach, "Building a Blockchain Application that Complies with the EU General Data Protection Regulation," *MISQE*, vol. 18, no. 4, pp. 263–279, Dec. 2019, doi: 10.17705/2msqe.00020.
[9] D. Gozman, J. Liebenau, and T. Aste, "A Case Study of Using Blockchain Technology in Regulatory Technology," *MISQE*, vol. 19, no. 1, pp. 19–37, Mar. 2020, doi: 10.17705/2msqe.00023.
[10] W. Presthus and H. Sørum, "Consumer perspectives on information privacy following the implementation of the GDPR," *JISPM - International Journal of Information Systems and Project Management*, no. 7, pp. 19–34, 2019, doi: 10.12821/ijispm070302.
[11] A. Alketbi, Q. Nasir, and M. A. Talib, "Blockchain for government services — Use cases, security benefits and challenges," in *2018 15th Learning and Technology Conference (L&T)*, Jeddah, Feb. 2018, pp. 112–119. doi: 10.1109/LT.2018.8368494.
[12] 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.
[13] M. Murray, "Tutorial: A Descriptive Introduction to the Blockchain," *CAIS*, pp. 464–487, 2019, doi: 10.17705/1CAIS.04525.
[14] A. I. Sanka, M. Irfan, I. Huang, and R. C. C. Cheung, "A survey of breakthrough in blockchain technology: Adoptions, applications, challenges and future research," *Comput. Commun.*, 2021.
[15] 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, Mar. 2019.
[16] O. Labazova, E. Kazan, T. Dehling, T. Tuunanen, and A. Sunyaev, "Managing Blockchain Systems and Applications: A Process Model for Blockchain Configurations," p. 27.
[17] M. Fleischmann and B. S. Ivens, "Exploring the Role of Trust in Blockchain Adoption: An Inductive Approach," p. 10.
[18] R. Beck, J. S. Czepluch, N. Lollike, and S. Malone, "BLOCKCHAIN – THE GATEWAY TO TRUST-FREE CRYPTOGRAPHIC TRANSACTIONS," p. 15, 2016.
[19] H. Treiblmaier and R. Beck, Eds., *Business Transformation through Blockchain: Volume II*. Cham: Springer International Publishing, 2019. doi: 10.1007/978-3-319-99058-3.
[20] K. Emerson, T. Nabatchi, and S. Balogh, "An Integrative Framework for Collaborative Governance," *Journal of Public Administration Research and Theory*, vol. 22, no. 1, pp. 1–29, Jan. 2012, doi: 10.1093/jopart/mur011.
[21] T A Pai Management Institute and A. Das, "Trust in 'Trust-free' Digital Networks: How Inter-firm Algorithmic Relationships Embed the Cardinal Principles of Value Co-creation," *THCI*, vol. 12, no. 4, pp. 228–252, Dec. 2020, doi: 10.17705/1thci.00137.
[22] M. Warkentin and C. Orgeron, "Using the security triad to assess blockchain technology in public sector applications," *International Journal of Information Management*, vol. 52, p. 102090, Jun. 2020.
[23] S. K. Boell and D. Cecez-Kecmanovic, "A Hermeneutic Approach for Conducting Literature Reviews and Literature Searches," *CAIS*, vol. 34, 2014.
[24] T. Lushi, "Blockchain in Education: possibilities for a blockchain based study management system for Higher Education Institutions," presented at the International Conference at Brno University of Technology, Brno, Jul. 2019.
[25] S. Alam, H. A. Y. Ayoub, R. A. A. Alshaikh, A. Hayawi, and H. AL-Hayawi, "A Blockchain-based framework for secure Educational Credentials," *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, vol. 12, no. 10, pp. 5157–5167, Apr. 2021.
[26] E. Leka and B. Selimi, "Development and Evaluation of Blockchain based Secure Application for Verification and Validation of Academic Certificates," *AETiC*, vol. 5, no. 2, pp. 22–36, Apr. 2021.
[27] C. A. Ardagna, M. Anisetti, B. Carminati, E. Damiani, E. Ferrari, and C. Rondanini, "A Blockchain-based Trustworthy Certification Process for Composite Services," in *2020 IEEE International Conference on Services Computing (SCC)*, Beijing, China, Nov. 2020, pp. 422–429.
[28] F. Molina, G. Betarte, and C. Luna, "A Blockchain based and GDPR-compliant design of a system for digital education certificates," *ArXiv*, Oct. 2020.
[29] M. P. Jaramillo and N. Piedra, "A blockchain model proposal for the decentralized management of academic credentials in Ecuadorian universities," in *2020 9th International Conference On Software Process Improvement (CIMPS)*, Mazatlan, Sinaloa, Mexico, Oct. 2020, pp. 94–102.
[30] N. Sarganachari, "Digital Degrees and Markcards Using Blockchain Technology," *International Journal of Innovative research in science engineering and technology*, vol. 9, no. 2, p. 9, Sep. 2020.
[31] O. S. Saleh, O. Ghazali, and M. Rana, "BLOCKCHAIN BASED FRAMEWORK FOR EDUCATIONAL CERTIFICATES VERIFICATION," *Journal of critical reviews*, vol. 7, no. 3, pp. 79–84, Jul. 2020.
[32] D. Dilshan, S. Piumika, C. Rupasinghe, I. Perera, and P. Siriwardena, "MSChain: Blockchain based Decentralized Certificate Transparency for Microservices," Jul. 2020, p. Moratuwa, Sri Lanka.
[33] B. Awaji, E. Solaiman, and L. Marshall, "Investigating the Requirements for Building a Blockchain-Based Achievement Record System," in *ICIEI 2020: Proceedings of the 51th International Conference on Information and Education Innovations*, Jul. 2020, pp. 56–60.
[34] P. Gundgurti, K. Alluri, P. E. Gundgurti, S. H. K, and

V. G, "Smart and Secure Certificate Validation System through Blockchain," *2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA)*, 2020, doi: 10.1109/ICIRCA48905.2020.9182975.

[35] A. Gayathiri, J. Jayachitra, and S. Matilda, "Certificate validation using blockchain," *2020 7th International Conference on Smart Structures and Systems (ICSSS)*, 2020, doi: 10.1109/ICSSS49621.2020.9201988.

[36] R. Xie *et al.*, "Ethereum-Blockchain-Based Technology of Decentralized Smart Contract Certificate System," *IEEE Internet of Things Magazine*, vol. 3, no. 2, pp. 44–50, Jun. 2020.

[37] P. Otte, M. de Vos, and J. Pouwelse, "TrustChain: A Sybil-resistant scalable blockchain," *Future Generation Computer Systems*, vol. 107, pp. 770–780, Jun. 2020.

[38] B. Nguyen, T.-C. Dao, and B.-L. Do, "Towards a blockchain-based certificate authentication system in Vietnam," *PeerJ. Comput. Science*, vol. 6, p. e266, 2020.

[39] A. M. San, N. Chotikakamthorn, and C. Sathitwiriyawong, "Blockchain-based Learning Credential Verification System with Recipient Privacy Control," in *2019 IEEE International Conference on Engineering, Technology and Education (TALE)*, Yogyakarta, Indonesia, Dec. 2019, pp. 1–5.

[40] A. Tariq, H. B. Haq, and S. T. Ali, "Cerberus: A Blockchain-Based Accreditation and Degree Verification System," *arXiv:1912.06812 [cs]*, Dec. 2019.

[41] A. Rachmat and Albarda, "Design of Distributed Academic-record System Based on Blockchain," in *2019 International Conference on ICT for Smart Society (ICISS)*, Bandung, Indonesia, Nov. 2019, pp. 1–6.

[42] M. Baldi, F. Chiaraluce, M. Kodra, and L. Spalazzi, "Security Analysis of a Blockchain-based Protocol for the Certification of Academic Credentials," *ArXiv*, Oct. 2019.

[43] A. Badr, L. Rafferty, Q. H. Mahmoud, K. Elgazzar, and P. C. K. Hung, "A Permissioned Blockchain-Based System for Verification of Academic Records," in *2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, CANARY ISLANDS, Spain, Jun. 2019, pp. 1–5.

[44] A. Kamišalić, M. Turkanović, S. Mrdović, and M. Hericko, "A Preliminary Review of Blockchain-Based Solutions in Higher Education," in *LTEC 2019: Learning Technology for Education Challenges*, May 2019, p. pp 114-124.

[45] K. Gowri Shankar, A. David, M. Kamesh, and B. Jaison, "Blockchain based Certificate Issuing and Validation," *International Research Journal of Engineering and Technology (IRJET)*, vol. 6, no. 3, Mar. 2019.

[46] E. E. Bessa and J. S. B. Martins, "A Blockchain-based Educational Record Repository," presented at the ADVANCE 2019 - International Workshop on ADVANCEs in ICT Infrastructures and Services, Praia, Mar. 2019.

[47] C. Alexopoulos, M. A. Loutsaris, Y. Charalabidis, A. Androutsopoulou, and Z. Lachana, "Benefits and Obstacles of Blockchain Applications in e-Government," in *Towards Government 3.0: Disruptive ICTs, Advanced Policy Informatics/ Analytics and Government as a Platform*, Grand Wailea, Hawaii, Jan. 2019, p. 10.

[48] B. Faber, G. Michelet, N. Weidmann, R. R. Mukkamala, and R. Vatrapu, "BPDIMS:A Blockchain-based Personal Data and Identity Management System," in *The Transformational Impact of Blockchain*, Grand Wailea, Hawaii, Jan. 2019, p. 10.

[49] N. Prado and M. Henriques, "On-block certs: blockchain-based lightweight digital certificates," in *Anais Estendidos do XVIII Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais*, Natal, Oct. 2018, pp. 177–180.

[50] A. Curmi and F. Inguanez, "BlockChain Based Certificate Verification Platform," in *Business Information Systems Workshops*, Cham, Jul. 2018, pp. 211–216.

[51] J.-C. Cheng, N.-Y. Lee, C. Chi, and Y.-H. Chen, "Blockchain and smart contract for digital certificate," in *2018 IEEE International Conference on Applied System Invention (ICASI)*, Chiba, Apr. 2018, pp. 1046–1051.

[52] M. Turkanovic, M. Holbl, K. Kosic, M. Hericko, and A. Kamisalic, "EduCTX: A Blockchain-Based Higher Education Credit Platform," *IEEE Access*, vol. 6, pp. 5112–5127, Jan. 2018.

[53] P. Raj, "Empowering digital twins with blockchain," in *Advances in Computers*, vol. 121, Elsevier, 2021, pp. 267–283.

Sind Token Sachen? Eine rechtsvergleichende Analyse zwischen Deutschland und Italien

Serena Maria Scalera
Institut für Italienisches Recht, Leopold-Franzens-Universität, Innrain 52, 6020 Innsbruck

Als § 2 Abs 3 des elektronischen Wertpapiergesetzes (eWpG) in Kraft getreten am 10. Juni 2021 eine Sachfiktion die für elektronische Wertpapiere – worunter Kryptowertpapiere auch zu verstehen sind – eingeführt hat, stellte sich die Frage nach der zivilrechtlichen Rechtsnatur von Token. Ausgehend von einer eingehenden und rechtsvergleichenden Analyse der Grund-lagen des deutschen Sachenrechts, das eine engere Auffassung des Sachbegriffes vornimmt, und des italienischen Sachen-rechts, welches einen weiteren Interpretationsspielraum des Sachbegriffes zulässt, befasst sich die vorliegende Arbeit mit dieser Fragestellung und versucht eine Antwort zu finden.

As the eWpG has entered into force and introduced the legal provision of § 2 (3), that places digital securities, including crypto securities, under property law, the question of the legal nature of tokens under civil law arised. Based on an in-depth and comparative analysis of the fundamentals of German property law, which adopts a narrower view of the concept of property, and Italian property law, which allows a broader scope of interpretation of the concept of property, this paper deals with such a question and attempts to find an answer.

1. Einleitung

Aus Anlass des Inkrafttretens des Gesetzes über elektronische Wertpapiere – eWpG (BGBl. I S. 1423) am 10. Juni 2021 ist es von grundlegender Bedeutung, die Rechtsnatur von Token zu hinterfragen. Das eWpG hat nämlich die Möglichkeit eingeführt, elektronische Wertpapiere und Kryptowertpapiere zu emittieren, wobei die zweiten dem Oberbegriff der Wertpapiere angehören. Mit diesem Gesetzgebungsakt hat Deutschland Öffnungsschritte in Richtung Digitalisierung gemacht, indem es die Stützung auf Blockchain oder auf anderen DLT-Systemen erlaubt. In Italien ist dagegen noch nicht auf gesetzgeberischer Ebene die Rede, die Rechtsordnung für solche neuen Systeme zu öffnen. Mittlerweile bemüht sich dann die Lehre – in einigen Fällen mit Unterstützung der Rechtsprechung – diesbezüglich einige Fragen zu beantworten, die man von der Praxis herleiten kann, wie zB welche Rechtsnatur man den Token zuzuschreiben kann. Die vorliegende Arbeit setzt sich das Ziel, diese Frage eine Antwort durch eine rechtsvergleichende Analyse des Sachbegriffes in beiden Rechtsordnungen – deutsch und italienisch – zu geben, wobei grundlegende Kenntnisse der Funktionsweise einer Blockchain bzw eines DLT-Systems und der Emittierungsmechanismen eines Tokens als bekannt angenommen werden.

2. Begriffsbestimmungen

2.1. Der Token-Begriff

Token werden als Einheiten definiert, welche „direkt auf einer Blockchain emittiert werden und als Teil eines Protokolls einer üblicherweise ansehbaren Datenbank existieren, welche den Bestand und die Übertragung der Tokens dokumentiert". [1] Jede solche Einheit kann sowohl digitale als auch reale Rechte oder Werte repräsentieren. Es wird des Weiteren zwischen einigen Kategorien von Token unterschieden. Token weisen die folgenden Eigenschaften auf: sie sind unkörperliche Datensätze (1), die einen Wert – oder ein Recht – repräsentieren (2) und zu einem Rechtsträger zugeordnet werden (3). [2]

Abhängig davon, welches Recht oder welchen Wert sie repräsentieren, lassen sich drei Klassen von Token unterscheiden: Token die digitalen Werteinheiten – wie zB virtuelle Währungen und Kryptowährungen – repräsentieren fallen in die Klasse von Currency-Token (a), und wenn sie Rechte auf Benutzung gewisser Dienstleistungen bzw digitale Nutzungen repräsentieren, sind sie Utility-Token (b). Letztlich werden diejenigen Security-Token (c) genannt, die unter anderem auch Mitgliedschaftsrechte repräsentieren. [3]

Aus dieser Dreiteilung lässt sich eine allgemeinere Zweiteilung ableiten. Token unterscheiden sich zwischen intrinsischen und extrinsischen Token. Zu den Ersten gehören jenen Token, denen aufgrund ihrer Existenz ein Wert zugemessen werden kann, wie Currency-Token. Im Gegensatz dazu wird den extrinsischen Token ein Wert nur zugeschrieben, wenn sie mit einem Vermögensgegenstand oder mit einem daraus ergebenden Anspruch verbunden sind. [4] Beispiel von extrinsischen Token sind Utility- und Security-Token.

2.2. Der Sachbegriff nach deutschem und italienischem Recht

Nach dem deutschen Recht ist zwischen Sachen und Gegenstände zu unterscheiden. Beide gehören zum Oberbegriff „Rechtsgut", wobei aber der Begriff Sachen nur jene Gegenstände bezeichnet, die körperlich sind, und der Begriff Gegenstand unkörperliche Gegenstände umfasst. [5] § 90 BGB definiert nämlich die Sachen nur als körperliche Gegenstände. Eine solche enge Definition von Sache braucht man nicht weit auszulegen.

Im italienischen Rechtssystem begegnet man einem anderen Sachbegriff. Art 810 des italienischen Zivilgesetzbuches (folglich: Codice civile) bezeichnet eine Sache bzw ein Rechtsgut als ein Ding, das Gegenstand von

Rechten sein kann. Eine so scheinbar klare Definition von Sache hat mit sich die Notwendigkeit gebracht, von der Lehre eine ausführliche Auslegung zu erschaffen. Zu erläutern ist nämlich, was als Ding und was als Gegenstand von Rechten zu verstehen ist. Erstens soll man zwischen Dingen im naturalistischen Sinn, wie Luft, [6] und Dingen im Sinne des Art 810 Codice civile unterscheiden. Die Verwendung in der Praxis von den Worten Ding, Gegenstand und Sache als Synonyme könnte dann zu Verwirrung führen. Eben das Wort Ding könnte zu der Annahme verleiten, dass eine grundlegende Voraussetzung dafür, dass man einem Gut die Rechtsnatur einer Sache iSv Art 810 Codice civile zuschreiben kann, seine Körperlichkeit ist. Es würden demzufolge immaterielle Güter nicht vom Sachbegriff umfasst. Die Vorschrift wurde bis in die 1950-er Jahren in diese Richtung ausgelegt, da die Lehre einstimmig für eine restriktive Auslegung des Codice civile war. Den Sachbegriff nur auf körperliche Gegenstände einzuschränken wäre in zweierlei Hinsicht problematisch. Einerseits würde der Umfang der Sachen verengt, wobei es auch Sachen gibt, die zB Dienstleistungen als Gegenstand haben. Es würden denn alle neuen Gegenstände nicht umgefasst, die in dem Zeitalter der Digitalisierung entstanden sind. [7] Auf der anderen Seite würde die Anzahl an Sachen mit der Anzahl an körperlichen Sachen in unangemessener Weise gleichgesetzt. [8] Gemäß Art 810 Codice civile sind dann Sachen sowohl körperliche als auch immaterielle Gegenstände. [9]

Ferner war die Eigenschaft, Gegenstand von Rechten zu sein, nicht einfach auszulegen. Die Lehre hat sich unterschiedlich darüber geäußert. Sachen wären nur die Dinge, an denen man ein – vom Gesetz geschütztes – Interesse hat, sie sich anzueignen, sie zum Gegenstand eines eigenen Rechtes zu machen und andere von ihrer Nutzung auszuschließen. Der Sachbegriff würde dann mit der Möglichkeit verbunden, ein absolutes Recht über die Sache ausüben zu können bzw Eigentümer von der Sache zu sein. [10] Ein anderer Teil der Lehre behauptet dagegen, dass der Sachbegriff auf dem Tauschwert der Sache selbst berühren würde, [11] wobei man als Tauschwert die Eigenschaft einer Sache verstehen soll, vererbbar oder verkehrsfähig zu sein. Eine solche Eigenschaft könnte man aber im allgemein an Sachen zuschreiben, die auch keine Rechtsgüter sind. Dieses Kriterium wäre dann nicht erforderlich für eine Trennung zwischen Sachen iSv Art 810 Codice civile und anderen Gegenstände. [12]

Die Lehre ist dann einheitlich dazu gelangt, das Interesse des Menschen bei der Auslegung der Vorschrift in den Mittelpunkt zu setzen: Sachen im Sinne von Art 810 Codice civile sind diejenigen, die ein schutzwürdiges privaten oder öffentlichen Interesse erfüllen. [13] Damit wird es gerechtfertigt, dass der Begriff auch die Sachen umfasst, die dem Staat gehören, sog beni demaniali.

Aus diesen Ausführungen folgt, dass dem im Art 810 Codice civile enthaltenen Begriff von Sachen im Sinne von Rechtsgütern eine wirtschaftlich-soziale Bedeutung zugemessen wird. Es wird dann – wie später ersichtlich wird - vorstellbar, die Sachen je nach dem zu erfüllenden Interesse unterschiedlichen Rechtsbestimmungen zu unterwerfen. [14]

3. Klassifizierung von Sachen

3.1. Körperliche Sachen

Gemäß § 90 BGB ist eine Sache ein körperlicher Gegenstand. Damit versteht man, dass die Sache als Gegenstand von Besitz und Eigentum beherrschbar sein muss, dh sinnlich wahrnehmbar (a) und im Raum abgegrenzt oder abgrenzbar sein (b). Körperlich sind jene Gegenstände, man entweder anfassen oder sinnlich wahrnehmen und technisch beherrschen kann. Fehlt die Wahrnehmbarkeit, kann der Gegenstand nicht beherrscht werden. Als Beispiel davon kann man Strom nennen: er ist nicht wahrnehmbar und nicht beherrschbar. Demzufolge ist Strom keine Sache iSv § 90 BGB. Die Abgrenzbarkeit in einem Raum bezeichnet die Verkehrsauffassung eines Gegenstanden, indem er körperlich begrenzbar oder in einem Behälter absperrbar ist. Gegenstände, die durch künstliche Kennzeichnungen abgegrenzt werden können, fallen auch unter den Sachbegriff. Die Eigenschaft abgrenzbar zu sein, führt zur Beherrschbarkeit der Gegenstände. [15]

Im Gegensatz zum deutschen Recht, wo die Körperlichkeit eines Gegenstandes Tatbestand des Sachbegriffes ist und explizit im BGB darauf hingewiesen wird, hat der italienische Gesetzgeber eine mögliche Unterscheidung zwischen körperlichen und immateriellen Sachen nicht zum Ausdruck gebracht. Was dann unter körperlich zu verstehen ist, ist von der Lehre erforscht worden. Damit eine Sache die Eigenschaft der Körperlichkeit aufzeigen kann, soll sie anfassbar und wahrnehmbar sein und eine wirtschaftliche Verwertbarkeit aufweisen. Um ein ähnliches Beispiel wie das oben genannte zu nehmen, sind natürliche Energien – wie Strom – Sachen bzw Rechtsgüter, da sie einen wirtschaftlichen Wert haben (Art 814 Codice civile). [16]

3.2. Nichtkörperliche Gegenstände und immaterielle Sachen

Während nach italienischem Recht eine Gegenüberstellung zwischen körperlichen und immateriellen Sachen möglich ist, wie später ersichtlich wird, ist dies in Deutschland aufgrund des engen Sachbegriffes vom § 90 BGB nicht vorstellbar. Es ist auf einer Seite die Rede von Sachen und auf der anderen die Rede von nichtkörperlichen Gegenständen, uzw diejenigen, die nicht anfassbar oder physisch wahrnehmbar sind. Dazu zählen sowohl Vermögensrechte als auch weitere Gegenstände des Wirtschaftsverkehrs, die vom Gesetzgeber nicht geregelt worden sind. Anlässlich einer zunehmend fortgeschrittenen Digitalisierung neigt die Lehre dazu, immaterielle Güter als Sachen behandeln zu wollen, indem man ihnen die Rechtsnatur einer Sache zuschreibt oder

sie den Rechtsvorschriften des Sachenrechtes unterwirft. Dies scheint aber natürlicherweise nicht möglich zu sein, bis der Gesetzgeber einen Reformvorgang des Sachenrechtes nicht einsetzt. [17]

Zu den nichtkörperlichen Gegenständen zählen dann zB Immaterialgüterrechte, die in speziellen Gesetzen – Markengesetz, Urheberrechtgesetz - geregelt werden, Forderungen, beschränkte dingliche Rechte, Gestaltungsrechte usw.

Nach dem italienischen Recht können dagegen Sachen iSv Art 810 Codice civile aufgrund der wirtschaftlich-sozialen Bedeutung des Begriffes sowohl körperlich als auch immateriell sein. [18] Darüber, dass eine solche Unterkategorie von Sachen eigenständig und gültig ist, ist die Lehre sich einig, obwohl sie sehr unterschiedliche Sachenarten erfassen kann. [19] Immaterielle Sache ist dann das geistige Eigentum, dessen Gegenstand im Art 2575 Codice civile [20] definiert wird. Das Urheberrecht ist in dem Gesetz Nr 633 vom 22. April 1941 geregelt. Die heutige Fassung dieses Gesetztes zielt darauf ab, eine Regelung auch zB für Datenbanken und Softwares zu schaffen. Mit gesetzesvertretendem Dekret Nr 169 vom 6. Mai 1999 sind die Datenbanken als Sammlung von Werken, Daten oder anderen Elementen, die systematisch angeordnet und einzeln elektronisch zugänglich sind, dem geistigen Eigentum gleichgestellt worden und werden denn durch das Gesetz Nr 633/1941 geregelt. [21] Eine Gleichstellung mit dem geistigen Eigentum ist auch für Software im Jahr 1992 erschaffen worden. [22]

Schuldverschreibungen und entmaterialisierte Wertpapiere, sog valori mobiliari/titoli scritturali, [23] zählen auch zu den immateriellen Sachen, da sie Gegenstand von Rechtsverhältnissen sein können. Wie es für das geistige Eigentum gilt, werden sie speziellen Gesetzen – TUF, Testo unico della finanza (Einheitstextes über Finanz) – unterworfen. Sie entsprechen den deutschen elektronischen Wertpapieren, deren Emission seit Juni 2021 durch das Inkrafttreten des eWpG zugelassen wird.

Ob entmaterialisiere Wertpapiere als immaterielle Sachen zu verstehen sind, ist aber noch umstritten. Ein Teil der Lehre behauptet, dass aufgrund der Vertretbarkeit und der Gleichmäßigkeit der entmaterialisierten Einheiten die Regelung, die normalerweise für die Sachen gilt, unanwendbar sei. Die titoli scritturali werden nämlich wie folgt emittiert: der Emittent benennt eine Verwahrstelle und teilt ihr die Charakteristiken der Emissionen und der Intermediäre (uzw zum Beispiel Banken) mit, denen die emittierten Wertpapiere gutgeschrieben werden sollen. Die Verwahrstelle eröffnet für jede Emission ein Konto im Namen des Emittenten und für jeden Intermediär, der eines beantragt, ein Konto zur Erfassung der getätigten Aktienverfügungen. Es wird dann ein Netzwerk zwischen der zentralen Verwahrstelle und den gewerblichen Vermittlern geschaffen, um die Werte der verschiedenen Aktien oder Wertpapierarten der jeweiligen Inhaber zu empfangen. In diesem Netzwerk zirkulieren die Werte selbst durch dokumentarische Verbuchungsvorgänge, wobei die Konten der beteiligten Parteien belastet und gutgeschrieben werden. [24]

3.3. Unbewegliche Sachen

Unbewegliche Sachen werden in beiden Rechtsordnungen beweglichen Sachen gegenübergestellt.

Im deutschen BGB findet man keine Definition von unbeweglichen Sachen, der Begriff gar nicht verwendet. Es ist nämlich die Rede von Grundstücken und deren Bestandteile (§§ 94-97 BGB), die das Hauptbeispiel von unbeweglichen Sachen darstellen. Sie werden als ein räumlicher und im Grundbuch als solchen geführten Teil der Erdoberfläche definiert [25] und unterstehen der Grundbuchordnung. Im Gegensatz zum BGB wird der Begriff „unbewegliche Sache" oft in der ZPO - §§ 24, 26, 848, 855 usw [26] verwendet.

Im Art 812 Codice civile wird zwischen unbeweglichen und beweglichen Sachen unterschieden. Unbewegliche Sachen sind der Grund, der Boden, die Quellen usw und alles was auf natürliche oder künstliche Weise mit dem Grund verbunden ist (Abs 1). Als unbeweglich sind auch andere Sachen zu verstehen, die vom Gesetzgeber selbst eine solche Bezeichnung bekommen haben, wie zB Mühlen und Bäder (Abs 2). Die Eigenschaft einer Sache, unbeweglich zu sein, bringt Folgen bezüglich der anzuwendenden Regelung mit sich: zB ist die schriftliche Form für die Wirksamkeit von Rechtshandlungen erforderlich, die solche Sachen als Gegenstand haben (Art 1350 Codice civile).

3.4. Bewegliche Sachen

Alle sonstigen Sachen, die nicht Grundstücke oder deren Bestandteile sind, sind bewegliche Sachen (§§ 93- 95 BGB).

Gemäß Art 812 Abs 3 Codice civile sind bewegliche Sachen alle anderen Sachen, uzw diejenigen die nicht unbeweglich sind. Wie oben schon erwähnt, führt die Eigenschaft einer Sache un- oder beweglich zu sein zur Anwendung verschiedener Vorschriften: zB kann man mittels verlängerten Besitzes Eigentümer einer beweglichen Sache werden (Art 1153 und 1158 ff Codice civile).

3.5. Finanzprodukte

Nach dem italienischen Recht stellen Finanzprodukte eine andere Kategorie von Sachen dar. Sie werden nicht im Codice civile, sondern im TUF, Testo Unico della Finanza-Einheitstext über Finanz, definiert und geregelt. Finanzinstrumente, die im Art 1 Abs 2 und in der 1. Anlage Sek. C TUF definiert werden, und jede andere Form von Anlagen gehören zu den Finanzprodukten. Sie werden durch öffentliche Angebote emittiert, die nach den Vorschriften vom Art 94 TUF geführt werden sollen, und unterstehen der Kontrolle der Consob, Commissione Nazionale per le Società e la Borsa (Art 99-101 TUF). Im Fall eines Verstoßes gegen die Vorschriften über die Emission von Finanzprodukten hat sie nämlich die

Macht solche Angebote zu unterbrechen oder zu sperren (Art 99 ff TUF).

Ferner ist zu erwähnen, dass die Finanzinstrumente auf dem Kapitalmarkt handelbar sind. [27]

4. Rechtsnatur von Token

4.1. Intrinsische Token: *Currency*-Token

Wie im Punkt 2.1. erwähnt, stellen virtuelle Währungen und Kryptowährungen das Hauptbeispiel von Currency-Token. Sie spielen in diesem Zeitalter eine zentrale Rolle in vielen Rechtsordnungen, indem sie die grundlegenden Kenntnisse in Frage stellen. Virtuelle Währungen werden als eine digitale Darstellung eines Werts, die von keiner Zentralbank oder öffentlichen Stelle emittiert wurde oder garantiert wird und nicht zwangsläufig an eine gesetzlich festgelegte Währung angebunden ist und die nicht den gesetzlichen Status einer Währung oder von Geld besitzt, aber von natürlichen oder juristischen Personen als Tauschmittel akzeptiert wird und die auf elektronischem Wege übertragen, gespeichert und gehandelt werden kann. [28]

Dass virtuelle Währungen nicht in einem zentralisierten System entstehen, scheint in beiden Rechtsordnungen gegen die Anerkennung solcher Währungen als Geld zu sprechen. [29]

Würde man sie als Forderung qualifizieren, hätte man keine emittierende Stelle, gegen die man eine solche Forderung richten könnte. [30]

Nach dem deutschen Recht wäre es nicht möglich, Kryptowährungen als Sachen zu bezeichnen. Wie im Punkt 2.2. angegeben, ist die Körperlichkeit erforderlich, damit eine Sache gem § 90 BGB vorliegen kann. [31]

Fehlt die Verkörperung, sind Gegenstände nicht als Sachen zu bezeichnen. Dies ist genau bei virtuellen Währungen und Kryptowährungen der Fall, [32] da sie nur in digitaler Form existieren. Daraus folgt, dass sie nicht Gegenstand von Sacheigentum iSv §§ 903 ff BGB sein können. [33] Es entsteht dann die Frage, ob sie als Immaterialgüter behandelt werden können. § 2 UrhG legt fest, dass Werke solche sind, die eine geistige Schöpfung voraussetzen (Abs 2). Schaut man die Schöpfungsprozesse von Token, wird ersichtlich, dass Token durch die Ausführung technischen Rechnerprotokolle entstehen, die nur Strom und Rechnerenergie bedürfen. [34] Aus demselben Grund könnten Token auch nicht Computerprogrammen iSv § 69a UrhG gleichgestellt werden. [35] Dass Token als „sonstige Rechte" iSv § 823 BGB bezeichnet werden können, wird von einem Teil der Lehre behauptet. [36] Die Voraussetzung der Existenz einer Rechtsposition, die konkret zuwiesen werden kann, und der Möglichkeit, dass alle übrigen Personen von deren Nutzung ausgeschlossen werden können, soll bestehen, damit man diese These vertreten kann. Der Inhaber von Token besitzt keine unmittelbare Verfügungsgewalt über die tokenisierten Daten, da Token keine nutzreinigenen Daten darstellen. Zu schützen wäre dann nicht die Rechtsposition in sich, sondern die Nutzung der privaten Schlüssel und die damit verbundene Einwirkungsmöglichkeit auf fremden Daten. Genau eine solche Einwirkungsmöglichkeit würde die Zustimmung eines Rechtsschutzes gem § 823 Abs 1 BGB begründen, wenn man Token mit dem anerkannten Besitz vergleicht, da er nur auf die tatsächliche Verfügungsgewalt abstellt. [37] Currency-Token könnten nach deutschem Recht als sonstige Rechte behandelt werden und damit würden sie den §§ 823 ff BGB unterstehen. Aus aufsichtsrechtlicher Sicht werden Currency-Token von der BaFin als Rechnungseinheiten iSv § 1 Abs 11 S 1 Nr 7 KWG qualifiziert. [38] Gegen diese Einordnung hat sich das KG Berlin geäußert. [39] Das Gericht legt den Begriff eng. Obwohl dann Waren und Dienstleistungen in den Nachbarländern den Rechnungseinheiten gleichgestellt werden können, wäre dies in Deutschland nicht möglich und demzufolge könnten Kryptowährungen nicht als solchen bezeichnet werden. [40] Trotzdem qualifiziert die BaFin Currency-Token weiter als Rechnungseinheiten.

Nach dem italienischem Recht scheint die Einstufung von Currency-Token lösbar zu sein. Sind Kryptowährungen Tauschmittel, entsteht als erstes die Frage, ob man sie als Geld bezeichnen kann. Minderheitstheorien würden diese Frage positiv beantworten. Token könnten nämlich Geld gleichgestellt werden und damit dem Art 1278 Codice civile unterworfen werden, der Geldschulden in einer Währung regelt, die im Inland nicht gilt. [41] Diese Auffassung wird aber von einem anderen Teil der Lehre aus einem schon erwähnten Grund stark kritisiert: um bei Kryptowährungen von Geld zu reden, sollte sich die Währung auf ein zentralisiertes System stützen. Ist das nicht der Fall, kann man nicht von Geld reden. Auch wenn man eine nicht-zentralisierte Auffassung vertreten würde, könnte man behaupten, dass Kryptowährungen die Hauptfunktionen von Geld – Zahlungsmittel, Wertanlage, Recheneinheit – nicht ausüben können. [42]

Mehrheitstheorien sprechen den Token die Rechtsnatur einer Sache iSv Art 810 Codice civile zu. Im Sinne des Codice civile sind Sachen Dinge, die Gegenstand von Rechten sein können. Da die Körperlichkeit der Sache nicht vorausgesetzt wird, bleibt viel Spielraum in der Auslegung. So ein weiter Begriff umfasst alle Sachenarten. Token könnten dann als Sachen iSv Art 810 Codice civile bezeichnet werden, da sie immaterielle Sachen sind, die aber Gegenstand von Rechtsbeziehungen sein können. [43]

Zum gleichen Ergebnis ist auch die Rechtsprechung gelangt. Das Gericht der ersten Instanz von Florenz – Abteilung Insolvenz - hat sich klar dazu geäußert, indem es in der Entscheidung Nr 18 vom 21. Januar 2019 den Kryptowährungen die Rechtsnatur von Sachen gem. Art 810 Codice civile zuschreibt. [44] Ferner wurde in einem Urteil vom Gericht von Brescia aus dem Vorjahr auch dieses Thema nebensächlich behandelt: bei der Entscheidung hat das Gericht nichts gegen eine Einordnung

der Token als Sachen iSv Art 810 Codice civile. [45] Anzumerken ist aber, dass das oben genannte Gericht in zweiter Instanz eine mögliche Bezeichnung als Geld nicht in Frage stellt, nachdem das sich deutlich dafür gesprochen hat, Kryptowährungen die Rechtsnatur von Sachen zuzuschreiben. [46]

Man sollte aber sich bewusst sein, dass die Einordnung von Kryptowährungen als Sachen nicht ausschließt, sie dem Geld iSv Art 1278 Codice civile gleichzustellen. Beide der oben genannten Urteile vom Gericht von Brescia haben sich dagegen ausgesprochen, dass die Regelung der Erbringung der Einlagen in Natur oder in Form von Forderungen – Art 2364 ff Codice Civile – bei Kryptoeinlagen in einer GmbH Anwendung findet. Man könnte diese Stellungnahme aber kritisieren und daraus die Rechtsnatur von Sachen bzw. eine Gleichstellung der Kryptowährungen mit Geld iSv Art 1278 Codice civile herleiten. Vorausgesetzt, dass die entsprechende Regelung schon für Kryptoeinlagen einer AG Anwendung findet (Art 2343 ff Codice civile), wie es normalerweise bei Geldeinlagen in einer nicht im Inland geltenden Währung der Fall ist. [47]

4.2. Extrinsische Token: *Security*-Token und *Utility*-Token

Für extrinsiche Token ist nach dem deutschen Recht die Bezeichnung als Sache iSv § 90 BGB wegen des Mangels an Körperlichkeit auch zu verneinen. Solche Token repräsentieren Ansprüche auf Vermögensgegenstände. [48] Deren Übertragung ist darauf gezielt, die Berechtigung des Token-Erstellers über das repräsentierte Recht oder den repräsentierten Gegenstand zu verfügen, nachzuweisen. [49] Man könnte denn extrinsische Token den Inhaberschuldverschreibungen - § 793 BGB – gleichstellen. Diese These würde erstens von der Regelung des § 807 BGB gestützt, nach dem die vom Aussteller ausgegebenen Urkunden, in denen der Gläubiger nicht bezeichnet ist und die einen Anspruch gegenüber dem Inhaber repräsentieren, den §§ 793 und 794, 796, 797 entsprechend unterstehen. [50] Zweitens sollte man auf den in der ZPO beinhalteten Urkundenbegriff zurückgreifen. Damit eine Urkunde gem § 371 a ZPO vorliegen kann, sollen kumulativ drei Voraussetzungen erfüllt werden. [51] Die Verkörperung durch übliche Wortzeichen stellt die erste Voraussetzung dar (1). Obwohl es im Fall der Token um Codes und nicht um Wortzeichen geht, könnte man annehmen, dass diese Voraussetzung aufgrund der leichte Nachverfolgbarkeit der Codes vorliegen würde. Eventuelle nachträgliche Änderungen würden auch erkennbar sein. Eine Urkunde soll noch lesbar uzw wahrnehmbar sein (2). Die Erfüllung dieser Voraussetzung könnte auch bejaht werden, indem das Quellcode der Token mit einem maschninenoptimierten Binärcode übereinstimmt. Im Gegensatz dazu kann man leicht annehmen, dass Token nicht jederzeit verfügbar sein können: Verkehrsfähigkeit (3). Was aber sie und das darunter stehende System gewähren können, ist ein hoher Grad an Zuverlässigkeit des Schriftstückes, das schwer fälschbar ist. Ist eine Urkunde fälschungssicher, weist sie eine hohe Beweiskraft iSv § 580 Nr 7b ZPO vor und kann als Beweismittel gelten. [52] Da eine hohe Fälschungssicherheit durch Token erschaffen werden kann, könnte man Token Urkunden gleichstellen. [53] Ferner wie schon erwähnt, hat das Inkrafttreten des eWpG die Möglichkeit eingeführt, elektronische Wertpapiere zu emittieren. Sie werden im § 2 Abs 1 eWpG definiert als Wertpapiere, die durch die Eintragung in ein elektronisches Wertpapierregister entstehen, definiert. Wird das Wertpapierregister von einer zentralen Behörde aufbewahrt wird, redet man von reinen elektronischen Wertpapieren. Ist das Wertpapierregister dezentralisiert aufbewahrt und geführt, ist von Kryptowertpapieren die Rede, wobei sie von dem Oberbegriff elektronischen Wertpapiere umfasst werden. Dass in diesem Fall um Token geht, wird erstens vom Begriff „Krypto-wertpapiere“ ersichtlich. Es fallen dann die Merkmale des Kryptowertpapierregisters auf: dies soll auf einem fälschungssicheren Aufzeichnungssystem geführt werden, in dem Daten in der Zeitfolge protokolliert und gegen unbefugte Löschung sowie nachträgliche Veränderung geschützt gespeichert werden (§ 16 Abs 1 eWpG). Dies wird möglich, wenn man Wertpapiere in Form von Token auf einer Blockchain bzw auf einem anderen DLT-System emittiert. Gemäß § 2 Abs 3 eWpG sollen die Rechtsvorschriften des Sachenrechts auf elektronische Wertpapiere – und damit auch auf Kryptowertpapiere bzw (Security-)Token – angewendet werden. Durch die Einführung einer solchen Sachfiktion unterstehen Kryptowertpapiere den §§ 90 ff BGB. Reine Wertpapiere, uzw Urkunden, die Vermögensrechte verkörpern, fallen schließlich in die Kategorie der (beweglichen) Sachen iSv § 90 BGB.

Aufsichtrechtlich gesehen, können Security-Token funktional Wertpapieren iSv § 2 Abs 1 WpHG gleichgestellt werden, da sie die wirtschaftliche Stellung des Inhabers gewähren, und damit als Finanzinstrumente iSv § 2 Abs 4 Nr 1 WpHG behandelt werden. Im Gegensatz dazu können Utility-Token nicht als Finanzinstrumente iSv § 2 Abs 4 WpHG eingestuft werden, da sie als eine Identifikationsmarke für die Nutzung bestimmter Dienstleistungen zu bezeichnen sind. [54]

Bei Utility-Token neigt die Lehre in Italien dazu, ihnen die Rechtsnatur eines Finanzproduktes zuschreiben. [55] Gemäß Art 1 Abs 1 Lit u) TUF ist jene Finanzinvestition und jenes Finanzinstrument darunter zu verstehen, die in der Sektion C der ersten Anlage zum TUF aufgelistet sind. [56] Eine solche Auffassung wird durch die Berichte der ESMA, European Securities and Markets Authority, und ua der italienischen Behörde Consob, [57] Commissione Nazionale per le Società e la Borsa, unterstützt. In dem ESMA-Hinweis für die Europäische Kommission, Advice: Initial Coin Offerings and Crypto-Assets, [58] wird die Möglichkeit erforscht, Krypto-Assets als Finanzinstrumente zu behandeln, wie sie im Art 4 Abs 1 Nr 15 MiFID II definiert werden. Man redet unter anderem von ‘transferable securities’, ‘money market instruments’, ‘units in

collective investment undertakings' and various derivative instruments. [59] Die ESMA weist in ihrem Bericht darauf hin, dass eine solche Zuschreibung für alle Arten von Krypto-Assets nicht gelten kann. Man muss eine Abgrenzung zwischen Currency-Token und Utility- und Security-Token vornehmen, in dem man nur Security-Token die Rechtsnatur von Finanzinstrumenten zuschreiben könnte. [60] Kehrt man zurück zu der italienischen Rechtsordnung findet man eine Vielzahl von Maßnahmen, die das öffentliche Angebot von im Rahmen von ICOs eben emittierten Token eben aus dem Grund, dass sie nach den Vorschriften von TUF Finanzprodukte sind, verbieten. [61] Was den Security-Token betrifft, könnten diese auch als Finanzprodukte betrachtet werden. Ein Token solcher Art, der ua eine Dienstleistung repräsentieren könnte, könnte dann ein Finanzprodukt darstellen, wenn er dem Markt zum Handel angeboten würde. [62] Das Kriterium der Zuerkennung dieser Einordnung basiert sich dann nicht auf die statische Natur der Token selbst, sondern auf dessen konkreter Nutzung.

5. Schlussfolgerungen

Nach dem deutschen und nach dem italienischen Recht wird der Sachbegriff unterschiedlich abgefasst. Einerseits ist die Voraussetzung der Körperlichkeit erforderlich, damit eine Sache vorliegen kann (§ 90 BGB), andererseits stellt die Eigenschaft, Gegenstand von Rechtsbeziehungen zu sein, die Grundannahme, damit man von Sache im rechtilchen Sinn reden kann (Art 810 Codice civile). Es folgt daraus, dass die Rechtweite des deutschen Sachbegriffes sehr eng im Vergleich zu dem italienischen ist, und dass man das Privatrecht im Allgemeinen erforschen soll, um die Rechtsnatur der Token feststellen zu können.

Als digitale Einheiten können Token – unabhängig von deren Funktion (Currency-, Utility-, oder Security-Token) – wegen mangelnder Körperlichkeit nicht als Sachen iSv § 90 BGB bezeichnet werden. Currency-Token könnten dann als sonstige Rechte gem § 823 BGB rechtlich geschützt werden, wobei solche digitalen Einheiten nicht in sich Schutz finden würden. Gegenstand des Rechtsschutzes würde dann die Nutzung der privaten Schlüssel – und die damit verbundene Einwirkungsmöglichkeit auf fremde Daten – sein. Aus aufsichtsrechtlichem Sinn werden sie als Rechnungseinheiten bezeichnet, wobei diese Auffassung noch umstritten bleibt. Was im Allgemeinen extrinsische Token betrifft, uzw Token die Ansprüche auf Vermögensgegenständen repräsentieren, werden sie Inhaberwertpapieren iSv § 793 BGB gleichgestellt und damit als Urkunde gem § 371b ZPO bezeichnet. Obwohl dann nicht alle Voraussetzungen vorliegen, damit eine solche Einstufung problemlos angenommen werden kann, gewähren Token einen hohen Grad an Fälschungssicherheit, sodass diese Eigenschaft in sich reichen würde, um Token als sicheres Beweismittel – und damit als Urkunde – zu behandeln.

Dagegen könnte man nach italienischem Recht Token die Rechtsnatur einer Sache iSv Art 810 Codice civile zuschreiben. Großteil der Lehre hat sich dafür ausgesprochen, Currency-Token als Sachen zu behandeln, da sie nur als eine, auf einem DLT-System entstehende Einheit, (zentralisiert emittiertem) Geld nicht gleichgestellt werden könnten. Solche Auffassung wird auch von der bisherigen Rechtsprechung geteilt. Ihrerseits werden Utility- und Security-Token mit Unterstützung von nationalen und europäischen Behörden als Finanzprodukte, wie sie im TUF definiert und geregelt werden, bezeichnet. Eben aus dem Grund, dass dem im Art 810 Codice civile beinhaltete Sachbegriff eine wirtschaftlich-soziale Bedeutung zugemessen wird, umfasst der Begriff verschiedene Arten von Sachen, wobei auch Finanzprodukte – als Gegenstand von Rechtsbeziehungen – hineinbezogen werden können. Würde man dann Token als Finanzprodukte bezeichnen und sie den TUF-Vorschriften unterwerfen, würde man sowieso von Sachen iSv Art 810 Codice civile reden.

Zivilrechtlich gesehen, kommt man letztendlich zu unterschiedlichen Antworten auf die Frage, ob Token Sachen im rechtlichen Sinn sein können, da eben die Sachbegriffe selbst unterschiedlich von den jeweiligen Gesetzgebern ausgestaltet worden sind. Nennenswert ist aber, dass der deutsche Gesetzgeber im eWpG eine Sachfiktion (§2 Abs 3 eWpG) eingeführt hat, die im Einklang mit der Auffassung, Token als Urkunden zu behandeln, zu sein schein. Eine solche Fiktion wäre dann nach italienischem Recht nicht notwendig.

Es wird dann sinnvoll zu beobachten, wie sich die Einführung von Kryptowertpapieren in dem deutschen Rechtssystem weiterentwickeln wird; wann und ob der italienische Gesetzgeber konkrete Schritte in Richtung Blockchain und DLT-Systeme machen wird, und vor allem auch wie die Europäische Union mit dieser Thematik weiter umgehen wird.

6. Literaturverzeichnis

[1] Eggen M., Glarner A., Hess M., Icangelo S., Stengel C., Weber R.: Positionspapier zur rechtliche Einordnung von ICOs, Blockchain Taskforce (2018), 3-4. URL: https://www.ibr.unibe.ch/unibe/portal/fak_rechtwis/c_dep_private/inst_bankrecht/content/e7718/e675035/e675547/Positionspapier_Legal_ger.pdf (abgerufen am 31.08.2021).

[2] Omlor S., Link M.: Kryptowährungen und Token, 1. Aufl. (2021), 260 ff.

[3] FINMA: Wegleitung für Unterstellungsanfragen betreffend Initial Coin Offerings (ICOs) (2018), 3. URL: https://www.finma.ch/de/news/2018/02/20180216-mm-ico-wegleitung/ (abgerufen am 31.08.2021). Kumpan C.: WpHG §2 Begriffsbestimmungen, Kapitalmarktsrechtskommentar in Schark/Zimmer, 5. Aufl. (2020), Rn 81-86.

[4] Möllenkamp S./Shmatenko L.: Blockchain und Kryptowährungen, Handbuch Multimedia-Recht, 56. Aufl (2021), Rn 29-31.

[5] Stresemann C.: § 90, MüKo BGB, 8. Aufl. (2018), Rn 1-3.
[6] Biondi B.: I beni, Trattato di diritto civile Vassalli, IV (1956), 36.
[7] De Nova G.: I nuovi beni come categorie giuridiche, Dalle res alle new properties (1991), 15.
[8] Pugliatti S.: Beni (teoria generale) Enciclopedia del diritto, V (1959), 173.
[9] Bondi B.: Cosa (diritto civile), Novissimo digesto italiano, IV (1968), 1009 ff.
[10] Scozzafava O.T.: Dei beni, Commentario Schlesinger sub Art 810 c.c. (1999), 6. *Contra* Costantino M.: La proprietà in generale, Trattato Rescigno, VII (1982), 18.
[11] Barcellona P.: Diritto privato e società moderna (1996), 229.
[12] Messinetti D.: Oggetto dei diritti, Enciclopedia del diritto, XXIX (1979), 810.
[13] Pugliatti S.: Interesse pubblico e interesse privato nel diritto di proprietà, La proprietà nel nuovo diritto (1964), 3 ff.
[14] Pugliatti S.: *supra 8*, 173. Maiorca C.: Beni, Enciclopedia giuridica, V (1988), 146.
[15] Fritzsche J: § 90, BeckOK BGB, 59. Ed. (2021), Rn 5-9.
[16] Pardolesi R.: Le energie, Trattato di Diritto Privato Rescigno, VII (2005), 26 ff.
[17] Fritzsche J: § 90, *supra 15*, Rn 18.
[18] Messinetti D.: Oggettività giuridica delle cose incorporali (1970), 205; Are M.: Beni immateriali, Enciclopedia del diritto, V (1959), 244.
[19] Rodotà S.: Note critiche in tema di proprietà, Rivista trimestrale di diritto e procedura civile (1960), 1315.
[20] Art 2575 Codice civile: *Gegenstand des Urheberrechts sind unabhängig von der Art und Weise oder der Form des Ausdrucks geistige Werke schöpferischer Natur, die den Wissenschaften, der Literatur, der Musik, der bildenden Künsten, der Architektur, dem Theater und dem Filmschaffen zuzwurechnen sind*. Übersetzt von: Bauer M.W., Eccher B., König J., Kreuzwer J., Zanon H.
[21] Chiarolla M.: Diritto d'autore: la prima volta delle banche dati (in Italia), Foro.it, I (1990), 2674-2678.
[22] Carnevali U.: Sulla tutela giuridica del software, Quadrimestre (1984), 254; Alpa G., Ferri B.: Profili della tutela giuridica dei programmi per elaboratore in Italia, I programmi per elaboratore – Tutela degli utenti e delle software house (1988), 9-35.
[23] Cian M.: La dematerializzazione degli strumenti finanziari, Banca, Borsa e Titoli di credito, 6 (2007).
[24] *Ibidem*.
[25] Stresemann C.: § 90, *supra 5*, Rn 11-13.
[26] Fritzsche J: § 90, *supra 15*, Rn 12.
[27] Onza M., Salamone L.: Prodotti, strumenti finanziari, valori mobiliari, Banca Borsa Titoli di credito, 5 (2009), 567 ff.
[28] Richtlinie Nr 843/2018 des Europäischen Parlaments und des Rates v 30.05.2018 zur Änderung der Richtlinie (EU) 2015/849 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung und zur Änderung der Richtlinien 2009/138/EG und 2013/36/EU ABl 2018 Nr L 156 43 – 74.
[29] Möllenkamp S./Shmatenko L.: *supra 4*, Rn 40. Cian M.: La criptovaluta – Alle radici dell'idea giuridica di denaro attraverso la tecnologia: spunti preliminari, Banca Borsa Titoli di credito, 3 (2019), 315 ff.
[30] Schlund A./Pongratz H.: Distributed-Ledger-Technologie und Kryptowährungen eine rechtliche Betrachtung, DStR (2018), 598 ff.
[31] Möllenkamp S./Shmatenko L.: *supra 4*, Rn 32.
[32] *Ibidem.*
[33] Zahrte K.: Müko HGB, 4. Aufl. (2019), Rn 374-377.
[34] Möllenkamp S./Shmatenko L.: *supra 4*, Rn 32.
[35] Schlund A./Pongratz H.: *supra 30.*
[36] Möllenkamp S./Shmatenko L.: *supra 4*, Rn 32.
[37] Möllenkamp S./Shmatenko L.: *supra 4*, Rn 37.
[38] Kumpan C.: *supra 3.*
[39] KG Berlin 25.09.2018 – (4) 161 Ss 28/18 (35/18), WM 2083 (2018).
[40] Kumpan C.: *supra 3.*
[41] Art 1278 Codice civile: *Ist der geschuldete Betrag in einer Währung ausgedrückt, die im Inland nicht gilt, so ist der Schuldner befugt zu dem am Tag der Fälligkeit am festgesetzten Zahlungsort bestehenden Wechselkurs zu zahlen.* Übersetzt von: Bauer M.W., Eccher B., König J., Kreuzwer J., Zanon H.
[42] Cian M.: *supra 29.* Lemme G., Peluso S.: Criptomoneta e distacco dalla moneta legale: il caso bitcoin, Rivista di diritto bancario, IV (2016), 381 ff.
[43] Cian M.: *supra 29*, 339. Donadio G.: Dalla "nota di banco" all'informazione via Blockchain, profili civilistici e problemi applicativi della criptovaluta, Giustizia civile, 7 (2020), 179.
[44] Tribunale di Firenze, sezione fallimentare, 21.01.2019 – 18, Banca Borsa Titoli di credito 3 (2021), 385: *Le criptovalute, dunque, possono essere considerate "beni" ai sensi dell'art. 810 c.c., in quanto oggetto di diritti*.
[45] Tribunale di Brescia, sezione spec. impresa, 18.07.2019 – 7556, Giurisprudenza commerciale, 4 II (2020), 883.
[46] Corte appello Brescia, sez. I, 30.10.2018, Banca Borsa Titoli di Credito, 6 II (2019) 736.
[47] Rubino De Ritis M.: Conferimenti di criptomonete in società a responsabilità limitata, La società a responsabilità limitata: un modello transtipico alla prova del Codice della Crisi (2020).
[48] Siehe Punkt 2.1.
[49] Möllenkamp S./Shmatenko L.: *supra 4*, Rn 47.
[50] Möllenkamp S./Shmatenko L.: *supra 4*, Rn 48.
[51] Kaulartz M., Matzke R.: Die Tokenisierung des Rechts, NJW (2018), 3278.
[52] Schreiber K.: § 415, MüKo ZPO, 3. Aufl. (2008), Rn 5.
[53] Matzke R.: Rechtliche Einordnung der Emission von

tokenisierten Schuldverschreibungen in Deutschland, Rechtshandbuch Legal Tech, 2. Aufl. (2021), Rn 29 ff.

[54] Kumpan C.: *supra 3.*

[55] Annunziata F.: Speak, if You Can: What Are You? An Alternative Approach to The Qualification of Tokens and Initial Coin Offerings, Bocconi Legal Studies Reaserch Paper Series, 2636561 (2019), 37 ff.; Franza E.: Nuove modalità di finanziamento: la blockchain per le startup e piccolo e medie imprese. Rischi e possibili vantaggi, www.dirittobancario.it (2019).

[56] Vgl. Punkt 2.5.

[57] Vgl. Raffaele F.: The recent view of the Italian Market Authority (Consob) on Initial Coin Offerings (ICOs) and crypto assets, Diritto del commercio internazionale, 3 (2020), 799.

[58] ESMA: Advice, Initial Coin Offerings and Crypto-Assets, 09.01.2019. URL: https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf (abgerufen am 31.08.2021).

[59] ESMA, *supra 58,* 19.

[60] ESMA, *supra 58,* 19: *The results reflected below should not be extrapolated to the entire crypto-asset universe. In particular, payment-type crypto-assets, like the Bitcoin which accounts for around half of the total market value of crypto-assets, are not represented in the survey sample*.

[61] Vgl. ua Consob Berichte Nr 20944/2019, 20845/2019, 20843/2019, 29844/2019.

[62] Gitti G.: Emissione e circolazione di criptoattività tra tipicità e atipicità nei nuovi mercati finanziari, Banca, borsa, titoli di credito, I (2020), 38; Sandei C.: Initial Coin Offerings e appello al pubblico risparmio, Diritto del Fintech, (2020).

Decentralised Finance: Dezentrale Kreditplattformen – (ver)sicher(t)?

Stefan Mitzlaff, Lucas Johns
Deutsche Bundesbank, Wilhelm-Epstein-Straße 14, 60431 Frankfurt am Main & Hochschule Mittweida, Technikumplatz 17, 09648 Mittweida

Dezentrale Kreditplattformen ermöglichen Nutzern die Aufnahme sowie die Bereitstellung von Liquidität in Form von Krypto-Token gegen Verzinsung. Dieser Teil des dynamisch wachsenden Bereichs dezentraler Anwendungen erweist sich zwar als sehr innovativ, birgt jedoch auch Risiken. Dazu zählen insbesondere Kreditrisiken, Liquiditätsrisiken, Marktrisiken und operationelle Risiken. Um diesen Risiken entgegenzuwirken existieren vereinzelt Absicherungsmechanismen. Diese Mechanismen haben durchaus Potenzial die genannten Risiken zu verringern, wenngleich dadurch keine vollumfängliche Risikobewältigung erfolgen kann. Somit verbleiben immer Restrisiken, die letztlich vor allem von den Nutzern zu tragen sind.

1. Einleitung

Der Bereich Decentralised Finance (DeFi) entwickelt sich dynamisch und bringt neue Formen von Finanzdienstleistungen und -produkten hervor. So entstehen etwa Anwendungsfälle in Verbindung mit Krypto-Token, die Ähnlichkeiten zu Leistungen des konventionellen Finanzsystems aufweisen, wie beispielsweise dem Kredit- und Einlagengeschäft oder Versicherungen. Erbracht werden diese Leistungen von sogenannten dezentralen Anwendungen (Decentralised Applications, dApps).

Dezentrale Anwendungen basieren auf einem Distributed Ledger – üblicherweise in Form einer Blockchain – und auf Smart Contracts. Während die Blockchain als Transaktionssystem und -register dient, spezifizieren die darauf aufbauenden Smart Contracts die Anwendungslogik, also welche Bedingungen bei Transaktionen zu prüfen sind und welche Aktivitäten daraus folgen. So können komplexe, aufeinander aufbauende Geschäftsfälle automatisch abgewickelt werden. Im Extremfall können ganze Prozessketten, ähnlich zu Abläufen in Unternehmen, autonom implementiert werden. Der Begriff Dezentralität findet seinen Ursprung dabei insbesondere in dezentralen Prozessen zum Betrieb und zur Weiterentwicklung der Anwendungen [1]. Abbildung 1 zeigt eine Einordnung von dezentralen Anwendungen aus technischer Sicht.

Obwohl sich dezentrale Anwendungen aus technischer Sicht ähneln, können sie unterschiedliche Geschäftsfelder abdecken. Dezentrale Anwendungen etwa, denen Netzwerkakteure Krypto-Token gegen eine Verzinsung bereitstellen und die entsprechende Kredite herausgeben, werden auch als dezentrale Kreditplattformen bezeichnet. Gemessen an der Liquidität, die von Netzwerkakteuren in dezentralen Anwendungen hinterlegt wird, zählen Aave und Compound zu den größten Vertretern solcher Plattformen [2].

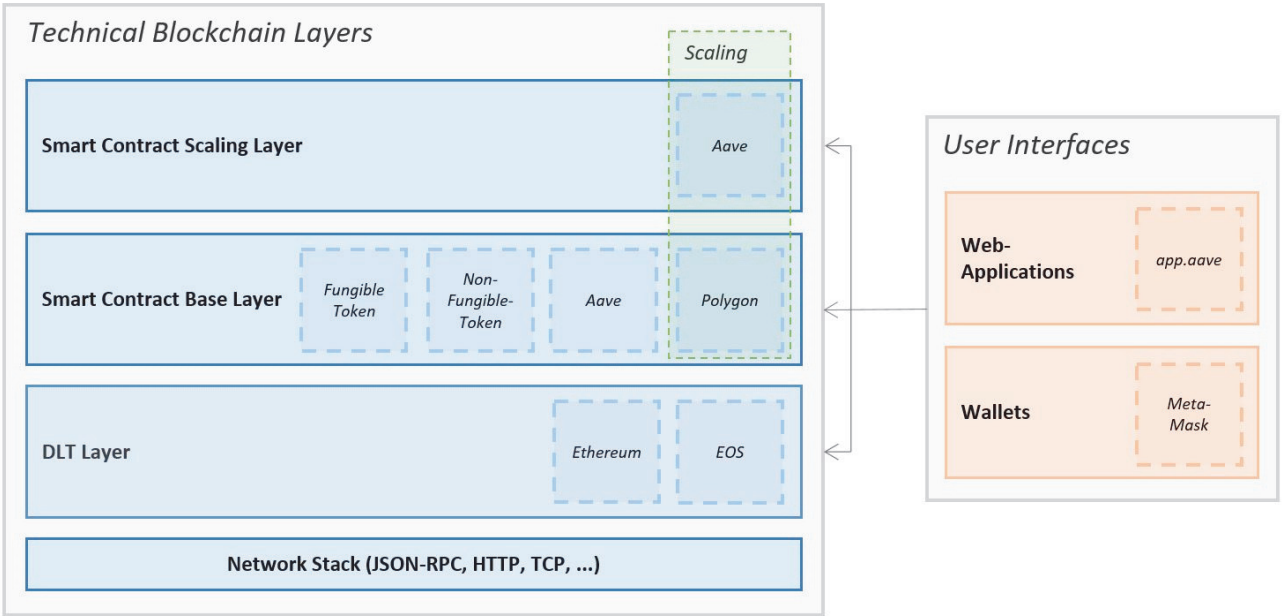

Abbildung 1: Stilisierte technische Darstellung dezentraler Anwendungen, Quelle: Eigene Darstellung. Beachte: Einträge mit gestrichelter Umrandung stellen Beispiele dar.

Die Nutzung dezentraler Anwendungen ist mit verschiedenen Risiken verbunden, die durch unklare oder fehlende Regulierungsanforderungen sowie die mangelnde Einhaltung ebendieser zum Teil verstärkt werden. Dabei ist insbesondere das Kreditrisiko hervorzuheben, das auch im konventionellen Finanzsystem eine der bedeutendsten Risikoarten darstellt. Kreditrisiken in Verbindung mit dezentralen Anwendungen können dadurch auftreten, dass Netzwerkakteure Anwendungen, etwa dezentralen Kreditplattformen Liquidität in Form von Krypto-Token bereitstellen und diese anschließend an andere Netzwerkakteure verliehen wird. Der genaue rechtliche Status dezentraler Anwendungen ist bislang ungeklärt, sodass auch Fragen der Haftung ungewiss sind. Entsprechend übertragen sich Kreditrisiken, die eigentlich durch die Anwendungen eingegangen werden, implizit auf deren Nutzer, die den Anwendungen Liquidität bereitstellen.

Der Artikel zielt darauf ab, zu einem besseren Verständnis der Risiken beizutragen, die mit der Nutzung dezentraler Kreditplattformen verbunden sind. Dabei spielen neben den Kreditrisiken auch Liquiditätsrisiken, Marktrisiken und operationellen Risiken eine Rolle. Diese vier Risikokategorien werden gemäß den Mindestanforderungen an das Risikomanagement (MaRisk) auch im Rahmen der Ausgestaltung des Risikomanagements von Kreditinstituten als wesentlich angesehen, weshalb sich der Artikel auf diese Risikoauswahl beschränkt [3]. Zudem wird aufgezeigt, welche anwendungsinhärenten sowie externen Absicherungsmechanismen gegen diese Risiken existieren.

Dezentrale Anwendungen befinden sich in einem frühen Entwicklungsstadium und entwickeln sich dynamisch weiter. Ein besseres Verständnis der Risiken, die innerhalb des Ökosystems dezentraler Anwendungen existieren, könnte zu einer besseren Regulierung dieses Bereiches beitragen. Denn eine effektive Regulierung könnte das Vertrauen in den Bereich stärken, wenngleich die Regulierung dabei vor besonderen Herausforderungen steht.

2. Arten dezentraler Kreditvergabe

Dezentrale Kreditplattformen ermöglichen Nutzern die Aufnahme sowie die Bereitstellung von Liquidität in Form von Krypto-Token gegen Verzinsung. Anders als Kreditinstitute betreiben sie dabei allerdings keine Geldschöpfung. Das klassische Beispiel für die Buchgeldschöpfung wäre die Kreditgewährung einer Bank an eine Nichtbank, bei der der Kreditbetrag auf einem Konto des Kreditnehmers gutgeschrieben wird. Auf der Bankbilanz entstehen eine Forderung und eine Verbindlichkeit, sodass es zu einer Bilanzverlängerung kommt. Im Ergebnis wurde Buchgeld geschaffen [4]. Dezentrale Kreditplattformen reichen hingegen lediglich Krypto-Token aus, die ihnen zuvor bereitgestellt wurden, sodass im Rahmen der Kreditvergabe keine neuen Krypto-Token geschaffen werden.

Dabei vermitteln dezentrale Kreditplattformen üblicherweise nicht direkt zwischen Kreditgebern und Kreditnehmern, wie es etwa bei Plattformen für Peer-To-Peer-Kredite der Fall ist. Stattdessen basieren dezentrale Kreditplattformen in der Regel auf sogenannten Lending Pools [5]. Eine direkte Kreditvergabe zwischen einzelnen Netzwerkakteuren kann jedoch etwa im Zusammenhang mit der Besicherung sogenannter Non Fungible Token (NFT) erfolgen. Dabei hinterlegt ein Nutzer Krypto-Token in einem Smart Contract und erhält im Gegenzug individuelle Kreditangebote von anderen Nutzern [6]. Nutzer können dabei also nicht unmittelbar ein Geschäft abschließen, sondern müssen zunächst immer erst einen geeigneten Kontrahenten finden. Dadurch ist die direkte Kreditvergabe zwischen Netzwerkakteuren im Vergleich zur Kreditvergabe mittels Lending Pools üblicherweise umständlicher und weniger liquide, weshalb sie seltener zur Anwendung kommt [7]. Lending Pools werden, wie in Abbildung 2 dargestellt, mittels Smart Contracts implementiert. Netzwerkakteure können den Pools Liquidität in Form von Krypto-Token bereitstellen. Im Gegenzug erhalten

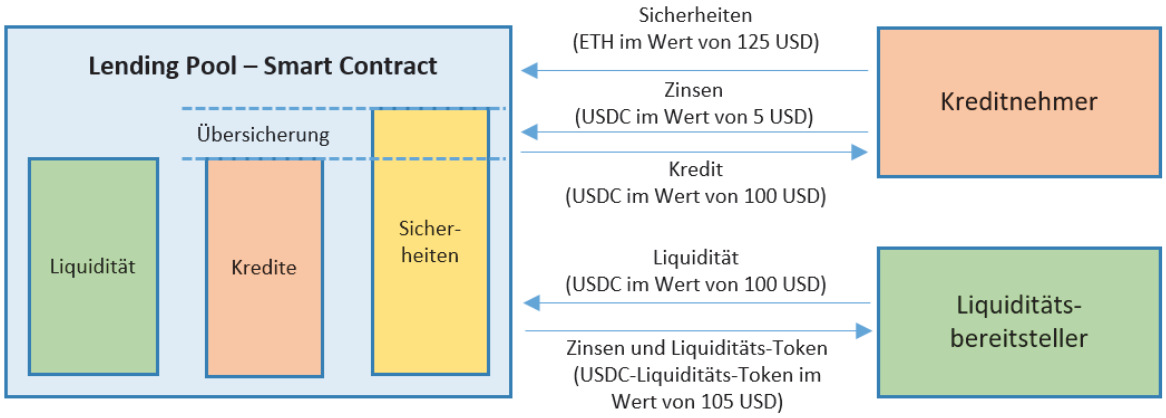

Abbildung 2: Exemplarische Funktionsweise von Lending Pools am Beispiel USD Coin (USDC), Quelle: Eigene Darstellung.

sie sogenannte Liquiditäts-Token, die ihre eingebrachte Liquidität repräsentieren und über welche die Zuteilung der Verzinsung abgebildet wird. Durch Rückgabe der Liquiditäts-Token kann die ursprünglich eingebrachte Liquidität wieder entnommen werden. Kreditnachfrager können dem Pool Liquidität entnehmen, sofern sie entsprechende Sicherheiten bereitstellen. Um einen Anreiz zur Rückzahlung zu schaffen und aufgrund der hohen Volatilität und Illiquidität vieler als Sicherheit verwendeter Krypto-Token müssen Kreditnehmer ihre Verbindlichkeiten oftmals überbesichern. Wie viel Kredit man erhält, hängt von der Art der Sicherheit ab [8]. Die Sicherheiten werden in einem Smart Contract hinterlegt und wieder freigegeben sobald der Kredit getilgt wurde [9, 10].

Unbesicherte Kredite können in Form sogenannter Flash Loans vergeben werden. Diese müssen innerhalb desselben Blockchain-Blocks zurückbezahlt werden, andernfalls erfolgt eine Rückabwicklung bzw. Nicht-Ausführung des gesamten Geschäfts. Dies wird durch die sequentielle Verarbeitung von Transaktionen der zugrundeliegenden Blockchain ermöglicht. Dabei wird ein Smart Contract verwendet, über welchen ein Kredit aufgenommen wird. Mit dieser Liquidität werden dann Transaktionen ausgeführt und der Kredit plus Zinsen im Anschluss automatisch zurückgezahlt. Diese Schritte müssen gebündelt und innerhalb eines Blockintervalls, also dem Zeitfenster zwischen der Erstellung zweier Blöcke, erfolgen. Ohne Rückzahlung würde eine Rückabwicklung sämtlicher vorher ausgeführter Schritte erfolgen, sodass auch die Kreditaufnahme nicht auf die Blockchain geschrieben wird [9, 11].

3. Mögliche Gründe für Kreditaufnahme

Die Vergabe von Krediten durch dezentrale Kreditplattformen grenzt sich aufgrund der Pseudo-Anonymität der Netzwerkakteure und den daraus resultierenden Sicherheitsanforderungen von traditionellen Bankkrediten deutlich ab. Durch die Übersicherung mit äquivalenten Vermögensgegenständen – in Form von Krypto-Token – oder der sehr kurzfristigen Laufzeit einiger Kreditarten gerät die Motivation eines Kreditnehmers sich Liquidität zu Konsum- oder Investitionszwecken zu beschaffen in den Hintergrund. Vielmehr dürften andere Gründe für eine Kreditaufnahme bei dezentralen Kreditplattformen sprechen, wie etwa Belohnungen, Leveraging, Arbitrage und dolose Handlungen.

Belohnungen: Anwendungen belohnen Nutzer – sowohl Liquiditätsbereitsteller als auch Kreditnehmer – zum Teil mit Governance-Token [7,12]. Governance-Token können eingesetzt werden, um dezentrale Governance-Prozesse mithilfe von kollektiven Abstimmungsverfahren abzubilden. Einige Anwendungen schütten zudem Erträge an die Inhaber der Governance-Token aus – vergleichbar mit einer Dividende. Governance-Token können dann sowohl zum Zweck der Stimmrechtsausübung als auch mit Ertragsaussichten gehalten oder veräußert werden. Die Nutzung einer dezentralen Kreditplattform könnte demnach mit der Erwartung auf Belohnungen in Form von Governance-Token einhergehen (sog. Liquidity Mining), und erhält dadurch einen Selbstzweck, da das eigentliche Kreditgeschäft von eher nachrangiger Bedeutung ist.

Leveraging: Die besicherte Kreditaufnahme kann beispielsweise dem Hebeln eigener Positionen dienen. Hält man Krypto-Token etwa in der Erwartung steigender Kurse, können diese als Kreditsicherheit verwendet werden [7, 12]. Wird der Kredit nun in Form von Stablecoins aufgenommen, können diese gegen volatilere Krypto-Token mit angenommenen Kurspotenzial getauscht werden. Dieser Anwendungsfall deckt sich damit, dass Kredite üblicherweise in Form von Stablecoins aufgenommen werden, wohingegen volatilere Krypto-Token eher als Kreditsicherheit verwendet werden [8]. Steigen die erworbenen Krypto-Token im Wert, kann der Kreditnehmer einen Gewinn erzielen, sofern der Wertzuwachs größer ist als der Zinsaufwand des Kredites zuzüglich Transaktionskosten [13]. Die aufgenommenen Krypto-Token könnten ihrerseits als Kreditsicherheit verwendet werden. Derartige Strategien werden in Verbindung mit dem Erzielen von Belohnungen auch als Yield Farming bezeichnet, bei dem die Nutzer das vorrangige Ziel der Gewinnmaximierung verfolgen [14].

Arbitrage: Flash Loans eignen sich für Arbitrage-Zwecke, etwa durch das monetarisieren von Preisunterschieden an verschiedenen dezentralen Handelsplattformen [13, 15]. Dabei würde in einem ersten Schritt ein Flash Loan aufgenommen werden. Die aufgenommen Krypto-Token könnten dann an einer dezentralen Handelsplattform veräußert werden. Idealerweise können die Krypto-Token dann an einer anderen dezentralen Handelsplattform zu einem niedrigeren Preis zurückgekauft werden. Dadurch könnten einerseits die ursprünglich geliehenen Krypto-Token im Rahmen des Flash Loans sowie dafür anfallende Zinsen zurückgegeben werden. Andererseits ergäbe sich ein Gewinn sofern die Transaktionskosten des Vorgangs niedriger ausfallen als der Handelsgewinn.

Dolose Handlungen: Flash Loans können beispielsweise für schädliche Attacken auf dezentrale Anwendungen eingesetzt werden, etwa durch den Erwerb von Governance-Token und anschließender Änderung des Programmcodes der jeweiligen Anwendung zum eigenen Vorteil [5, 14, 15].

4. Risiken und Absicherungsmechanismen

Die von dezentralen Kreditplattformen angebotenen Leistungen ähneln in Ansätzen dem Kredit- und Einlagegeschäft von konventionellen Banken, inklusive den damit einhergehenden Risiken. Diese sind zwar vergleichbar mit den Risiken, denen auch Kreditinstitute im Rahmen ihres Risikomanagements ausgesetzt sind.

Allerdings sind im Fall von dezentralen Kreditplattformen insbesondere die Nutzer von den Risiken betroffen, während die Plattformen selbst keinerlei Haftung unterliegen. Zur Verringerung der Risiken existieren vereinzelte anwendungsinhärente Absicherungsmechanismen und externe Versicherungen.

4.1 Kreditrisiken

Netzwerkakteure, die Lending Pools Liquidität bereitstellen, sind grundsätzlich dem Risiko ausgesetzt, dass sie die von ihnen eingereichte Liquidität zuzüglich der zustehenden Zinsen nicht vollumfänglich wiedererhalten. Dieses Risiko vergrößert sich insbesondere dadurch, dass die Lending Pools die Liquidität ohne Bonitätsprüfung an pseudoanonyme Netzwerkakteure verleihen. Ohne adäquate Absicherungsmechanismen hätten Kreditnehmer kaum einen Anreiz geliehene Krypto-Token zurückzuzahlen. Zudem achten dezentrale Kreditplattformen nicht auf Risikokonzentrationen, etwa mit Hilfe von kreditnehmerbezogenen Limiten wie es beispielsweise für Banken im Rahmen der MaRisk vorgeschrieben ist. Abbildung 3 zeigt am Beispiel von Aave mehrere aufeinanderfolgende Mechanismen, die Liquiditätsbereitsteller vor Verlusten ihrer Krypto-Token schützen sollen. Diese Kaskade besteht aus vier wesentlichen Stufen:

1) Um die Rückzahlung von Krediten trotz der Pseudo-Anonymität der Netzwerkakteure und ohne vorherige Bonitätsprüfung zu gewährleisten, müssen Kreditnehmer diese mit Krypto-Token besichern. Damit Wertschwankungen der Sicherheiten keinen direkten Einfluss auf den Wert eines Lending Pools haben und um einen möglichst hohen Anreiz zur Rückzahlung des Kredites zu schaffen erfolgt die Besicherung üblicherweise zu Quoten von mehr als 100%. Sinkt der Wert der Sicherheiten, muss der Kreditnehmer Sicherheiten nachschießen, um das Recht zur Auslösung seiner Sicherheiten zu erhalten [8, 9, 11].

2) Schießt der Kreditnehmer keine Sicherheiten nach, sodass diese anschließend unter einen bestimmten Schwellenwert fallen, erhalten sogenannte Liquidatoren die Möglichkeit die Sicherheiten mit einem Abschlag zu erwerben. Dieser Mechanismus soll eine Unterdeckung des Lending Pools verhindern, sofern Kreditnehmer keine ausreichende Besicherung mehr bereitstellen [12].

3) Durch einen plötzlichen Wertverfall von Sicherheiten kann es dazu kommen, dass etwaige Liquidierungsereignisse nicht genügend Liquididatoren finden und es dadurch zur Unterdeckung eines Lending-Pools kommt [12]. Aave sieht in einem solchen Fall ex ante einen Ausgleich für die Liquiditätsbereitsteller durch ein sogenanntes Safety Module vor – vergleichbar mit einem Verlustabsorptionspuffer. Diesem können AAVE-Token gegen eine Verzinsung bereitgestellt werden. Dabei handelt es sich um die Governance-Token der dezentralen Kreditplattform Aave. Die Token können mit einer Frist von sieben Tagen wieder aus dem Safety Module entnommen werden – was etwa mit der Kündigungsfrist von Genossenschaftsanteilen verglichen werden kann, wenngleich diese üblicherweise deutlich länger ist. Die Unterdeckung eines Lending Pools würde durch die Aave Governance festgestellt werden, woraufhin die Liquidierung der Token des Safety Module angestoßen werden würde. Die AAVE-Token würden dann gegen die entsprechenden Krypto-Token verkauft werden, bei deren Lending Pool es zu einer Unterdeckung gekommen ist. Der Verkaufserlös würde dem Lending Pool solange zugeführt werden, bis die Unterdeckung ausgeglichen ist [16].

4) Reichen die Erlöse des Safety Module nicht aus, kann ex post eine zusätzliche Reserve aktiviert werden, um die Unterdeckung auszugleichen. Zu diesem Zweck kann die Aave Governance die Ausgabe zusätzliche AAVE-Token beschließen und diese veräußern [16]. Deren Verkaufserlös wiederum kann zum Ausgleich der Unterdeckung verwendet werden. Gleichzeitig würde jedoch der Kurs der AAVE-Token verwässert werden: Der Anteil der Alt-Inhaber verringert sich hierdurch und es kommt effektiv zu einem Verlust – vergleichbar mit einer Gläubigerbeteiligung. Dabei ist es im Vorfeld jedoch nicht klar, ob die neu geschaffenen AAVE-Token ausreichend Abnehmer finden werden, um die Liquiditätsbereitsteller zu entschädigen.

Grundsätzlich sollten anwendungsinhärente Absicherungsmechanismen die Nutzung einer Anwendung im Vergleich zu anderen – ohne entsprechende Mechanismen – verteuern. So sind die Zinsen, die Governance-Token Inhaber für die Speisung eines Verlustabsorptionspuffers erhalten, ceteris paribus letztlich von den Nutzern in Form höherer Kreditzinsen, niedrigerer Einlagenzinsen oder zusätzlicher Gebühren zu tragen. Zudem dürften Governance-Token-Inhaber die Gefahren einer Gläubigerbeteiligung in ihre Renditekalkulation einpreisen und sich entsprechend höhere Gewinne auszahlen, was ebenfalls zulasten der Nutzer gehen dürfte. Fehlende anwendungsinhärente Absicherungsmechanismen würden für die Liquiditätsbereitsteller jedoch mit größeren Kreditrisiken einhergehen, was wiederum in die individuelle Renditekalkulation einbezogen werden müsste.

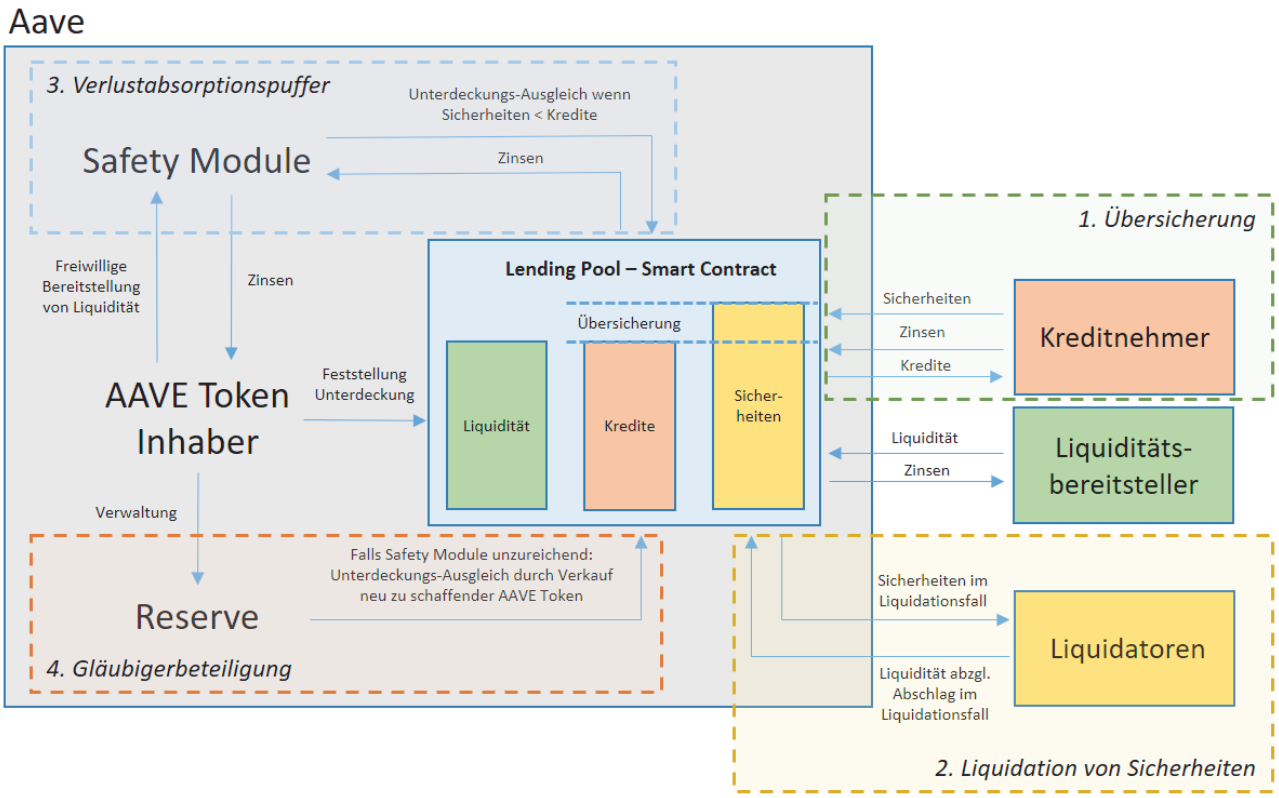

Abbildung 3: Anwendungsinhärente Absicherungsmechanismen am Beispiel Aave, Quelle: Eigene Darstellung nach [9, 11, 16].

4.2 Liquiditätsrisiken

Liquiditätsrisiken können auftreten, wenn Netzwerkakteure einer Plattform Liquidität bereitstellen und sie diese nicht zu einem gewünschten Zeitpunkt wieder abrufen können. So können Lending Pools illiquide werden, sobald die Summe aller ausgegebenen Kredite der Summe der eingereichten Liquidität entspricht. In diesem Fall müssten Netzwerkakteure, die ihre Liquidität entnehmen wollen, darauf warten, dass Kredite getilgt werden oder weitere Netzwerkakteure dem Lending Pool Liquidität bereitstellen. Die Gefahr der Illiquidität eines Lending Pools soll durch variable Zinssätze verringert werden [17, 18]. Sinkt die verfügbare Liquidität im Pool, steigen die Einlagen- und Kreditzinsen, sowohl für Neu- als auch Bestandsgeschäft. Einleger haben dadurch einen größeren Anreiz Liquidität bereitzustellen, wohingegen Kreditnehmer einen größeren Anreiz haben, ihre Kredite zu tilgen. Selbiges Prinzip gilt in umgekehrter Logik für den Fall eines Überangebots an Liquidität [5, 18]. Die Funktion, derer die Zinssätze dabei folgen, kann verschiedene Formen annehmen. Aave und Compound etwa setzen auf Funktionen mit linear ansteigendem Verlauf und „Knickstelle“, ab der die Funktion deutlich steiler verläuft. Wesentliche Einflussgröße ist dabei die Utilisation Rate *U*, welche das Verhältnis aus Krediten *L* und Einlagen *D* für einen bestimmten Lending Pool angibt [18]:

$$U = \frac{L}{D}$$

Sodass sich der Kreditzins i_b wie folgt ergeben kann:

$$i_b = \begin{cases} \alpha + \beta U & wenn\ U < U_{optimal} \\ \alpha + \beta U_{optimal} + \gamma(U - U_{optimal}) & wenn\ U \geq U_{optimal} \end{cases}$$

wobei α eine Konstante ist und β die Steigung des Zinses im Verhältnis zur Utilisation Rate widergibt. Überschreitet U ein gewisses Optimum am Punkt $U_{optimal}$ erzeugt γ einen Multiplikator-Effekt, der zu einem steileren Anstieg führt. $U_{optimal}$ wird üblicherweise für jeden Lending Pool individuell festgelegt und kann beispielsweise einem Verlauf wie in Abbildung 4 annehmen.

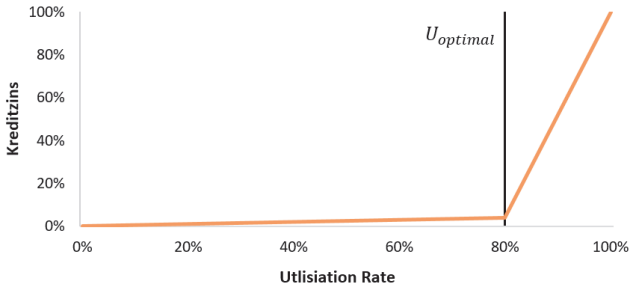

Abbildung 4: Exemplarische Kreditzinskurve mit Knickstelle, Quelle: Eigene Darstellung nach [18].

Darüber hinaus existieren Anwendungen, deren Zinssätze linearen oder nichtlinearen Verläufen folgen. Unabhängig von der Art der Zinssatzermittlung kann sich dieses Anreizsystem jedoch als unzureichend erweisen, etwa im Fall von abrupten

Liquiditätsabflüssen – vergleichbar mit einem Bank Run. Nutzer sind dann möglicherweise nicht mehr dazu bereit Liquidität trotz hoher Verzinsung bereitzustellen. Demnach kann das Risiko der Illiquidität von Lending Pools zwar verringert, aber nicht ausgeschlossen werden [5].

4.3 Marktrisiken (einschließlich Zinsänderungsrisiken)

Marktrisiken sind gemäß Artikel 4 Nr. 141 Verordnung (EU) Nr. 575/2013 (Kapitaladäquanzverordnung) Verlustrisiken, die aus Markpreisbewegungen, einschließlich Wechselkurs- oder Warenpreisbewegungen erwachsen. In Bezug auf die Nutzung dezentraler Kreditplattformen können sich entsprechende Marktrisiken für Kreditnehmer aus Wertschwankungen der zu hinterlegenden Sicherheiten und Veränderungen der variablen Zinssätze ergeben. Letztere stellen somit auch für die Liquiditätsbereitsteller ein Risiko dar.

Krypto-Token, die als Kreditsicherheit verwendet werden, unterliegen üblichen Kursschwankungen. Diese Wertschwankungen können von Kreditnehmern im Zusammenhang mit Leveraging-Strategien zwar bewusst in Kauf genommen werden. Gleichwohl existieren ohnehin keine anwendungsinhärenten Absicherungsmechanismen gegen derartige Wertschwankungen, die entsprechend durch die Kreditnehmer zu tragen sind.

Zinsänderungsrisiken, als Teil der Marktrisiken, ergeben sich sowohl für Kreditnehmer als auch Liquiditätsbereitsteller, da die Zinssätze dezentraler Kreditplattformen üblicherweise variabel sind. Dabei sind die Risiken für Liquiditätsbereitsteller gleichwohl geringer, da diesen keine negativen Zinssätze vergeben werden, und sie, im Fall geringer ausstehender Liquidität im Lending Pool, von steigenden Zinsen profitieren würden. Demgegenüber würde es in einem solchen Szenario zu einem starken Anstieg der Kreditzinsen kommen, mit entsprechend negativen Auswirkungen für die Kreditnehmer.

Um die Zinsänderungsrisiken für Kreditnehmer zu verringern bietet etwa Aave die Möglichkeit fixer Zinssätze an. Allerdings ist die Stabilität dieser Zinssätze an Bedingungen geknüpft. Kommt es beispielsweise zu einem Rückgang der verfügbaren Liquidität in einem Lending Pool, sodass die Utilisation Rate über 95% steigt, werden die fixen Zinssätze angepasst. Für Krypto-Token, deren Lending Pools hohen Liquiditätsrisiken ausgesetzt sind, sodass die Utilisation Rate häufig in den Bereich von 100% steigt, werden von vornherein keine fixen Zinssätze angeboten. Kreditnehmer müssen für dieses anwendungsinhärente Angebot zur Verringerung der Zinsänderungsrisiken höhere Zinssätze in Kauf nehmen. Diese liegen in der Regel im einstelligen Prozentpunkte-Bereich über den variablen Zinssätzen [18].

4.4 Operationelle Risiken

Während Kredit-, Liquiditäts- und Marktrisiken im Wesentlichen die Nutzung dezentraler Kreditplattformen betreffen, stellen operationelle Risiken eine Gefahr für die Nutzung sämtlicher dezentraler Anwendungen dar. Denn Softwarefehler und missbräuchliches Verhalten einzelner Netzwerkakteure können trotz externer Sicherheitsüberprüfungen und

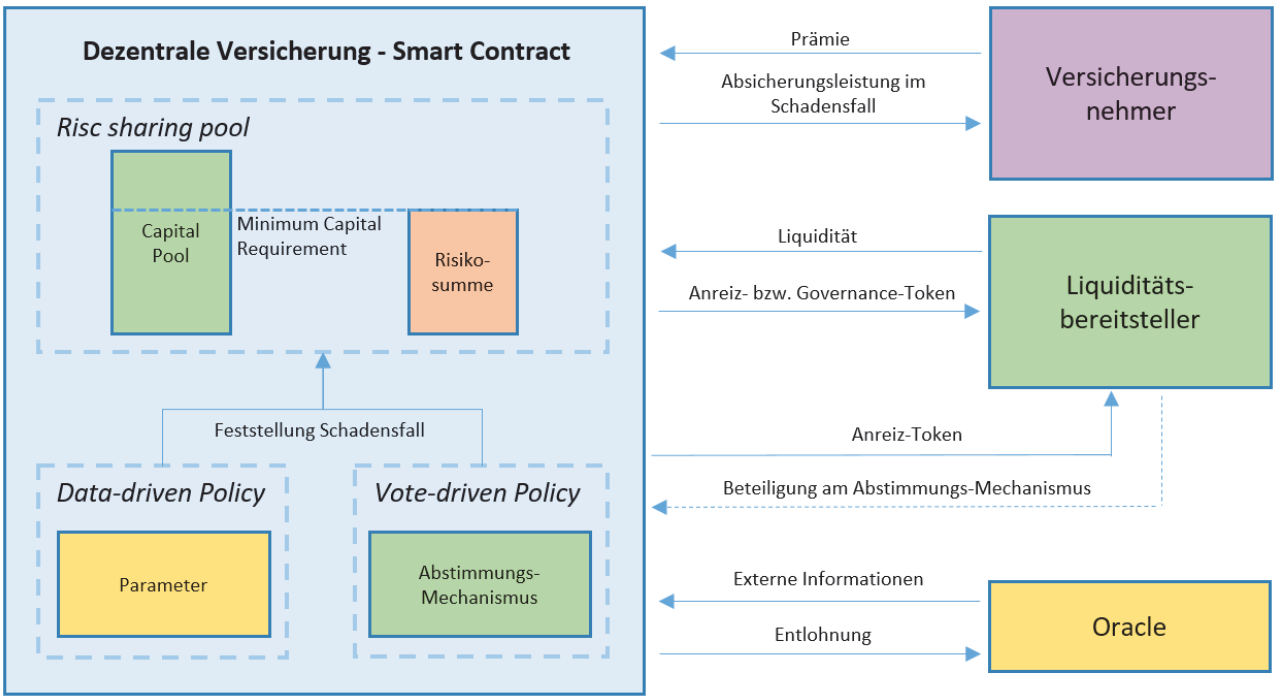

Abbildung 5: Exemplarische Architektur dezentraler Versicherungen, Quelle: Eigene Darstellung.

entsprechender Anreizsystemen die intendierte Funktionsweise dezentraler Anwendungen beeinträchtigen. Gleichzeitig sind schnelle administrative Eingriffe durch eine zentrale Instanz bei dezentralen Anwendungen üblicherweise nicht vorgesehen. Operationelle Risiken sind gemäß Artikel 4 Nr. 52 Verordnung (EU) Nr. 575/2013 (Kapitaladäquanzverordnung) die Risiken von Verlusten, die durch die Unangemessenheit oder das Versagen von internen Verfahren, Menschen, Systemen oder durch externe Ereignisse verursacht werden, einschließlich Rechtsrisiken.

Im Fall von dezentralen Anwendungen können etwa Programmierfehler (sog. Smart Contract Bugs) zu unbeabsichtigten Problemen und damit verbundenen Verlusten für deren Nutzer führen. Durch die Ausnutzung von derartigen Fehlern in Smart Contracts konnten Angreifer in der Vergangenheit immer wieder große Summen erbeuten. Um für einen solchen Fall administrative Eingriffe zu ermöglichen, werden üblicherweise dezentrale Governance-Prozesse implementiert. Dies kann mit Hilfe von Governance-Token erfolgen, mit denen die Entscheidungsprozesse technisch über die zugrundeliegende Blockchain abgebildet werden (sog. On-Chain-Governance). Diese Verfahren sind in der Regel jedoch langsamer als das direkte Einschreiten eines Administrators. Zudem eröffnet sich durch den Einsatz von Governance-Token die Gefahr, dass einzelne Akteure unbemerkt die Stimmenmehrheit erlangen und den Programmcode zu ihren Gunsten ändern (sog. Governance Attack). Diese Gefahr wird durch die Pseudo-Anonymität der Netzwerkakteure und die damit verbundene Intransparenz bezüglich der Entscheidungsstrukturen begünstigt. Die externen Datenquellen der Smart Contracts, sogenannte Oracles, stellen ebenfalls eine kritische Komponente dar, die bei Versagen die Funktionalität der Anwendung gefährdet. Oracles sind gewöhnliche zentrale Informationsquellen wie Sensoren, Dienste oder Institutionen, die einem Smart Contract gewisse Informationen bereitstellen. Daher sind Oracles sämtlichen Bedrohungen, wie Manipulation, Man-in-the-Middle- oder Denial-of-Service-Angriffen ausgesetzt.

Aave etwa sieht für Verluste, die seinen Nutzern aufgrund von Smart Contract Bugs oder Fehlern durch Oracle entstehen, eine Kompensation durch das anwendungsinhärente Safety Module und die Reserve vor [16]. Allerdings können Smart Contract Bugs auch diese Mechanismen selbst betreffen, sodass Nutzer immer Restrisiken ausgesetzt sind. Zudem besteht auch hier Unsicherheit darüber, ob die Mittel des Safety Module und der Reserve ausreichen, um die Nutzer zu entschädigen. Dementsprechend können operationelle Risiken durch die Anwendungen selbst nicht vollumfänglich abgedeckt werden, sodass sich Nutzer gegen diese über Drittanbieter absichern können.

Operationelle Risiken stellen auch den derzeit wesentlichsten Geschäftsfall dezentraler Versicherungslösungen dar. Grundsätzlich sind die existierenden Lösungen ähnlich aufgebaut. Abbildung 5 stellt eine allgemeingültige Architektur dar. Der genaue Aufbau einzelner Komponenten, wie Abstimmungsprozesse, Anreizsysteme, Risikobewertung oder Schadensabwicklung kann je nach Implementierung entsprechend unterschiedlich sein.

Einer der wichtigsten Vertreter ist Nexus Mutual. Diese Plattform bietet beispielsweise Absicherungen gegen Softwarefehler an. Gleichzeitig ist Nexus Mutual selbst eine dezentrale Anwendung. Daher existieren bei derartigen Lösungen große Abhängigkeiten zwischen Versicherer und Schadensereignis, da kritische Ereignissen, die das ganze Ökosystem – in Form der zugrundeliegenden Blockchain – betreffen, ebenfalls für die Versicherungsplattform relevant werden können. Ein Extremereignis könnte somit auch zum Ausfall des Absicherungsgebers führen. Risiken, wie beispielsweise eine kritische Schwachstelle in der Ethereum-Plattform oder in einer kryptografischen Hashfunktion können daher nicht auf diesem Weg abgesichert werden. Obwohl mit einem breiten Anwendungsspektrum und dem Plattformcharakter geworben wird und diese Faktoren auch im White Paper von Nexus Mutual hervorgehoben werden, sind derzeit lediglich Absicherungen von Risiken – insbesondere Softwarefehler – innerhalb des Blockchain-Ökosystems erwerbbar [19].

Bei Abschluss eines Absicherungsgeschäfts ist durch den Nutzer eine Prämie zu leisten, die prozentual von der Versicherungssumme abhängt und je nach Produkt angefangen bei 2,6% bis zu teilweise 27% betragen kann [19]. Nutzer müssen zudem vor dem Abschluss ein Know-your-Customer-Verfahren (KYC) durchlaufen, d.h. sich mit einem amtlichen Ausweisdokument verifizieren. Der Prozess der Schadensabwicklung sieht bei Nexus Mutual vor, dass im Schadensfall durch den Geschädigten entsprechende Beweise eingereicht werden müssen. Dieser Vorgang wird als Claim Submission bezeichnet. Bei parametrischen Leistungen werden Oracles verwendet, um eine Auszahlung zu genehmigen. Bei anderen Leistungen kommt ein Abstimmungsmechanismus zum Einsatz, bei welchem über die Gültigkeit eines Anspruchs entschieden wird. Im Fall von Nexus Mutual erfolgen die Abstimmungen auf der Basis von NXM-Token, die sowohl für Abstimmungen über Schadensfälle dienen, als auch der operativen Governance, etwa im Fall von Protokolländerungen. Zunächst stimmen nur die dafür vorgesehenen Assessors ab (Assessor Vote), die ihre Token dafür gesondert hinterlegen müssen. Die hinterlegten Token können bei schädlichem Verhalten, ebenfalls abstimmungsbasiert, entzogen werden. Kommt es bei der Abstimmung durch die Assessors zu keinem Ergebnis, wird die diese für alle Mitglieder

Risiken	Auswirkungen für Liquiditäts-bereitsteller	Auswirkungen für Kreditnehmer	Eintritts-wahrscheinlich-keit	Beispiel anwendungs-inhärenter Mechanismen	Beispiel externer Maßnahmen
Kreditrisiken	hoch	–	hoch	▪ Übersicherung ▪ Liquidation von Sicherheiten ▪ Verlust-absorptionspuffer ▪ Gläubiger-beteiligung	–
Liquiditäts-risiken	gering	–	mittel	▪ Variable Zinssätze	–
Marktrisiken	gering	mittel	hoch	▪ Feste Zinssätze	–
Operationelle Risiken	hoch	hoch	gering	▪ Verlust-absorptionspuffer ▪ Gläubiger-beteiligung	▪ Dezentrale Versicherungen

Tabelle 1: Risikoeinschätzung dezentraler Kreditplattformen, Quelle: Eigene Darstellung. Beachte: Es wird angenommen, dass ohne das Vorhandensein entsprechender Absicherungsmechanismen sowohl Liquiditätsbereitsteller als auch Kreditnehmer finanzielle Auswirkungen erleiden, sollten Risiken schlagend werden. Die Eintrittswahrscheinlichkeiten stehen dabei in einem relativen Verhältnis zueinander. Ohne entsprechende Absicherungsmechanismen, sollte ein Risiko mit einer hohen Eintrittswahrscheinlichkeit, häufiger schlagend werden, als ein Risiko mit einer geringen Wahrscheinlichkeit.

freigegeben (Member Vote). Bei einem Assesor Vote muss die Mehrheit mindestens 70% der Stimmen erhalten. Bei einem Member Vote reicht die einfache Mehrheit [20].

Die NXM-Token sind in nativer Form nicht handelbar, sondern lassen sich nur direkt bei Nexus Mutual nach Abschluss eines KYC-Prozesses erwerben. Derzeit ist Nexus Mutual als Limited organisiert und soll langfristig durch eine dezentrale autonome Organisation (DAO) ersetzt werden. Der genaue rechtliche Status und damit auch die Regulierungsanforderungen dieser Art von Unternehmensorganisation sind bislang unklar, wodurch auch der KYC-Prozess entfallen könnte [21].

Das Kapitalmodell ist nach Aussage von Nexus Mutual an die Solvency II-Richtlinie angelehnt und berechnet das Minimum Capital Requirement (MCR) so, dass die Wahrscheinlichkeit, alle Schadensereignisse eines Jahres zu decken, bei 99,5% liegt. Der Kapitalpool von Nexus Mutual muss immer mindestens so groß sein, wie das täglich neu berechnete MCR, sonst können keine Absicherungen erworben werden [22].

5. Risikoeinschätzung

Die Nutzung dezentraler Kreditplattformen erfolgt üblicherweise pseudo-anonym, sodass Kreditnehmer nicht auf ihre Bonität hin überprüft werden können – wie es etwa im konventionellen Bankgewerbe üblich wäre. Dadurch ergeben sich, wie in Tabelle 1 dargestellt, erhebliche Kreditrisiken, die letztlich von den Liquiditätsbereitstellern zu tragen sind. Die Kreditrisiken könnten sich dadurch verstärken, dass Kreditnehmer mit guter Bonität in der Erwartung niedrigerer Zinsen tendenziell auf Plattformen mit Bonitätsprüfungen ausweichen, wodurch letztlich insbesondere Netzwerkakteure mit schlechter Bonität Kredite über dezentrale Kreditplattformen aufnehmen könnten. Um die Kreditrisiken für die Liquiditätsbereitsteller zu verringern, greifen die Anwendungen zum Teil auf verschiedene Mechanismen zurück, wie etwa der Übersicherung von Krediten, der automatischen Liquidation von Sicherheiten, Verlustabsorptionspuffern und der Gläubigerbeteiligung. Vollends ausgeschlossen kann zumindest der teilweise Verlust der eingebrachten Liquidität für deren Bereitsteller dadurch jedoch nicht, sodass immer ein Restrisiko verbleibt.

Liquiditätsrisiken sollten nicht unmittelbar zu Verlusten der Liquiditätsbereitsteller führen. Gleichwohl können sich mittelbare Verluste ergeben, sofern die bereitgestellte Liquidität beispielsweise in Form eines Kredites bei einer anderen Plattform aufgenommen wurde und dort hohe Zinssätze drohen. Dementsprechend sind die Auswirkungen für Liquiditätsbereitsteller eher als gering einzustufen, wenngleich derartige Szenarien – ohne entsprechende anwendungsinhärente Mechanismen – häufig eintreten könnten, da dezentrale Kreditplattformen – im Gegensatz zu herkömmlichen Finanzmarktteilnehmern – keine aktive Liquiditätssteuerung betreiben. Mit Hilfe variabler Zinssätze sollten die Liquiditätsrisiken jedoch verringert werden können, wenngleich es dabei insbesondere im Rahmen von Extremereignissen zu Illiquiditätsereignissen kommen kann.

Marktrisiken können sich für Kreditnehmer und Liquiditätsbereitsteller durch Änderungen der variablen Zinsen ergeben. Liquiditätsbereitsteller unterliegen

dabei lediglich dem Risiko sinkender Zinsen, wohingegen Kreditnehmer hohen Verlustrisiken in Form stark steigender Kreditzinsen ausgesetzt sind. Zudem unterliegen Kreditnehmer dem Risiko, dass ihre Sicherheiten im Wert schwanken und bei plötzlichem Wertverfall sogar liquidiert werden könnten. Grundsätzlich sollten Marktrisiken jedoch nicht zu einem Totalverlust führen. Gleichwohl müssen insbesondere die Kreditnehmer mit Verlusten rechnen, die mittels fixer Zinssätze nur bedingt verringert werden könnten. Da die Lending Pools kein aktives Liquiditätsmanagement betreiben, sollte die Liquidität in den Pools permanent schwanken und mit ihr die variablen Zinssätze. Zudem sind auch die Kurse vieler Krypto-Token häufigen Schwankungen unterworfen, sodass die Eintrittswahrscheinlichkeit für Marktrisiken durchaus als hoch eingestuft werden kann.

Operationelle Risiken ergeben sich im Fall von dezentralen Anwendungen insbesondere aus Fehlern in den Softwareprotokollen, die wiederum zu erheblichen Schäden bei den Nutzern führen könnten. Der Programmcode dezentraler Anwendungen kann als Open-Source-Software von jedem eingesehen werden. Dadurch können die Netzwerkakteure zumindest potenziell nachvollziehen, wie Anwendungen aufgebaut sind und funktionieren. Zudem sind die Programmcodes vieler Anwendungen Gegenstand regelmäßiger externer Sicherheitsüberprüfungen. Dementsprechend könnten operationelle Risiken im Verhältnis zu Kredit-, Liquiditäts- und Marktrisiken zwar seltener eintreten [23]. Allerdings könnten ihre negativen Auswirkungen nicht zuletzt aufgrund fehlender Eingriffsmöglichkeiten höher ausfallen und im Extremfall zum Verlust der gesamten eingebrachten Liquidität und Sicherheiten führen. Um dem entgegenzuwirken können sich Nutzer mittels dezentraler Versicherungen absichern. Allerdings sind diese mit Unsicherheiten behaften und können zudem keine Extremereignisse absichern, die auch den Ausfall des Absicherungsgebers einschließen, sodass die Nutzung dezentraler Anwendungen immer mit einem Restrisiko verbunden bleibt.

6. Fazit

Dezentrale Kreditplattformen stellen eine innovative Möglichkeit dar, um Krypto-Token gegen eine entsprechende Verzinsung anzulegen oder zu leihen. Gleichwohl sind damit – wie im konventionellen Bankgewerbe – Risiken verbunden, die sich jedoch im Gegensatz zum konventionellen Kredit- und Einlagengeschäft zu einem großen Teil auf die Nutzer abwälzen. Dazu zählen insbesondere Kreditrisiken und operationelle Risiken. Zudem ergeben sich aufgrund der technischen Funktionsweise der Plattformen für die Nutzer zusätzliche Liquiditäts- und Marktrisiken.

Um die Risiken zu verringern, gibt es erste anwendungsinhärente Absicherungsmechanismen. Diese erscheinen geeignet, um zumindest einen Teil der Risiken zu verringern. Allerdings befinden sich die Mechanismen noch in einem frühen Entwicklungsstadium, sodass keine abschließende Beurteilung ihrer Wirkungsweise erfolgen kann. Dennoch lässt sich bereits sagen, dass sie zumindest theoretisch keine vollumfängliche Risikobewältigung ermöglichen. Insofern sollten Nutzer sich der Risiken bewusst sein, die sich aus der Nutzung dezentraler Kreditplattformen ergeben. Entsprechende Regulierungsanforderungen könnten dazu beitragen, die Robustheit der Plattformen zu erhöhen und damit das ihnen entgegengebrachte Vertrauen zu vergrößern.

Literaturverzeichnis

[1] Deutsche Bundesbank, Krypto-Token und dezentrale Finanzanwendungen, Monatsbericht, Juli (2021), S. 33–51.

[2] DeFi Pulse, online, https://defipulse.com, (2021).

[3] Bundesanstalt für Finanzdienstleistungsaufsicht, Mindestanforderungen an das Risikomanagement – MaRisk, Rundschreiben, 09/2017 (2017).

[4] Deutsche Bundesbank, Die Rolle von Banken, Nichtbanken und Zentralbank im Geldschöpfungsprozess, Monatsbericht, April (2017), S. 15–36.

[5] L. Gudgeon, S. Werner, D. Perez, W. J. Knottenbelt, DeFi Protocols for Loanable Funds: Interest Rates, Liquidity and Market Efficiency, online, https://arxiv.org/pdf/2006.13922.pdf, Oktober (2020).

[6] NFTfi, NFTfi.com Introduction and FAQ, online, https://nftfi.medium.com/nftfi-com-f9ecf4ab1e7d, Mai (2020).

[7] F. Schaer, Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets, Federal Reserve Bank of St. Louis Review, Vol. 103 (2021), S. 153–74.

[8] Aave, Risk Parameters, online, https://docs.aave.com/risk/asset-risk/risk-parameters, 2021.

[9] Aave, Protocol Whitepaper V1.0, online, https://github.com/aave/aave-protocol/blob/master/docs/Aave_Protocol_Whitepaper_v1_0.pdf, Januar (2020).

[10] R. Leshner, G. Hayes, Compound: The Money Market Protocol, online, https://compound.finance/documents/Compound.Whitepaper.pdf, Februar (2019).

[11] Aave, Protocol Whitepaper V2.0, online, https://github.com/aave/protocol-v2/blob/master/aave-v2-whitepaper.pdf, Dezember (2020).

[12] D. Perez, S. Werner, J. Xu, B. Livshits, Liquidations: DeFi on a Knife-edge, online, https://www.doc.ic.ac.uk/~livshits/papers/pdf/fc21a.pdf, April (2021).

[13] Bitkom, Decentralized Finance (DeFi) – A new Fintech Revolution?, online, https://www.bitkom.org/sites/default/files/2020-

07/200729_whitepaper_decentralized-finance.pdf, (2020).
[14] U. W. Chohan, Decentralized finance (DeFi): an emergent alternative financial architecture, Critical Blockchain Research Initiative, Discussion Paper Series: Notes on the 21st Century, Januar (2021).
[15] D. Wang, S. Wu, Z. Lin, L. Wu, X. Yuan, Y. Zhou, H. Wang, K. Ren, Towards A First Step to Understand Flash Loan and Its Applications in DeFi Ecosystem, online, https://arxiv.org/pdf/2010.12252.pdf, April (2021).
[16] Aave, Safety Module, online, https://docs.aave.com/aavenomics/safety-module, (2021).
[17] DeFi Rate, online, https://defirate.com/lend/, (2021).
[18] Aave, Borrow Interest Rate, online, https://docs.aave.com/risk/liquidity-risk/borrow-interest-rate, (2021).
[19] Nexus Mutual, Buy cover - Nexus Mutual App, online, https://app.nexusmutual.io/cover, 2021.
[20] H. Karp, R. Melbardis, Nexus Mutual A peer-to-peer discretionary mutual on the Ethereum blockchain, White Paper, online, https://nexusmutual.io/assets/docs/nmx_white_paperv2_3.pdf, (2021).
[21] A. Thurman, cointelegraph - Nexus Mutual moves to sunset legal entity, lift KYC requirements, online, https://cointelegraph.com/news/nexus-mutual-moves-to-sundown-legal-entity-lift-kyc-requirements, April (2021).
[22] Nexus Mutual, How-to Guides: How to participate, online, https://nexusmutual.gitbook.io/docs/how-to-use-nexus/how-to-participate, (2021).
[23] D. Perez, B. Livshits, Smart Contract Vulnerabilities: Vulnerable Does Not Imply Exploited, Proceedings of the 30th USENIX Security Symposium, August (2021).

Kryptowährungen im Kontext der Gründung einer liechtensteinischen Aktiengesellschaft

Marco Lettenbichler
Universität Liechtenstein, Fürst-Franz-Josef-Strasse, 9490 Vaduz

Das vorliegende Paper untersucht die Einlage von Kryptowährungen bei der Gründung einer liechtensteinischen Aktiengesellschaft. Es wird aufgezeigt, dass Liechtenstein einen sehr liberalen Weg geht und zudem das liechtensteinische Gesellschaftsrecht die Einlage von Kryptowährungen als Sacheinlage ohne Sachverständigenbericht zulässt.

This paper examines the contribution of cryptocurrencies in the formation of a Liechtenstein corporation. It is shown that Liechtenstein takes a very liberal approach and, moreover, Liechtenstein company law allows the contribution of cryptocurrencies as a contribution in kind without an expert report.

1. Einleitung

Seit jeher gelten Währungen als Rückgrat für die Wirtschaftssysteme der Welt. Es verwundert also nicht, dass Geld älter als die Geschichtsschreibung ist und daher über seinen Ursprung nur gemutmaßt werden kann. Als gesichert gelten nur einige Daten; z.B., dass in Europa mit dem Aufkommen des römischen Reiches in der Antike erstmalig hochentwickelte Währungstandards auf dem europäischen Kontinent galten. [1] Eine weitere disruptive Entwicklung erfuhr das Geld durch die Einführung von Papiergeld – heute kaum mehr wegzudenken – im Schweden des 17. Jahrhunderts. [2] Aktuell erleben wir mit der Digitalisierung der Zahlungsmittel die jüngste Revolution des Geldes. Kryptowährungen, wie Bitcoin und Ethereum sind schillernde Begriffe, die nicht nur als neue Form des Zahlungsmittels gelten, sondern auch die Sehnsucht nach schnellem Reichtum, wie der „Goldrush" in den USA des 19. Jahrhunderts, wecken. Noch sind Kryptowährungen nicht als offizielle Zahlungsmittel anerkannt, trotzdem arbeiten verschiedene Nationalbanken an der Einführung von staatlichen Kryptowährungen. Ein vielversprechender Feldversuch wird derzeit von der schwedischen Nationalbank unternommen, die eine E-Krona einführen will. [3] Ebenso scheint es, dass China fieberhaft an einer Implementierung arbeitet. [4] Die zugrundeliegende Blockchain-Technologie wurde bekanntermaßen in Liechtenstein vom Gesetzgeber zur Schaffung des TVTG [5] genommen, um erstmalig einen zivil- und aufsichtsrechtlichen Rahmen für Blockchains zu bieten. [6] Da Kryptowährungen ein ökonomischer Wert zugemessen werden kann, stellt sich die Frage der Verwendung auch in anderen Rechtsbereichen. So wäre es denkbar, dass Kryptowährungen in Gesellschaften zur Aufbringung des Gesellschaftskapitals verwendet werden. Fraglich bleibt dabei, ob es sich um eine Bareinlage oder um eine Sacheinlage handelt. Dieser Aufsatz soll aufgrund der aufgezeigten Aktualität des Themas eine wissenschaftliche Untersuchung von Kryptowährungen iZm Kapitaleinlagen bei liechtensteinischen Aktiengesellschaften vornehmen.

2. Rechtsgrundlage

Strukturell ist das PGR zweigeteilt, es stellt jeweils vor die Körperschaften und die Gesellschaften ohne Persönlichkeit einen allgemeinen Teil. Für die Aktiengesellschaft sind grundsätzlich die allgemeinen Regelungen für die Körperschaften relevant, welche gem Art 245 Abs 1 PGR auf alle Körperschaften, die nachstehend im PGR zu finden sind, angewendet werden. Das liechtensteinische Aktienrecht wird in den Art 261 – 366 PGR [7] geregelt, die Spezialbestimmungen für die Gründung der Aktiengesellschaft sind in den Art 281 – 288 PGR zu finden. Wichtig zu erwähnen ist, dass gem Satz 2 *leg cit* die allgemeinen Regelungen der Art 106 – 245 PGR nur als *leges speciales* gelten sollen, falls sich Regelungslücken in den Spezialnormen ergeben. [8] Zur Interpretation der aktienrechtlichen Normen ist hier noch die Entstehungsgeschichte des PGR zu erläutern. Die beiden liechtensteinischen Juristen *Wilhelm* und *Emil Beck* gelten als Schöpfer dieses wohl einzigartigen Gesetzeswerkes. Emil Beck war Sekretär beim großen Schweizer Rechtsprofessor *Eugen Huber*, der einen Entwurf für eine Revision des schweizerischen Aktienrechts ausgearbeitet hatte, der jedoch in der Schweiz nie in Kraft trat. Die beiden liechtensteinischen Juristen Emil und Wilhelm Beck haben sich jedoch bei der Ausarbeitung des liechtensteinischen Aktienrechts an diesem Entwurf orientiert und auch teilweise die Normen unverändert übernommen. [9] Insofern ist als historische Auslegungsquelle neben dem „kurzen Bericht zum Personen- und Gesellschaftsrecht" [10] auch subsidiär der Entwurf Huber und der dazugehörige Bericht von 1920 heranzuziehen. [11] Für die Gründung einer Aktiengesellschaft sind zudem die Regelungen der Handelsregisterverordnung [12] relevant. Insbesondere sind die besonderen Bestimmungen für die Aktiengesellschaft in Art 52 – 70 HRV von Bedeutung.

3. Gründungsmodalitäten der liechtensteinischen Aktiengesellschaft

3.1. Sukzessivgründung

Im PGR gibt es grundsätzlich zwei verschiedene Formen der Gründung einer Aktiengesellschaft. Bei der Sukzessivgründung, welche in der Praxis kaum eine Rolle spielt, erfolgt der Gründungsprozess in drei Schritten. Zunächst müssen gem Art 281 Abs 1 Z 1 PGR die Statuten in öffentlicher und von den Gründern zu unterzeichnender Urkunde festgesetzt werden. Anschließend müssen schriftlich die Aktien, welche das Aktienkapital bilden, gezeichnet werden. In einem dritten Schritt bedarf es einer konstituierenden Gründerversammlung, in der ein Konstituierungsbeschluss gefasst werden muss. [13] Dieser muss gem Art 284 PGR festhalten, dass das Aktienkapital vollständig gezeichnet ist und der statutarische Mindestbetrag, zumindest aber 25 % des Aktienkapitals, durch Bar- oder Sacheinlage gedeckt ist. Zudem muss der Beschluss die notwendigen Organe bezeichnen, sowie der Statutenentwurf beraten und endgültig festgesetzt werden. Gem Art 177 Abs 1 PGR ist über den Beschluss der Konstituierung eine öffentliche Urkunde zu errichten. [14]

3.2. Simultangründung

Der praktische Regelfall in Liechtenstein ist jedoch die Simultangründung. Bei dieser fallen die Gründungsstufen zusammen. Die Gründer sind mit den späteren Aktionären identisch und die von ihnen zu errichtenden Gründerurkunde muss gem Art 288 Abs 1 PGR folgende Mindestinhalte aufweisen: Erklärung, dass eine Aktiengesellschaft gegründet werden soll; Festsetzung der Statuten; Erklärung, dass die Gründer sämtliche Aktien übernehmen; Feststellung, dass 25 % der auf jede Aktie entfallende Einlage geleistet ist (durch Bar- oder Sacheinlage) und die Bestellung der notwendigen Organe. [15] Die nach Art 177 Abs 1 PGR öffentlich zu errichtende Gründerurkunde tritt gem Art 288 Abs 2 PGR an die Stelle der konstituierenden Generalversammlung. [16]

Beiden Varianten ist gemein, dass die Aktiengesellschaft erst mit Eintragung ins Handelsregister konstitutiv gegründet ist und damit über eine Rechtspersönlichkeit verfügt. [17]

4. Mindestgrundkapital

Die Regelungen für das Mindestgrundkapital der Aktiengesellschaft findet sich im Art 122 PGR, wonach dieses mindestens 50.000 Franken beträgt. Die sehr liberale Ausgestaltung des liechtensteinischen Gesellschaftsrecht ist im folgenden Abs 2 *leg cit* erkennbar. In Liechtenstein ist es nämlich möglich, neben der Aufbringung des Mindestkapitals in der Landeswährung auch zusätzlich diesen Betrag in Euro oder auch US-Dollar einzubezahlen. Geschuldet ist dieser Umstand sicherlich der sehr internationalen Ausrichtung der liechtensteinischen Wirtschaft und des Vermögensstandortes. Zudem ist es möglich, die erforderliche Summe als Bareinlage zu tätigen oder diese auch als Sacheinlage aufzubringen. [18] Das Mindestgrundkapital muss voll liberiert oder eingebracht werden. [19] Beide Möglichkeiten sollen in weiterer Folge kurz erläutert werden.

4.1. Funktion des Mindestgrundkapital

Allen Aktiengesellschaften im deutschsprachigen Raum ist ein Mindestgrundkapital immanent. In der Schweiz beläuft es sich gem Art 621 OR auf 100.000 CHF, in Österreich gem § 7 öAktG 70.000 EUR und in Deutschland gem § 7 dAktG 50.000 EUR. Ziel eines solchen Mindestgrundkapitals ist sicherlich die Schaffung eines „minimalen Haftungssubstrats“. [20] Dieses soll als Ausgleich dafür dienen, dass der Aktionär keine Haftung mit seinem Privatvermögen übernimmt. Zudem dient es als gewisse finanzielle Hürde für Kleinunternehmensgründungen, da der Betrag eine nicht unerhebliche Summe für Privatpersonen darstellt. [21] Die Funktion des Haftungsfonds darf jedoch nicht überschätzt werden, denn natürlich wird das Mindestgrundkapital von der Gesellschaft weiterverwendet und ist sohin nur im Zeitpunkt der Gründung vollkommen vorhanden. [22] Zudem werden bei einer Aktiengesellschaft oft hohe Verbindlichkeiten eingegangen, sodass ein Mindestgrundkapital iHv 50.000 CHF eher für die Befriedigung eines nur sehr kleinen Teils von offenen Forderungen dienen wird. [23]

4.2. Bareinlagen

Grundsätzlich besteht die Möglichkeit, das Mindestgrundkapital als Bareinlage einzuzahlen. Die Einzahlung muss gegenüber dem Amt für Justiz nachgewiesen werden. In der Praxis erfolgt dies meist durch eine Bankbestätigung.

4.3. Sacheinlage

4.3.1. Standardfall

Falls das Mindestgrundkapital als Sacheinlage eingebracht wird, müssen zusätzliche Formerfordernisse eingehalten werden. Gem Art 280 Abs 1 Z 1 PGR müssen Angaben über die Sacheinlage in den Statuen getroffen werden. Zusätzlich muss der Wert der einzubringenden Sache(n) von einem Sachverständigen geprüft werden, damit gewährleistet werden kann, dass der Wert die Mindestgrundkapitalgrenzen einhält bzw übersteigt. Der hierüber zu erstellende Sachverständigenbericht muss von der Generalversammlung genehmigt werden. Dieser hat gem Art 285 Abs 2 PGR zu enthalten: Die Beschreibung des Gegenstandes der Einlage (Z1), die Methode, nach welcher die Wertermittlung erfolgt ist (Z2), ob der ermittelte Wert dem des Mindestkapitals entspricht (Z3) sowie Auskünfte über Gründe und Angemessenheit über gewährte Gründervorteile (Z4). [25] Dieser Bericht muss gem Art 55 Abs 2 lit a HRV bei der Gründung der Aktiengesellschaft beim Amt für Justiz eingereicht werden. Zudem sind auch die Sacheinlageverträge zu übermitteln (lit b *leg cit*). Bemerkenswert ist hier noch zu erwähnen, dass das PGR den Begriff des «Sacheinlagevertrags» nicht kennt. Erst aus dem Art 55 Abs 2

lit b HRV ergibt sich, dass zur Gründung der Sacheinlagevertrag dem Amt für Justiz vorgelegt werden muss.

4.3.2. Vereinfachter Bericht

Nach Art 286a PGR kann ein Sachverständigenbericht, als vereinfachter Bericht, durchgeführt werden, wenn übertragbare Wertpapiere oder Geldmarktinstrumente im Sinne der Richtlinie 2014/65/EU als Sacheinlagen eingebracht werden. Zusätzlich muss ein Wert an einem Markt oder an einer Börse festgestellt werden können und davon die Ermittlung eines Durchschnittspreises der letzten 30 Tage angegeben werden. Anschließend ist gem Art 286a Abs 3 PGR ein Monat nach Einbringung der Vermögensgegenstände ein Bericht beim Amt für Justiz einzureichen. Dieser muss eine Beschreibung der betreffenden Sacheinlage inklusive den Wert und die Bewertungsmethode enthalten. Zudem muss festgestellt werden, dass der Vermögenswert dem Wert der ausgegebenen Aktien entspricht. Es dürfen in der Zwischenzeit keine Umstände aufgetreten sein, welche einen anderen Wert der Vermögensgegenstände zur Folge hätten. [26]

Zu berücksichtigen ist hier allerdings, dass Kryptowährungen grundsätzlich keine Wertpapiere oder Geldmarktinstrumente im Sinne der Richtlinie 2014/65/EU sind [27] und insofern die Regelungen zum vereinfachten Bericht nicht zur Anwendung kommen. Trotzdem sind die Ausführungen für diesen Aufsatz von Bedeutung, weil so aufgezeigt werden soll, dass dem PGR eine Abweichung vom herkömmlichen Sacheinlageverfahren nicht unbekannt ist.

5. Aufbringung des Mindestgrundkapitals durch Kryptowährungen

Infolge soll daher untersucht werden, ob die Aufbringung des Mindestgrundkapitals durch Kryptowährungen in Liechtenstein möglich ist und wie diese aus rechtlicher Sicht zu beurteilen sind.

5.1. Bareinlage

5.1.1. Direkte Anwendung der Vorschriften

Auf den ersten Blick scheint es durchaus möglich zu sein, dass Kryptowährungen wie eine Bareinlage zu behandeln sind. Jedoch stellt das PGR in Art 122 Abs 1 PGR für das Mindestgrundkapital ganz klar auf die Landeswährung, also den „liechtensteinischen" Franken ab. Zusätzlich wird in Art 122 Abs 2 PGR noch Euro oder auch US-Dollar als mögliche Währung zur Aufbringung des Mindestkapitals genannt. [28] Zwar verteilt sich die Aufzählung der zulässigen Währungen auf zwei Absätze, jedoch ist mE trotzdem von einer taxativen Aufzählung auszugehen. Dem Gesetzgeber kommt es geradezu darauf an, den Sachverhalt abschließend zu regeln, hätte er eine demonstrative Aufzählung beabsichtig, hätte er eine Formulierung wie zB «oder auch anderer Währungen» gewählt. Durch die Endgültigkeit dieser Aufzählung können also nur drei Währungen zur Aufbringung des Mindestgrundkapitals verwendet werden. Im Ergebnis ist eine direkte Anwendung der Regelungen auf Kryptowährungen also nicht möglich.

5.1.2. Analoge Anwendung

Zu klären bleibt jedoch, ob eine analoge Anwendung auf Kryptowährungen möglich ist. Festzuhalten ist, dass eine taxative Aufzählung eine Analogie nicht ausschließt. [29] Grundvoraussetzung für eine ergänzende Rechtsfortbildung ist eine Gesetzeslücke. [30] Ein Mindestgrundkapital für Aktiengesellschaften wurde in Liechtenstein erst im Jahr 1955 iHv zunächst 25.000 Franken eingeführt. [31] Die Möglichkeit der Aufbringung des Mindestgrundkapitals in einer anderen Währung besteht erst seit dem Jahr 2003. [32] Die erste Kryptowährung – welche auf dem Blockchain-Netzwerk basiert – wurde am 03. Januar 2009 gegründet. [33] Insofern war es dem historischen Gesetzgeber nicht möglich, die Spannungsfelder, die sich durch die Einführung von Kryptowährungen ergeben, zu regeln. Eine Virtualisierung eines sicheren Zahlungssystems, welches Ähnlichkeiten zu gesetzlich anerkannten Währungen aufweist, konnte damals noch nicht abgesehen werden. Man könnte also durchaus eine planwidrige Lücke im Gesetz annehmen. Fraglich bleibt jedoch, ob Kryptowährungen, ebenso wie gesetzlich anerkannte Währungen von der ratio legis mitumfasst werden. [34] Kryptowährungen weisen durchaus Ähnlichkeiten mit gesetzlich anerkannten Währungen auf. So hat unlängst der Internetzahlungsdienst PayPal angekündigt, dass demnächst verschiedene Kryptowährungen als Zahlungsmöglichkeit zugelassen werden sollen. [35] Ebenso kann im Kanton Zug die Steuerschuld mittels Kryptowährung bezahlt werden. [36]

Die Akzeptanz und Verbreitung des virtuellen Geldes scheinen also immer grösser zu werden, jedoch bleiben auch gravierende Unterschiede zu Währungen. Erheblichster Unterschied ist sicherlich, dass gesetzlich anerkannten Zahlungsmitteln von staatlicher Seite, grundsätzlich von Zentralbanken, kontrolliert werden. Im Falle des Franken, der in Liechtenstein gesetzlich anerkanntes Zahlungsmittel ist, [37] wäre die zuständige Instanz die schweizerische Nationalbank. Diese hat die Preisstabilität des Franken zu gewährleisten und muss die Grundbedürfnisse eines Währungsraumes, wie bspw. Bargeldversorgung, Funktionsgewährleistung von Zahlungssystemen und Stabilität des Finanzsystems sicherstellen. [38] Dies führt auch dazu, dass die Wertbeständigkeit eines herkömmlichen Zahlungsmittels weit über dem einer Kryptowährung liegt. Bei Kryptowährungen gibt es hingegen keine Regulierungsinstanz, die Wertbildung erfolgt viel mehr nach dem Gesetz von Angebot und Nachfrage. Dies kann dazu führen, dass extrem große Schwankungen des Wertes entstehen. So ist bspw der Bitcoin mit Jahresanfang 2021 in kurzer Zeit bis auf 40.000 USD gestiegen und dann wieder auf 30.000 USD gesunken, um dann wieder im März auf 60.000 USD zu steigen. [39] Eine Vergleichbarkeit mit gesetzlich anerkannten Währungen ist hier also nicht gegeben. [40] Ein zusätzliches Unterscheidungsmerkmal zwischen einer

gesetzlich anerkannten Währung und einer Kryptowährung ist der Annahmezwang. Grundsätzlich ist in Liechtenstein jeder verpflichtet, den Franken anzunehmen. [41] Bei Kryptowährungen ist dies hingegen nicht der Fall.

5.1.3. Zwischenergebnis

Eine analoge Anwendung des Art 122 Abs 1 u 2 PGR auf Kryptowährungen ist aufgrund der genannten Unterschiede abzulehnen. Zusätzlich auch darum, weil eine zweite Möglichkeit der Einbringung in Form der Sacheinlage zur Verfügung steht.

5.2. Sacheinlage

Da es sich bei der Einbringung von Kryptowährung um keine Bareinlage handelt, liegt im Umkehrschluss eine Sacheinlage vor.

5.2.1. Einlagefähigkeit von Kryptowährungen

Zunächst gilt es zu klären, ob Kryptowährungen überhaupt einlagefähig sind. Aufgrund der fehlenden Literatur in Liechtenstein soll hier wegen der engen Verbindung mit dem schweizerischen Gesellschaftsrecht auf dessen Lehre zurückgegriffen werden.

Als Voraussetzungen für die Einlagefähigkeit von Sachen wird auf die Aktivierbarkeit, Übertragbarkeit, Verfügbarkeit und Verwertbarkeit abgestellt. [42] Die Aktivierbarkeit ist jedenfalls gegeben, da der Kryptowährung freilich ein ökonomischer Wert zukommt und die Aktiengesellschaft über diese verfügen kann. [43] Ebenso ist das Kriterium der Übertragbarkeit vorhanden. In der Regel wird die Kryptowährung über ein Blockchain-System gehandelt. Falls es sich um eine Blockchain eines inländischen VT-Dienstleisters handelt, würde hier die Übertragungsordnung des neu geschaffenen TVTG Anwendung finden. [44] Die Verfügbarkeit über Kryptowährungen wird grundsätzlich von der Verfügung über den Privat Key abhängen. Sobald dieser in der Verfügungsgewalt der Aktiengesellschaft steht kann sie über die Kryptoassets verfügen. [45] Auch hier ist wieder auf die Besonderheit von Blockchains im Anwendungsbereich des TVTG hinzuweisen. In Art 5 Abs 1 TVTG wird gesetzlich festgehalten, dass derjenige, welcher Inhaber des VT-Schlüssels ist, ebenso die Verfügungsgewalt über den Token hat. [46] Insofern ist die Verfügbarkeit im Zeitpunkt des Innehabens des VT-Schlüssels bei der Aktiengesellschaft gegeben. Das Kriterium der Verwertbarkeit ist jedenfalls durch die leichte Handelbarkeit von Kryptowährungen auf Kryptobörsen gewährleistet. [47] Auch durch die Annahme von Kryptowährungen als Zahlungsmittel kann die Erfüllung der Voraussetzung nochmals unterstrichen werden. Die Einlagefähigkeit von Kryptowährungen ist sohin gegeben, da alle Voraussetzungen – Aktivierbarkeit, Übertragbarkeit, Verfügbarkeit und Verwertbarkeit – klar erfüllt werden.

Für die Sacheinlage von Kryptowährungen müsste in weiterer Folge das oben beschriebene Verfahren eingehalten werden, insbesondere müsste eine Schätzung des Wertes aufgrund eines Sachverständigengutachtens eingeholt werden. Jedoch scheint es in Liechtenstein hiervon Ausnahmen zu geben, die in weiterer Folge aufgezeigt werden sollen.

5.2.2. Besonderheit in Liechtenstein

Zuständige Behörde für die Gründung und Eintragung einer Aktiengesellschaft ist in Liechtenstein das Amt für Justiz. Dieses hat in einem Merkblatt [48] präzisiert, dass eine Gründung mittels Kryptowährung grundsätzlich zulässig sei. Zur Spezifizierbarkeit von Kryptowährungen wird auf die Website von «Coinmarketcap» [49] zurückgegriffen. Aktuell wird die mögliche Auswahl jedoch noch auf Bitcoin und Ethereum beschränkt. Falls eine andere Kryptowährung als Sacheinlage eingebracht werden soll, wird empfohlen, vorab mit dem Amt für Justiz Kontakt aufzunehmen, um dies abzuklären. [50]

5.2.2.1. Sacheinlagevertrag

Es wird außerdem empfohlen, dass im Sacheinlagevertrag die Kryptowährung genau bezeichnet wird und die Bewertungsmethoden festgehalten werden bzw, falls eine Handelsplattform zur Wertermittlung herangezogen wurde, sollte diese ausgewiesen werden. Dem Amt für Justiz ist die große Marktwertschwankung von Kryptowährungen bewusst und legt daher nahe, dass bei Aufbringung des Mindestgrundkapitals eine gewisse Sicherheitsmarge berücksichtigt werden sollte, da im Zeitpunkt der öffentlichen Beurkundung und bei der Eintragung ins Handelsregister eine Deckung vorhanden sein muss. [51]

5.2.2.2. Sachverständigengutachten

Wie schon ausgeführt muss bei Sacheinlagen grundsätzlich eine Bewertung durch einen Sachverständigen durchgeführt werden. Normalerweise gilt dies auch für Kryptowährungen, die als Sacheinlage eingebracht werden müssen. Im Merkblatt des Amtes für Justiz wird jedoch festgehalten, dass der Sachverständigenbericht bei der Einbringung von Kryptowährungen nicht erbracht werden muss. Begründet wird dies damit, dass bei der Aufbringung des Gesellschaftskapitals durch Kryptowährungen auch Elemente der Bareinlage vorlägen. Dies daher, weil Referenzpreise täglich auf der Website der Eidgenössischen Steuerverwaltung [52] eingesehen werden können und daher ein objektiver Marktwert gegeben sei. Es könne daher jederzeit für jeden beliebigen Stichtag in der Vergangenheit der Wert der Kryptowährung erhoben werden. [53]

Es kann also festgehalten werden, dass das Amt für Justiz in Liechtenstein Kryptowährungen als Sacheinlage ansieht, jedoch auf den Sachverständigenbericht verzichtet wird und es daher eine Annäherung an die Bareinlagevorschriften gibt.

5.2.3. Erfüllung der privatrechtlichen Ratio

Nun soll geprüft werden, ob die im Merkblatt des Amtes für Justiz geschilderte Vorgehensweise des Handelsregisters auch mit den privatrechtlichen Vorgaben zur Gründung einer Aktiengesellschaft vereinbar ist. Wie oben geschildert ist eine analoge Anwendung der Bareinlage nicht möglich. Bei der Sacheinlage bedarf es grundsätzlich eines Sachverständigenberichts. Es ist also insbesondere zu untersuchen, ob eine teleologische Reduktion des Art 285 PGR möglich ist, sodass Kryptowährungen von der Sachverständigenberichtspflicht ausgenommen sind.

5.2.3.1. Gleichbleibender Gläubigerschutz

Die ratio legis des Art 285 PGR zielt auf den Gläubigerschutz als ein Grundprinzip des Gesellschaftsrechts ab. Es soll gewährleistet werden, dass dem Gläubiger ein gewisser Haftungsfond zur Verfügung steht. Gerade bei Sachen ist eine Bewertung oftmals schwierig möglich. Bei einer internen Bewertung durch die Gründer/Organe der Aktiengesellschaft könnte diese höher ausfallen, als bei einer Bewertung durch einen unabhängigen externen Sachverständigen, der einen objektiven Marktpreis nach anerkannten Bewertungsmethoden eruiert. [54]

Hier unterscheiden sich Kryptowährungen von anderen Rechten und Sachen. Denn der Wert von Kryptowährungen ist durch die Handelbarkeit auf Kryptobörsen jederzeit feststellbar. Hieraus ergibt sich also eine enorme Rechtssicherheit für die Feststellung des Wertes. Ein Sachverständiger würde nur den Wert von der Kryptobörse entnehmen und diesen dann für den Sachverständigenbericht verwenden. Insofern würde sich hier kein Mehrwert für den Gläubigerschutz ergeben. Der Gläubigerschutz wird also durch die Erstellung eines Sachverständigenberichts über Kryptowährungen nicht erhöht. Dies insbesondere vor dem Hintergrund, als dass im Sacheinlagevertrag der Gründer die eingebrachte Kryptowährung sowieso genau spezifizieren muss und sohin ein tagesaktueller Wert festgestellt werden kann. [55] Erwähnt werden soll hier auch noch, dass gem 286a PGR ein vereinfachter Bericht möglich ist, falls Wertpapiere oder andere Geldmarktinstrumente im Sinne der Richtlinie 2014/65/EU als Sacheinlagen eingebracht werden. Auch hier sieht der Gesetzgeber also Erleichterungen vor, wenn der Marktwert einer Sache unkompliziert ermittelt werden kann und somit offensichtlich ist. Insofern ist eine Einschränkung der Berichtspflicht dem PGR nicht fremd. Festzuhalten bleibt aber auch hier, dass Kryptowährungen nicht unter den Wertpapierbegriff bzw. Geldmarktinstrumente-Begriff der RL 2014/65/EU fallen. [56]

5.2.3.2. Funktion von Kryptowährungen in Abgrenzung zu Sachen und Rechten

Für eine Ungleichbehandlung von Kryptowährungen mit anderen Sachen und Rechten spricht zudem deren grundlegende Funktion. Sachen und Rechte sind grundsätzlich Gebrauchsgegenstände oder Wertanlagen, sie dienen insofern einem Zweck im Dienste des menschlichen Individuums. Hingegen ist die Funktion von Kryptowährungen sehr stark angelehnt an die Funktion gesetzlich anerkannter Währungen; es steht also eine gewisse Tausch- und Zahlungsfunktion im Vordergrund. [57] Wie bereits erwähnt ist es mittlerweile ohne weiteres möglich, im Kanton Zug seine Steuer mittels Kryptowährungen zu bezahlen [58] oder auch mittels Kryptokreditkarte seine Kryptowährungen wie herkömmliche Zahlungsmittel zu verwenden. [59] Ebenso arbeiten fast alle namhaften Staaten an einer eigenen Kryptowährung; insbesondere China ist mit seiner Kryptowährung Central Bank Digital Currency schon weit fortgeschritten. [60] Auch namhafte Unternehmen sind mittlerweile aufgeschlossen gegenüber Bezahlung mittels Kryptowährung; so kann man bei Starbucks und Tesla seine Zahlungen mit Bitcoins tätigen. [61] Ebenso sieht der liechtensteinische Gesetzgeber Ähnlichkeiten von Kryptowährungen und gesetzlich anerkannten Zahlungsmitteln. So schreibt der Bericht und Antrag zur Schaffung eines Gesetzes über Token und VT-Dienstleister (Blockchain-Gesetz) dem Bitcoin alle Funktionen von Geld – also die Zahlungsmittelfunktion, die Wertaufbewahrungsfunktion und die Funktion als Recheneinheit – zu. Jedoch wird aufgrund der mangelnden Kontrolle durch eine Zentralbank und gesetzliche Anerkennung keine Äquivalenz mit einem gesetzlich anerkannten Zahlungsmittel gesehen. [62] Trotzdem zeigt sich mE, dass der liechtensteinische Gesetzgeber durchaus die Problematik der Einordnung von Kryptowährungen aufgezeigt hat. Die vorherigen Ausführungen lassen durchaus auf eine funktionale Annäherung an gesetzliche Zahlungsmittel schließen, auch wenn diese jedenfalls nicht vollkommen vorliegt. [63]

Insgesamt zeigen die Argumente, der einfachen Feststellung des Wertes von Kryptowährungen und die angenäherte Funktion an gesetzlich anerkannte Währungen, dass eine teleologische Reduktion des Art 285 PGR tunlich ist. Sohin kann aus gesellschaftsrechtlicher Sicht auf einen Sachverständigenbericht gem Art 285 PGR bei Sacheinlage von Kryptowährungen verzichtet werden, falls diese einen einfach zu bestimmenden Wert über eine anerkannte Bewertungswebsite haben. Hier verweist das Merkblatt des Amtes für Justiz auf die Website der eidgenössischen Steuerverwaltung. [64]

6. Conclusio

Abschließend kann festgehalten werden, dass es sich bei der Einlage von Kryptowährungen um einen „Graubereich“ zwischen Bar- und Sacheinlage handelt. Jedoch aufgrund der nichtvorhandenen gesetzlichen Anerkenntnis durch Staaten kann jedenfalls keine Bareinlage vorliegen. Da aber Kryptowährungen durchaus die Geldfunktionen erfüllen und durch die leichte Feststellbarkeit des Wertes der Gläubigerschutz auf hohem Niveau gewahrt werden kann, sind ebenso die Sacheinlageregelungen überschießend. Dies auch aus dem Grund der genauen und nachvollziehbaren Feststellung des Wertes

im Sacheinlagevertrag durch die Gründer. Insbesondere kann nach Ansicht des Autors aufgrund einer teleologischen Reduktion auf den verpflichtenden Sachverständigenbericht aus den vorher genannten Gründen verzichtet werden. Die Argumentation verstärkt sich in Zukunft noch durch die Umstände der viel weiteren Verbreitung als Zahlungsmittel von Kryptowährungen und durch eine wohl künftige Einführung von gesetzlich anerkannten Kryptowährungen.

Literaturverzeichnis

[1] North, M.: Kleine Geschichte des Geldes: vom Mittelalter bis heute (2009), 8.

[2] Mäkeler, H.: Seit wann gibt es Papiergeld in Europa? URL: https://www.swr.de/wissen/1000-antworten/kultur/1000-antworten-3156.html (abgerufen am 31.08.2021).

[3] Balzter, S.: Schweden erfindet das Geld neu, URL: https://www.faz.net/aktuell/finanzen/digital-bezahlen/die-schwedische-notenbank-will-eigene-digitalwaehrung-einfuehren-15691368.html (abgerufen am 31.08.2021).

[4] Eger, B.: Chinas Antwort auf den Bitcoin, URL: https://www.tagesschau.de/wirtschaft/weltwirtschaft/china-kryptowaehrung-bitcoin-101.html (abgerufen am 31.08.2021).

[5] Gesetz vom 3. Oktober 2019 über Token und VT-Dienstleister (Token- und VT-Dienstleister-Gesetz; TVTG), LGBl 2019/301.

[6] Ministerium für Präsidiales und Finanzen: Regierung genehmigt Verordnungen im Zusammenhang mit dem TVTG, URL: https://www.regierung.li/de/mitteilungen/223135/?typ=content&nid=11072 (abgerufen am 31.08.2021).

[7] Personen- und Gesellschaftsrecht, LGBl 1926/4.

[8] Marxer & Partner (Hrsg): Liechtensteinisches Wirtschaftsrecht (2009) 44.

[9] Lettenbichler, M.: Holokratie im Liechtensteinischen Gesellschaftsrecht, SPWR 2020, 65 (67).

[10] Beck, E., Beck, W.: Kurzer Bericht über die Revision des Personen- und Gesellschaftsrechts (1925).

[11] Marxer, F.: Die personalistische Aktiengesellschaft im liechtensteinischen Recht (2007) 60-63; Schurr, F.: Die Liechtensteinische Aktiengesellschaft und die Bindung ihrer Aktionäre, ZVglRWiss 2012, 339 (342 f); Marxer, F.: Rezeption im liechtensteinischen Gesellschaftsrecht, LJZ 2006, 56 (59).

[12] Verordnung vom 11. Februar 2003 über das Handelsregister (Handelsregisterverordnung; HRV), LGBl 2003/66.

[13] Batliner, C.: Liechtenstein, in Wegen/Spahlinger/Barth (Hrsg), Gesellschaftsrecht des Auslands (3. EL September 2020), Rn 18.

[14] Marxer & Partner (Hrsg): Wirtschaftsrecht, 47 f; Batliner, C.: in Wegen/Spahlinger/Barth, Rn 19.

[15] Batliner, C.: in Wegen/Spahlinger/Barth, Rn 14.

[16] Marxer & Partner (Hrsg): Wirtschaftsrecht, 47; Batliner, C.: in Wegen/Spahlinger/Barth, Rn 15.

[17] Vgl für die Eintragung ins Handelsregister: Langer, M.: Das liechtensteinische Steuerrecht (2019), 39 f; Marxer & Partner (Hrsg): Wirtschaftsrecht, 46.

[18] Marxer & Partner (Hrsg): Wirtschaftsrecht, 54.

[19] Batliner, C.: in Wegen/Spahlinger/Barth, Rn 48.

[20] Morscher, L.: in OR Kommentar OFK - Orell Füssli Kommentar (Navigator.ch) (2016) Art 621 OR, Rn 2; Fichtinger, W.: in Napokoj/Foglar-Deinhardstein/Pelinka (Hrsg), AktG Taschenkommentar (2019) § 7 AktG, Rn 1.

[21] Arlt, M.: in MüKoAktG[5] (2019), § 6 AktG, Rn 110; Solveen, D.: in Hölters, Aktiengesetz[3] (2017), § 7 AktG, Rn 1.

[22] Solveen, D.: in Hölters, Aktiengesetz[3], § 7 AktG, Rn 1; Arlt, M.: in MüKoAktG[5], § 6 AktG, Rn 111.

[23] Vgl für Deutschland: Wöstmann, H.: in Henssler/Strohn, Gesellschaftsrecht[5] (2021), § 7 AktG, Rn 1.

[24] Marxer & Partner (Hrsg): Wirtschaftsrecht, 54.

[25] Langer, M.: Steuerrecht, 40 f.

[26] Vgl zur ähnlichen Regelung in Deutschland: Gerber, O.: in BeckOGK, § 33a AktG, Rn 1 ff (Stand: 01.07.2020).

[27] Patz, A.: Handelsplattformen für Kryptowährungen und Kryptoassets, BKR 2019, 435 (436); Nathmann, M.: Token in der Unternehmensfinanzierung, BKR 2019, 540 (542).

[28] Batliner, C.: in Wegen/Spahlinger/Barth, Rn 48.

[29] RIS-Justiz RS0008928.

[30] Bydlinski, F.: Juristische Methodenlehre und Rechtsbegriff (2011), 473 ff.

[31] Gesetz vom 21. Dezember 1954 betreffend die Abänderung von Art. 122 des Personen- und Gesellschaftsrechtes sowie von § 71 der Schlussabteilung des Personen- und Gesellschaftsrechtes vom 20. Januar 1926, LGBl 1955/2.

[32] Gesetz vom 20. Dezember 2002 über die Abänderung des Personen- und Gesellschaftsrechts, LGBl 2003/63.

[33] Grundlehner, W.: Der Bitcoin wird zu seinem 12. Geburtstag 35 000 Dollar schwer, NZZ, URL: https://www.nzz.ch/finanzen/bitcoin-steigt-an-seinem-12-geburtstag-auf-35000-dollar-ld.1594639?reduced=true (abgerufen am 31.08.2021)

[34] Bydlinski, F.: Methodenlehre[2], 475 ff

[35] ZDF: Kryptowährung - Ist Bitcoin jetzt salonfähig? URL: https://www.zdf.de/nachrichten/wirtschaft/bitcoin-kurs-image-100.html (abgerufen am 31.08.2021).

[36] Kanton Zug: Kanton Zug akzeptiert ab 2021 Kryptowährungen für Steuerzahlungen, URL: https://www.zg.ch/behoerden/finanzdirektion/direktionssekretariat/aktuell/kanton-zug-akzeptiert-ab-2021-kryptowaehrungen-fuer-steuerzahlungen (abgerufen am 31.08.2021).

[37] Vgl Art 1 Abs 1 des Gesetzes vom 26. Mai 1924 betreffend die Einführung der Frankenwährung (FrWG), LGBl 1924/8.

[38] Vgl Art 5 Bundesgesetz über die Schweizerische Nationalbank (Nationalbankgesetz, NBG), SR 951.11.

[39] Frankfurter Allgemeine Zeitung: Bitcoin steigt erstmals auf 60.000 Dollar, URL: https://www.faz.net/aktuell/finanzen/finanzmarkt/neuer-rekord-bitcoin-steigt-erstmals-auf-60-000-dollar-17243028.html (abgerufen am 31.08.2021).

[40] Tenhagen, H.: Hype um Bitcoin - Riskantes Spiel, Spiegel Online, URL: https://www.spiegel.de/wirtschaft/service/bitcoin-spielzeug-fuer-nerds-und-anarchisten-a-eb3f2b81-0f60-471b-8e88-b3f480db65f3 (abgerufen am 31.08.2021).

[41] Für Liechtenstein ergibt sich der Annahmezwang aus Art 2 Gesetz vom 26. Mai 1924 betreffend die Einführung der Frankenwährung, LGBl 1924/8.

[42] Frésard, P., Heller, J.: Kryptowährungen als Kapitaleinlagen, Jusletter 9. September 2019, 4; vgl für Österreich: Miernicki, M.: Kryptowährungen und Sachgründung im Gesellschaftsrecht, in Kirchmayr-Schliesselberger/Klas/Miernicki/Rinderle-Ma/Weilinger (Hrsg), Kryptowährungen (2019) 138 (142).

[43] Müller, T., Zysset, P., Kalaitzidakis, V.: Die Einlage von Kryptowährungen zur Gründung einer Gesellschaft, Jusletter 20. Mai 2019, 7; P. Frésard, P., Heller, J.: Jusletter 9. September 2019, 4 f.

[44] Vgl zur Übertragung von Token: Layr, A., Marxer, M.: Rechtsnatur und Übertragung von "Token" aus liechtensteinischer Perspektive. LJZ 2019, 11; Jörg, M., Layr, A., Lettenbichler, M.: Übertragung von Rechten auf VT-Systemen, in Sild, TVTG-Sammelband (in press).

[45] Müller, T., Zysset, P., Kalaitzidakis, V.: Jusletter 20. Mai 2019, 8; Frésard, P., Heller, J.: Jusletter 9. September 2019, 6; so auch in Österreich: Miernicki, M.: in Kirchmayr-Schliesselberger/Klas/Miernicki/Rinderle-Ma/Weilinger, 138 (143 f).

[46] Jörg, M., Layr, A., Lettenbichler, M.: Übertragung von Rechten auf VT-Systemen, in Sild, TVTG-Sammelband (in press).

[47] Frésard, P., Heller, J.: Jusletter 9. September 2019, 7; Müller, T., Zysset, P., Kalaitzidakis, V.: Jusletter 20. Mai 2019, 9.

[48] Amt für Justiz: Merkblatt zur Liberierung von Gesellschaftskapital mit einer Kryptowährung, AJU/ h70.038.08 (2021), URL: https://www.llv.li/files/onlineschalter/Dokument-3306.pdf (abgerufen am 31.08.2021).

[49] URL: https://coinmarketcap.com/ (abgerufen am 31.05.2021).

[50] Amt für Justiz: Merkblatt zur Liberierung von Gesellschaftskapital mit einer Kryptowährung, AJU/ h70.038.08 (2021), URL: https://www.llv.li/files/onlineschalter/Dokument-3306.pdf (abgerufen am 31.08.2021).

[51] Amt für Justiz: Merkblatt zur Liberierung von Gesellschaftskapital mit einer Kryptowährung, AJU/ h70.038.08 (2021), URL: https://www.llv.li/files/onlineschalter/Dokument-3306.pdf (abgerufen am 31.08.2021).

[52] Diese Website wird im Merkblatt AJU/ h70.038.08 angegeben: URL: https://www.ictax.admin.ch/extern/de.html#/ratelist/2020, vermutlich müsste es aber nun die Website für 2021 sein, also: URL: https://www.ictax.admin.ch/extern/de.html#/ratelist/2021, (abgerufen am 31.08.2021).

[53] Amt für Justiz: Merkblatt zur Liberierung von Gesellschaftskapital mit einer Kryptowährung, AJU/ h70.038.08 (2021), URL: https://www.llv.li/files/onlineschalter/Dokument-3306.pdf (abgerufen am 31.08.2021).

[54] Vgl zum Normzweck in Deutschland: Gerber, O.: in BeckOGK, § 33 AktG, Rn 1 f (Stand 01.07.2020).

[55] Vgl zur Bewertung in Österreich: Miernicki, M.: in Kirchmayr-Schliesselberger/Klas/Miernicki/Rinderle-Ma/Weilinger, 138 (149 ff); zur Feststellung des Marktpreises von Kryptowährungen bei Kapitaleinlagen in der Schweiz: Frésard, P., Heller, J.: Jusletter 9. September 2019, 6.

[56] Patz, A.: BKR 2019, 435 (436); Nathmann, M.: BKR 2019, 540 (542).

[57] Vgl ausführlich zur Funktion des Geldes: Enz, B.: Kryptowährungen im Lichte von Geldrecht und Konkursaussonderung (2019), 51-83.

[58] Kanton Zug: Kanton Zug akzeptiert ab 2021 Kryptowährungen für Steuerzahlungen, URL: https://www.zg.ch/behoerden/finanzdirektion/direktionssekretariat/aktuell/kanton-zug-akzeptiert-ab-2021-kryptowaehrungen-fuer-steuerzahlungen (abgerufen am 31.08.2021).

[59] Vgl hierfür den Dienst von Bitpanda: Bitpanda: Verwende deine Investments wie Bargeld, URL: https://www.bitpanda.com/de/card (abgerufen am 31.08.2021).

[60] Mattheis, P.: Warum China Bitcoin mit eigener Kryptowährung Konkurrenz macht, URL: https://www.derstandard.at/story/2000124456395/warum-china-bitcoin-mit-eigener-kryptowaehrung-konkurrenz-macht (abgerufen am 31.08.2021).

[61] Kort, K., Dörner, A.: Einkaufen mit Bitcoin: Wer Kryptowährungen akzeptiert – und wer bald folgen könnte, URL: https://www.handelsblatt.com/finanzen/maerkte/devisen-rohstoffe/zahlungsmittel-einkaufen-mit-bitcoin-wer-kryptowaehrungen-akzeptiert-und-wer-bald-folgen-koennte/26898758.html (abgerufen am 31.08.2021).

[62] Bericht und Antrag der Regierung an den Landtag des Fürstentum Liechtenstein betreffend die Schaffung eines Gesetzes über Token und VT Dienstleister (Token- und VT-Dienstleistergesetz; TVTG) und die Abänderung weiterer Gesetze Nr 54/2019 (BuA), 11 ff.

[63] Vgl zur vergleichbaren Funktion: Zöllner, L.: Kryptowerte vs. Virtuelle Währungen, BKR 2020, 117 (119); Enz, B.: Kryptowährungen, 51-83.

[64] Amt für Justiz: Merkblatt zur Liberierung von Gesellschaftskapital mit einer Kryptowährung, AJU/ h70.038.08 (2021), URL: https://www.llv.li/files/onlineschalter/Dokument-3306.pdf (abgerufen am 31.08.2021).

Blockchain Based Machine-to-Machine (M2M) Communication and Digital Twins

Mohammad Ghanem, Wolfgang Prinz
RWTH Aachen University, Templergraben 55, 52062 Aachen
Fraunhofer FIT, Schloss Birlinghoven, 53754 Sankt Augustin

Over the last two decades, the rapid advances in digitization methods put us on the fourth industrial era's cusp. It is an era of connectivity and interactivity between various industrial processes that need a new, trusted environment to exchange and share information and data without relying on third parties. Blockchain technologies can provide such a trusted environment. This paper focuses on utilizing the blockchain with its characteristics to build machine-to-machine (M2M) communication and digital twin solutions. We propose a conceptual design for a system that uses smart contracts to construct digital twins for machines and products and executes manufacturing processes inside the blockchain. Our solution also employs the decentralized identifiers standard (DIDs) to provide self-sovereign digital identities for machines and products. To validate the approach and demonstrate its applicability, the paper presents an actual implementation of the proposed design to a simulated case study done with the help of Fischertechnik factory model.

1. Introduction

Until today, the industry has seen three major revolutions, and the fourth is on its way [1] . The fourth industrial revolution (Industry 4.0) represents the next step in the evolution of traditional factories towards smart, automated factories. These factories are designed to reduce production costs, increase productivity, improve quality, and achieve efficient use of resources. Many technologies can be used to achieve the industry 4.0 goals like Robotics, Autonomous Systems, the Internet of Things, Cloud Computing, Intelligent Data Analytics, Artificial Intelligence, and many more [2]. However, all these technologies rely on centralized networks and need to trust intermediaries or third-party operators [3]–[7]. As a result, the industry faces many challenges related to the data like transparency, security, privacy, and trustworthiness. These challenges prevent Industry 4.0 from reaching its full potential. A decentralized and trusted platform is needed to facilitate the relationships among parties. Such a platform can be built with the help of blockchain technologies.

Given its key features such as immutability, traceability, and reliability, it represents a perfect candidate to be integrated into Industry 4.0 factories. This paper aims to shed light on the blockchain's capability to improve the manufacturing industry and understand how blockchain can work with other technologies to overcome the earlier challenges. In particular, the paper focuses on two aspects of manufacturing. The first one is the communication between machines to enable the concept of machine-to-machine (M2M) communication over the blockchain, where one machine can ask another machine to perform a particular task without human involvement. The second one is tracking and tracing the machines and products while executing the manufacturing processes and building a digital representation with the blockchain's help. Our work will also show how this technology can provide a blockchain-based digital identity for both the machines and the products, by applying emerging standards in this area: the Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs) [8], [9].

The fine-grained objectives are the following:

- Build a digital twin of the machine using the blockchain. The digital twin should include information about the machine's functions and operations like tasks, sensor readings, alerts. It also should reflect the status of the machine.
- Build a digital twin of the product using the blockchain. The product's digital twin should include information about the operations performed on the product and related information.
- Provide a blockchain-based digital identity for the digital twins.
- Model the manufacturing process and its business logic using the blockchain. In other words, make all the communication between the machines go through the blockchain.
- The design should be generic and replicable to different use cases.

The remainder of the paper is structured as follows. Following the introduction section, we present the related work, which includes the literature review. Section 3 gives a conceptual design and modeling for the solution. Then section 4 proceeds by explaining the conceptual design's implementation details. Besides, it provides information about the case study used and its prototype. Section 5 presents the results with some screenshots of the final prototype. The last section summarizes the finding and discusses future work.

2. Related Work

There has been an increased interest in applying blockchain in the manufacturing industry in the past few years. We found two groups of work done in this area, and both are utilizing the blockchain in industrial applications. The first group focused on horizontal integration between manufacturing parties to enable manufacturing as a service between manufacturers themselves or between manufacturers and customers. For example, in [3], the goal is to build a trustless distributed network. Where different industrial organizations can collaborate and share information about manufacturing processes. The network was built using blockchain and smart contracts technologies. They stored information about manufacturers, machines, and their capabilities. A participant of this network can be a human, manufacturing machine, computing node, or an agent representing any organization.

Another work in the same direction is done in [5]. The authors integrated cloud manufacturing technologies with blockchain. The work proposed a distributed peer-to-peer network architecture to improve manufacturing cloud platforms' security and scalability. They used smart contracts to write the rules of the agreement between the end-users and the service providers. These rules contain the due date, quality measurement, and payment information. A similar approach can be found in [10]. The goal of this work is to improve communication between manufacturing service users and manufacturing services providers. A use case in the 3D printing manufacturing industry has been conducted, and the results showed that blockchain technologies could help solve some existing problems found in cloud manufacturing literature. In all these works that focused on horizontal integration, the authors neglected the actual manufacturing processes and focused more on the concept of trading using smart contracts. In other words, they did not consider what is happening inside the factories.

The second group focused on manufacturing processes by enabling M2M communication over the blockchain. One of the first research works that used the M2M concept with blockchain was done in [4]. The authors explored the applications of blockchain with Industry 4.0. They built a proof of concept where a blockchain is used to facilitate the interaction between machines. The goal is to enable the M2M electricity market, where industrial plants autonomously trade electricity over a blockchain. The agreement between the producer and the consumer is built using smart contracts. The information about the energy consumption (in kWh) published by the machines is stored as transactions in the blockchain. Each transaction has a fee (in USD) according to the agreement specified by the smart contract.

A similar approach has been followed in [7]. The authors focused on industrial M2M communication and how blockchain technologies can improve it. They introduced smart contract-based middleware for M2M communication to make it secure and decentralized. Through this middleware, IoT devices can communicate without the need for a trusted intermediary. The middleware controls and executes contracts to order tasks from field devices. Also, it monitors the field devices' states and executes actions based on a change in their state. It may also request a field device to perform service under a smart contract. All information about the actions and processes is recorded in the blockchain through smart contracts. This work emphasizes the real-time requirement for M2M communication in industrial processes. The result showed that smart contracts technology is still not mature enough to provide such an essential requirement.

Overall, in the second group of related work, the use cases were oversimplified and, in most cases, limited in size to only two machines. This does not reflect the actual communications between machines on the production line. They did not mention how the machines are being modeled in their systems, and this is an essential aspect of M2M-based systems because it will help build a fully autonomous manufacturing process. Also, none of the works discussed how the products are being modeled within the blockchain.

Another essential aspect is the identity management of the machines and the products. Each machine needs to know and identify other machines before establishing the communication. All the works we discussed used only the public/private key pairs as identities. This approach has many limitations and problems [11]. It makes the identity tightly coupled with the algorithm used to generate the key pair. None of the work spouted the issue of managing the digital identities of the machines or the products.

3. Conceptual Design

This section presents the conceptual design for an envisioned system that utilizes the blockchain to build M2M communication and digital twins solutions. The system is functioning alongside the existing infrastructure of the factory. It uses the blockchain to store and manage the data generated by the factory infrastructure. The data stored in the blockchain is used to build a digital representation of the machines and the products. Furthermore, all the communications between the machines go through the blockchain. Therefore, the system consists of the following three components:

- **Factory Infrastructure:** It represents all the existing hardware and software of the factory. It includes machines, sensors, and other devices. It also includes a client application that connects the factory infrastructure with the blockchain.
- **Blockchain:** It is the data storage and computational component of the system. It is the network of all the nodes processing the transactions and running smart contracts.

- **Web Application:** It is the application used by different actors to access the information stored in the blockchain. It consists of a front-end application and a blockchain client application.

The following figure shows a high-level diagram of the system components and the data flows between them.

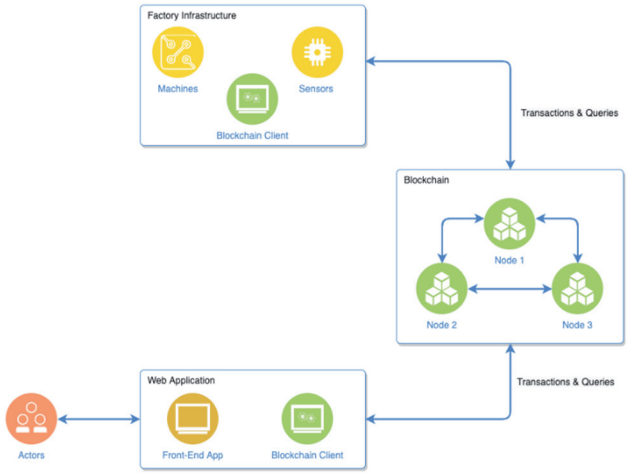

Fig. 1: High-Level System Overview

3.1. Machine Modeling

The machine is the main and the most crucial entity in the system. Our modeling is generic and can be applied to any machine. We use the term machine to refer to any factory component, including machines and robots of all sizes. We assume that the machine already has its digital representation provided by its manufacturer or third-party software. Each machine can perform several industrial tasks, and several processes can use the machine. There are no restrictions on the size and the complexity of the machine or its tasks.

3.1.1. Machine Digital Twin

We decided to model the machine as a smart contract to build the machine's digital twin in our system. Each machine will have a corresponding smart contract deployed into the blockchain. The smart contract with all the information stored within it represents the machine's digital twin created by the blockchain. Once the smart contract updates itself to include new information about the machine, it will be part of its digital twin, and it cannot be altered or changed. The ultimate goal when building a digital twin is to make a replica of the physical entity. However, we decided to limit the information included in the machine's digital twin to:

- **Identity:** The identity of the machine. More about the identity in the following section.
- **Basic Information:** Static information about the machine like the serial number, the model, manufacturing year, and similar info. Only the machine owner can provide such information, and once it is added to the digital twin, it cannot be changed.
- **Processes:** Information about the processes which use the machine. The authorized processes are allowed to assign tasks to the digital twin of the machine. The machine owner provides this information.
- **Tasks:** Information about the machine's tasks. It involves information about the starting time, finishing time, the parameters, the process, and the product.
- **Readings:** Any numeric information coming from the machine sensors like temperature or humidity. This information is sent by the physical machine and stored in the digital twin alongside the reading's timestamp.
- **Alerts:** Information about unexpected scenarios or failures. This information could be provided by the physical machine or by the digital twin itself. The digital twin can perform some logical checks as described later in this section and create alerts based on the check result.

All this information is managed and stored by the smart contract of the machine. Therefore, the machine's digital twin protects the information from being altered by unauthorized users or parties. However, all the information stored in the machine's smart contract will be publicly readable. So far, we have described the machine's digital twin as a registry of information. To go beyond this and make the digital twin of the machine an active component, we used the programmability feature of the blockchain. The smart contract of the machine can do complex programmable behaviors on the stored data. It could be programmed to perform conditions checks on the stored data and then do some actions once these conditions are verified. Of course, the physical machine can perform these checks by itself. However, having the digital twin to perform them will bring trust as the blockchain runs it. For example, it could be programmed to perform the following checks:

- **Product Quality Check:** This is a check performed to ensure that the product has some properties or meets a certain quality standard. The check might involve accessing the digital twin of the product.
- **Reading Values Check:** This is a check on the numerical values of the machine sensors. If a reading value, for example, the temperature, exceeded a certain threshold, the digital twin can do some actions like creating an alert.

3.1.2. Machine Identity

As we explained in the previous section, the machine's digital twin is an active actor. It needs a digital identity to facilitate communication and interaction with other entities of the system. The industrial and manufacturing systems have very long-life cycles, and therefore the identity of the machine should be the same during its lifetime. As our system is blockchain-based, identity

management cannot be based on traditional approaches. Otherwise, the objectives of the system cannot be achieved. The identity must be owned and controlled by the machine rather than stored or managed by a third party. Therefore, we decided to use a blockchain-based identity management approach. One of the emerging standards that use the blockchain features is Decentralized Identifiers (DIDs) [8]. Our system is using DID as a standard to manage the identities of the machines. Each machine has a permanent identifier called DID. A simple text string e.g. did:example:123456789abcdefghi. Each DID resolvable to a DID document that contains information associated with the identity of the machine. The DID document is stored within the blockchain, making the DID and its document persistent and immutable.

3.1.3. Twin Interaction

According to our modeling, the information between the physical and digital twins is being exchanged in both directions. The machine sends information stored in the digital twin and vice versa; the digital twin sends information to control and change the physical machine's behavior. Interacting with blockchain is done by participating in the network and running the client software of the blockchain platform. The details of this software may be different depending on the implementation of the platform. Regardless of this, every network node needs this client to process the transactions and validate/create blocks in the chain. Such functionality requires a large amount of storage and processing power as the node needs to have a full copy of the whole chain. The manufacturing machines could not have such capabilities to be a node and run the blockchain client software. Therefore, we decided that the physical machine will not run the blockchain client by itself. Instead, the physical machine will communicate via some protocol with a gateway running the blockchain client and acting like one of the blockchain nodes. The gateway will use the machine's private and public key pair to interact with the blockchain on behalf of the machine. An assumption has to be made regarding the communication channel between the machine and the gateway. We assume the channel is secured, and no attackers can alter or modify the messages exchanged between the machine and the gateway. Through this gateway, the machine will send data to its digital twin inside the blockchain.

So far, we have explained how the physical machine can send data to its digital twin. The next type of interaction is when the digital twin wants to notify or send data to the physical machine. As the machine's digital twin is a smart contract deployed on the blockchain, it runs in a closed execution environment and cannot directly interact with external systems. The only way the digital twin of the machine can communicate with the outside world is through events. The smart contract of the machine the following events to interact with the physical machine:

- **Task Assigned:** An event emits when a process assigns a task for the machine. The emitted event has all the information about the assigned task.
- **Task Started:** An event emits when the machine starts executing a task.
- **Task Finished:** An event emits when the machine finishes executing a task.

Anyone can watch these events, including the gateway. Once the gateway receives new events, it forwards them to the machine. Figure 2 illustrates the interaction between the machine and its twin while executing a task.

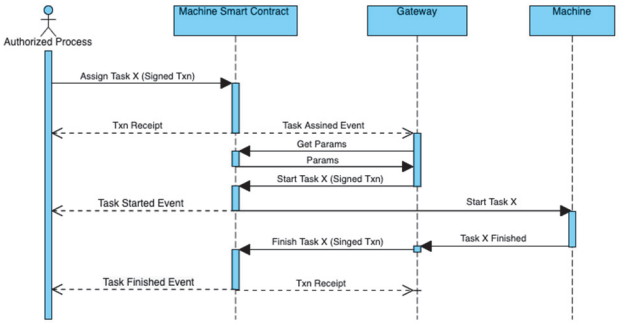

Fig. 2: Twins Interaction

The sequence starts when an authorized process assigns a task for the machine by calling a function on its smart contract. The contract emits a task-assigned event. The gateway is listening to the events generated by the smart contract of the machine. Once the gateway receives the task assigned event, it will first get its parameters and then send the task to the physical machine. At the same time, the gateway will call the start function on the machine's smart contract. Calling this function will store the starting time of the task and emit the 'Task Started' event. The physical machine is now performing the task. After it finishes the task, it will inform the gateway about the finished task. Then, the gateway calls the finish task function of the smart contract of the machine. This function call will store the finishing time of the task and emit the 'Task Finished' event. The machine might send information about the product operations being performed to the gateway during the task execution. The gateway takes this information and passes it to the machine's digital twin, which stores it in the product's digital twin.

3.2. Product Modeling

3.2.1. Product Digital Twin

The product is the second primary entity in our system. The product as an entity can be modeled in many ways. Lots of information can be stored throughout the product's life cycle. In our work, we focus only on what is happening during the manufacturing process inside the factory. Our modeling only takes into consideration simple non-compounded products, and the granularity is a single product. All the product information is stored in one smart contract called 'Product'. This information is provided autonomously by the machine's digital twins.

While the machine executes one of its tasks, the machine's digital twin will add this operation to the product's digital twin if the machine operates on the product. In this way, all the operations performed on the product by different machine is stored in one place, and they form the digital representation of the manufactured product. The contract stores the following information for each product:

- **Identity:** Information about the digital and physical identity of the product.
- **Operations:** This is general information about the operations performed on the product. Each operation is stored with a name, result, timestamp, and information about the machine that did this operation.
- **Processes:** Information about the authorized processes allowed to modify the digital twin of the product.

3.2.2 Product Identity

For the product identity, we are using the same identity management as the machine. Each product has a DID associated with it.

3.2.3 Product Credentials

Besides having the product information stored on-chain in the digital twin, the product has off-chain credentials. For every operation performed on the product, it receives an offline credential/claim from the machine. The credential can be verified by a third party to ensure its authenticity. To achieve this, we used the emerging standard from the W3C, which is called Verifiable Credentials (VCs) [9]. This standard fits well with the DID standard we used to build identity management. The machine is the issuer of the credential, and the product is the subject. It creates the credential containing information about the product, the operation, the machine's DID, and cryptographic proof. The product can claim it underwent a particular operation or satisfied a certain standard by presenting the corresponding credential to a verifier. The verifier can check the machine's DID document (the issuer) and cryptically verify the claim's authenticity. Having each operation as a separate credential allows the product to present the needed information to the verifier without revealing other information that might be sensitive.

3.3. Manufacturing Process Modeling

The actual manufacturing processes in real life tend to be complicated and consist of several stages or even sub-processes. Each one of them involves a lot of machines and devices. We are considering a simple manufacturing process that consists of several steps and no sub-processes. Each step is a high-level task performed by a specific machine, such as fetching an empty container. We also assume that the process is fixed. In other words, the steps, their order, and the corresponding task types are known in advance. However, the machine allocation is dynamic. So, the machine executing a specific task can be replaced by any other machine that can do the same type of task. Executing the process requires communication and interaction between the digital twins of the machines involved in the process.

3.3.1 Process Structure

We modeled the manufacturing processes as smart contracts. Each process is a smart contract written by a manufacturer and running on his behalf on the blockchain. The smart contract is programmed to assign tasks to the digital twins of the machines. The smart contract consists of several functions. Each function represents a step in the process. The function body assigns the task to the machine and executes other business logic if necessary. The contract is responsible for starting/finishing the execution of the process instances. For each execution, the contract creates a process instance and stores information like the starting time, the finishing time, and the execution status.

3.3.2 Process Execution

The process execution is done with the help of a client, which also runs in the gateway. The communication between the client and the smart contract of the process is done the same way explained in the twin interaction section. The client calls functions in the smart contract by signing transactions, and the smart contract emits the following events to communicate with the outside world:

- **Process Started:** An event emits when a process instance is started. The emitted event has all the information about the started instance.
- **Process Step Started:** An event emits when a process step is started.
- **Process Finished:** An event emits when a process instance is finished.

The client will be listening to these events and other events from machines' smart contracts. The execution is carried on by the client calling the process functions. Each function represents a step in the process, and the function call assigns a task to the corresponding machine. Before executing the process, the addresses of the digital twin of the involved machines must be supplied into the smart contract. It starts when the owner or an authorized actor triggers the process by calling the start function, which emits the 'Process Started' event. The client then calls the first step function, which assigns the first task of the process to the corresponding machine. Now the machine will work on the task as we explained in a previous section. Once the machine finishes its task, and the task finished event is emitted from its digital twin, the client can resume the execution by calling the second step function, assigning the second task to the responsible machine.

The execution continues in the same way until the process finishes all its steps, and then the 'Process Finished'

event is emitted. Before assigning each task, the process's smart contract needs to authorize the machine if the task involves performing product operations. During the execution of the process, the smart contract of the process can access the digital twin of the product or the machines' digital twins and get data from them. In such a way, the smart contract will enforce the manufacturing process's rules and requirements. With this modeling, the machines act as separate entities and can be used by several processes.

To illustrate the execution, we present an example of a process that involves two machines. Each machine has its digital twin as a smart contract deployed into the blockchain. These two machines belong to different owners and might be in different locations. The process owner (the manufacturer) decided that his process needs two machines capable of doing task 1 and task 2. The manufacturer writes and deploys the smart contract of the process, including all the business logic that implements the argument between him and the machines' owners. The following figure shows the sequence diagram for executing this example process.

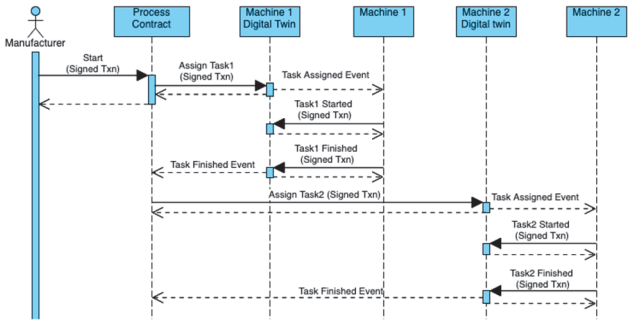

Fig. 3: Process Example

All the interactions between the machine and its digital twin go through the gateway. The gateway was omitted from the diagram for simplicity. However, the machines and the manufacturer might be using different gateways to access the blockchain in this process.

4. Implementation

To validate our conceptual design and modeling, we implemented it for a case study done with the help of the Fischertechnik Learning Factory [12]. The factory model is shown in figure 4. It has a built-in program that depicts the ordering, production, and delivery processes in digitized and networked steps. The factory model comes pre-configured and programmed to perform a set of built-in demo scenarios controlled and monitored through an online dashboard. Even though the Fischertechnik factory model is a fully functional simulation, we had to customize it to fit our needs. We split the factory into four machines Vacuum Gripper Robot (VGR), High-Bay Warehouse (HBW), Multi-Processing Station with Oven (MPO), and Sorting Line with Color Detection (SLD). Each machine has one or more task types. The machines collaborate to perform two processes, namely the supplying process and the production process.

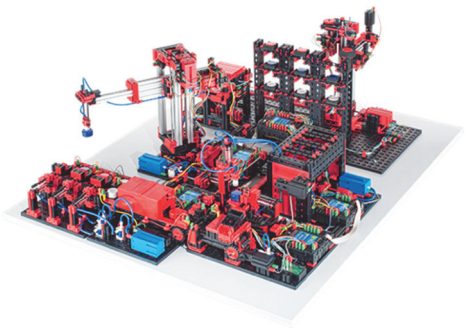

Fig. 4: Fischertechnik Factory Model

The implementation of this prototype was made using Ethereum blockchain with the help of open-source libraries and frameworks like Truffle, Ganache, Open Zeppelin, Web3.js, and others.

4.1. Smart Contracts Implementation

4.1.1. Machines

To make the implementation of the machine smart contract generic, we decided to use the template method pattern by making the machine contract an abstract contract. This abstract contract contains all the functionality mentioned in the machine modeling section, shared between all machines. In this way, all digital twins of our system will have the same interface, so other components can interact with any machine if its smart contract extent the abstract base contract. For a new digital twin of a machine to be created in the system, the machine's smart contract must extend the abstract machine contract. The new contract must implement few abstract functions to define the tasks and their types. The custom functionality can then be added to the child contract by using/overriding the parent contract's functions. The child contract can also implement and enforce custom rules or business logic by overriding the abstract contract's functions. For example, one machine can override the 'save reading' function and check the reading value. If the value is below/above a certain threshold, an alert will be created by calling the 'save alert' function.

4.1.2. Products

The implementation of the product digital twin is a single, smart contract called 'Product'. The contract stores information about all products of the system. The product smart contract allows creating a product by calling the create product function. The function takes an Ethereum address as the DID of the product and creates a record for this product. The caller of this function will be the product owner, and it cannot be changed. The product owner can add info to the product's digital twin using the web application by calling the corresponding functions and signing transactions with his keys. As we explained in the modeling section, the product smart contract authorizes processes that can authorize machines to modify the digital twin of a single product. The authorized machine can save the operations performed on a particular product in its digital twin. Operations info

and their results can be accessed later by smart contracts to ensure that they meet specific requirements. Another essential info stored about the product is the physical identifier. The identifier could be an NFC UID or a barcode. It is used to access the digital twin of a product and get all the information about it. Another way of retrieving the info is using the product's DID, an Ethereum address.

4.1.3. Processes

The implementation of processes uses the same approach as machines. Therefore, we created an abstract smart contract called Process to include all processes' standard functionality. For a new process to be created in the system, the smart contract must extend the abstract process contract and implement the functions that define the number of machines, the number of steps of the processes, the order of execution, and the process name.

After deploying the process smart contract, the process owner must set the smart contract address for every machine involved in the process. The machine address can be changed at any time but only by the owner of the process. The process can then be started on a particular product by calling the start process function, which takes the product's Ethereum address (DID) as an argument. The start process function calls the authorize process function in the product smart contract to authorize itself. Only the product owner can authorize a process; therefore, the product owner can only call the start process function.

Once the process owner calls the start function and the corresponding transaction is confirmed, the contract emits the 'Process Started' event. The process client which runs in the gateway will be listening to this event type. After the process contract emits the starting event, the client will begin executing the process by calling the first step function. All steps functions take the process instance ID as an argument, and inside each of them, the corresponding task is assigned to the machine by accessing its digital twin and calling the assign task function. In addition to this, custom functionality can be part of the step function body. The process client is also listening to the task finished events emitted by the machine smart contracts. Whenever a machine finishes a task assigned to it, the process client will trigger the next step, which assigns the next task in the process. This execution continues until the process reaches its final step. Then the process client calls the finish process function to mark this instance of the process as finished.

4.2. Identity Implementation

We used the DID standard to assign digital identities for machines and products. The DID standard is just a specification, and the implementation details are left to the DID method. There are many DID methods available with a functional implementation. Each one of them has different functions, but all of them comply with DID specifications. We used the ethr DID method developed by uPort. The ethr method uses the registry specified by the ERC 1056 which is available as an open-source project [13]. The implementation of the verifiable credentials in our system is based on the library called did-jwt developed by Decentralized Identity Foundation [14]. It allows signing and verifying JSON Web Tokens (JWT), and all public keys are resolved using DIDs. The library support ethr DID method alongside many other methods. In our case study, the signer is the machine, and the subject receiving the credential is the product. Each machine client uses the library to sign a credential using its DID. The content of the credential could be anything if it is a valid JSON object. In our implementation, the credential content is information about a product operation. Anyone interested in verifying the credential can use the library or a similar library to check its validity. Under the hood, the library access the DID registry to check the credential signer's validity. We build a verifiable credential resolver to decode the credential and verify its validity.

5. Results

The implementation result is a fully functional prototype of the conceptual design applied to the Fischertechnik factory. The prototype includes a distributed web application (DApp) that allows different actors to interact with the machines, products, and processes through the blockchain. It provides dashboards to monitor and control manufacturing machines and processes that run autonomously by smart contracts. The following are some of the web application user interfaces. As the web user interface is big and cannot fit in one image, some images are not a full user interface but rather a snippet that shows a particular part of the interface.

Dashboard Interface

This interface shows three kinds of information: machines' current status, processes' current status, and events log. The current machine's status is coming directly from the machine's digital twin for each machine. The web application is listening to the smart contract events, and based on the emitted events, it changes the machine's status in the UI. The upper part of the interface shows the status of the Fischertechnik machines.

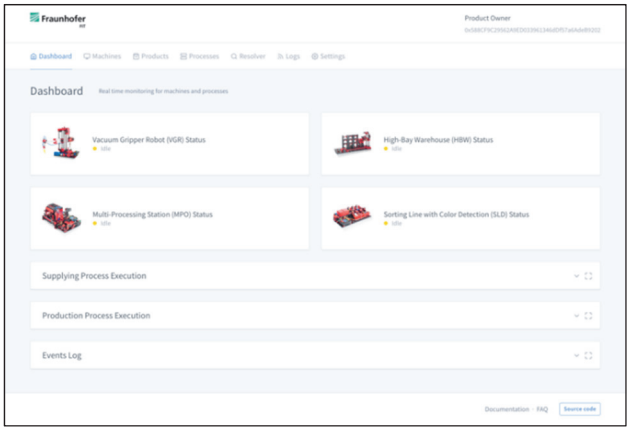

Fig. 5: Dashboard UI

Machine Interface

This interface displays the information stored in the digital twin of the machine. It includes information about tasks, readings, and alerts with links to the corresponding pages. Other information about the machine like the DID, the machine owner, the contact address is also presented. Moreover, the interface also lists the authorized processes with an option to unauthorize them. The following figure shows the interface for the SLD machine. There are three other similar interfaces for the rest of the Fischertechnik machines. This interface can display the information for any machine if its smart contract is inherited from the base Machine contract.

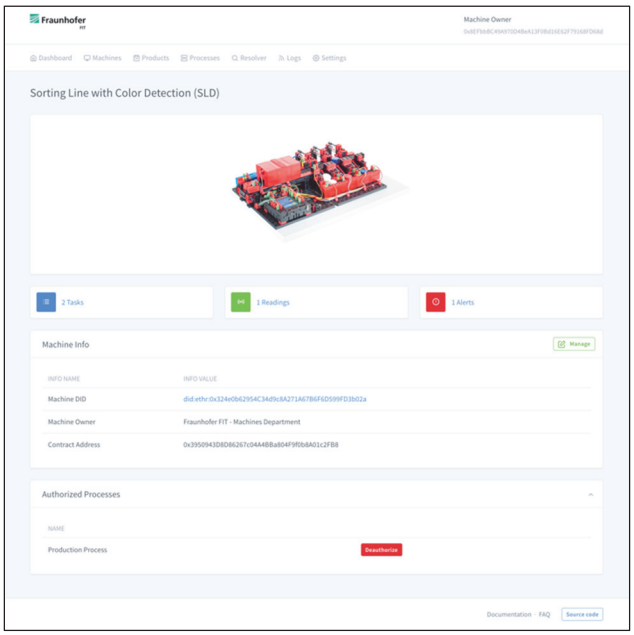

Fig. 6: Machine UI

Product Interface

This interface shows information about the digital twin of the product. Information about the product like the DID, owner name, owner address, and the creation time is displayed. Furthermore, it shows all the operations performed on this product by different machines. Figure 7 shows the information about a product that went through three operations by two machines. For each operation, a link to the corresponding verifiable credential is provided. The verifiable credential resolver interface is used to display the credential's details by clicking on the link.

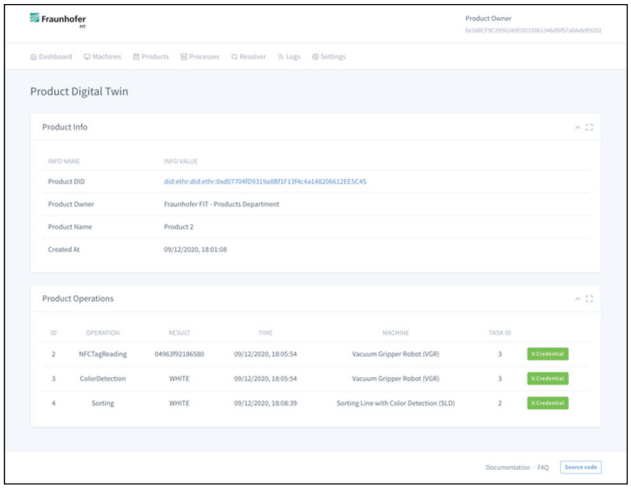

Fig. 7: Product UI

Process Interface

This interface displays the process information, including the number of instances, machines, and steps. Also, it allows starting the process on a particular product by providing the DID product. The execution can be tracked with the same UI compound used in the dashboard interface if the process is started. Figure 8 shows the interface for the Fischertechnik factory model's production process.

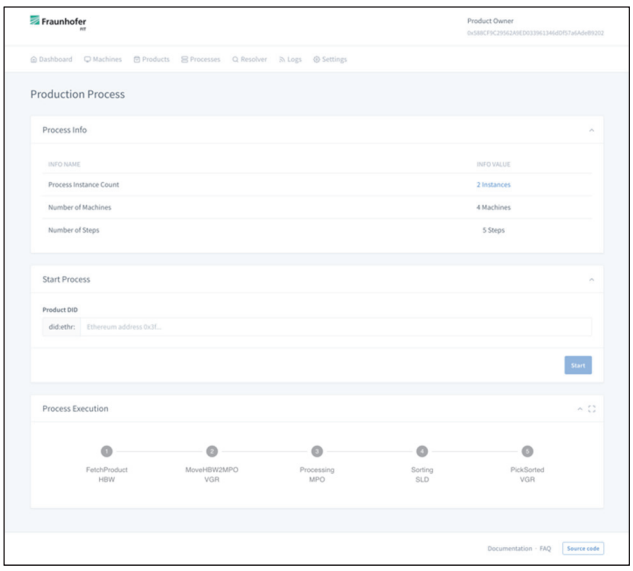

Fig. 8: Process UI

5.1. Source Code

The source code of the implementation is divided into two parts. The first one is the source code for the Fischertechnik factory model. It is a fork of the source code provided by the manufacturing company [15]. In this fork, we made the necessary changes to implement the presented scenarios. The second part is the source code of the smart contracts, the gateway, and the web application [16]. Inside the source code repositories, the Readme file contains technical details on how to get started with the code and run it and other implementation aspects that were not discussed in this paper.

6. Conclusion

This paper investigated the applicability of blockchain in the manufacturing industry. Our main contribution was building a generic conceptual design for a system that utilizes blockchain and smart contract technologies to implement M2M communication and digital twins for machines and products. The conceptual design discussed how machines, products, and manufacturing processes are modeled as smart contracts. The modeling defined which information is stored in the digital twins of machines and products. We showed how the digital twin and the physical machine could interact and share information. We also spouted the blockchain-based identities for both the machines and the products. The design also discussed how M2M communication is implemented and executed through the blockchain.

Different aspects could be improved upon in our work, which forms a basis for future work. Our modeling for the digital twin of the machine only included the operational aspect of the machine. However, there is much information directly related to the machine's operational conditions, like maintenance operations. Extending the digital twin information by considering other aspects of the machine will allow building more services that fit the industry 4.0 needs. M2M communication represents another area of interest. It was modeled in our design to fit particular types of manufacturing processes. Additional work needs to be done in order to make it applicable to other types of processes. Another direction to improve the process modeling is to use model-driven engineering. It allows auto-generation of the smart contract source code instead of writing it manually.

Even using our conceptual design without modification can still provide a foundation for building other services and applications. The smart contracts of the machines and the processes can be extended to enforce any custom logic. It can be a business logic to implement the payment between the machine owner and the product owner. Alternatively, it can be used to implement the warranty agreement between the machine owner and the maintenance company. Lastly, some technical aspects of the solution can be improved. For example, the interaction between the machine and its digital twin can be optimized by eliminating the gateway role and letting the machine interacts directly with the blockchain.

References

[1] A. Rojko, "Industry 4 . 0 Concept : Background and Overview," vol. 11, no. 5, pp. 77–90, 2017.

[2] T. M. Fernández-caramés and S. Member, "A Review on the Application of Blockchain for the Next Generation of Cybersecure Industry 4 . 0 Smart Factories," 2018.

[3] A. Angrish, B. Craver, M. Hasan, and B. Starly, "A Case Study for Blockchain in Manufacturing: 'fabRec': A Prototype for Peer-to-Peer Network of Manufacturing Nodes," *Procedia Manufacturing*, vol. 26, pp. 1180–1192, 2018, doi: 10.1016/j.promfg.2018.07.154.

[4] J. J. Sikorski, J. Haughton, and M. Kraft, "Blockchain technology in the chemical industry: Machine-to-machine electricity market," *Applied Energy*, vol. 195, pp. 234–246, 2017, doi: 10.1016/j.apenergy.2017.03.039.

[5] Z. Li, A. V. Barenji, and G. Q. Huang, "Toward a blockchain cloud manufacturing system as a peer to peer distributed network platform," *Robotics and Computer-Integrated Manufacturing*, vol. 54, no. January, pp. 133–144, 2018, doi: 10.1016/j.rcim.2018.05.011.

[6] M. Y. Afanasev, Y. V. Fedosov, A. A. Krylova, and S. A. Shorokhov, "An application of Blockchain and Smart Contracts for Machine-to-Machine Communications in Cyber-Physical Production Systems," no. May, 2018, doi: 10.1109/ICPHYS.2018.8387630.

[7] C. Garrocho, C. Marcio Soares Ferreira, A. Junior, C. Frederico Cavalcanti, and R. R. Oliveira, "Industry 4.0: Smart Contract-based Industrial Internet of Things Process Management," pp. 137–142, 2019, doi: 10.5753/sbesc_estendido.2019.8649.

[8] DID-Core, https://www.w3.org/TR/did-core/ (accessed Jan. 15, 2021).

[9] VC-Data-Model, https://www.w3.org/TR/vc-data-model/ (accessed Jan. 15, 2021).

[10] A. V. Barenji, Z. Li, W. M. Wang, G. Q. Huang, and A. David, "Blockchain-based ubiquitous manufacturing: a secure and reliable cyber-physical system," *International Journal of Production Research*, vol. 0, no. 0, pp. 1–22, 2019, doi: 10.1080/00207543.2019.1680899.

[11] X. Zhu and Y. Badr, "Identity management systems for the internet of things: A survey towards blockchain solutions," *Sensors (Switzerland)*, vol. 18, no. 12, pp. 1–18, 2018, doi: 10.3390/sxx010005.

[12] Fischertechnik, https://www.fischertechnik.de/en/products/teaching/training-models/ (accessed Jan. 15, 2021).

[13] uPort, https://github.com/uport-project/ethr-did-registry (accessed Jan. 15, 2021).

[14] D. Identity, https://github.com/decentralized-identity/did-jwt/ (accessed Jan. 15, 2021).

[15] M. Ghanem, https://github.com/ghanem-mhd/txt_training_factory/ (accessed Jan. 15, 2021).

[16] M. Ghanem, https://github.com/ghanem-mhd/master-thesis-implementation (accessed Jan. 15, 2021).

SAIRA – The Open Innovation Hub for Sustainable Development

Sabine Kolvenbach[1], Andrei Ionita[1], Urs Riedlinger[1], Rudolf Ruland[1], Dominik Reinertz[2], Anna Wohlrab[2]

[1]Fraunhofer FIT, Schloss Birlinghoven 1, 53757 Sankt Augustin, Germany

[2]Fraunhofer Gesellschaft, Schloss Birlinghoven, 53754 Sankt Augustin, Germany

Global challenges like climate change, food security, and infectious diseases such as the COVID-19 pandemic are nearly impossible to tackle when established experts and upstart innovators work in silos. If research organizations, governments, universities, NGOs, and the private sector could collaborate on these challenges more easily, lasting solutions would certainly come more quickly. Aligned with the United Nations' Sustainable Development Goals, SAIRA connects key players in different arenas: scientists and engineers at research and technology organizations (RTOs) looking to collaborate on sustainable development projects, companies seeking R&D support to tackle their most challenging problems, and startups with innovative ideas and a desire to scale. The platform is a blockchain-secured open innovation platform, anchored on Max Plank Digital Library's blockchain network bloxberg, that assures the authenticity and integrity of all user-generated content and collaboration processes.

1. Introduction

The United Nations' Sustainable Development Goals (SDG) [1] address the major challenges that people from developing countries and the planet are currently confronted with. The 17 SDGs have been adopted by all United Nations Member States and highlight a series of objectives such as ending poverty, improving health and education, spurring economic growth, and tackling climate change. Such goals are to be achieved in a global partnership by both developing and developed countries. The World Association of Industrial and Technological Research Organisations (WAITRO) [2] helps with bringing the SDGs to fruition. WAITRO's mission is to connect science, technology, and innovation stakeholders such as universities, research institutions in order to share their solutions and tackle global challenges such as the SDGs.

The SAIRA® platform was developed for the purpose of connecting researchers, companies**,** and organizations to share ideas, forge partnerships, generate synergies and promote technology. Members of the WAITRO have been using the SAIRA® Open Innovation Hub since early 2019. With SAIRA 2.0**,** we have extended the platform to a digital gateway for R&D service providers from around the world that enhances collaborative innovation. It focuses on international collaborations for the SDGs, is guided by principles of inclusiveness – publicly available and free of charge, and designed to deliver applicable solutions with benefits for societies and economies**.**

This paper presents the relaunched version of the SAIRA platform by highlighting its key features:

- An intuitive user interface that facilitates easy matchmaking between solution seekers and innovation providers
- Blockchain integration to secure the user-generated content and protect the intellectual property of the authors
- A self-sovereign identity concept to manage the actors' identities and data

The paper is structured as follows. After the introduction, a general overview of the platform is offered, with section 3 including more technical aspects of the architecture. Section 4 goes into detail about the blockchain integration, before the conclusion wraps up the results and provides some incentives to join the platform.

2. Platform Overview

The main purpose of SAIRA is to connect innovative ideas with knowledge and technology. Visitors of the SAIRA platform can browse published opportunities and search for opportunities that may be of interest and match their professional background (cf. Figure 2). To find ideal collaboration partners for implementing project ideas, a wizard guides SAIRA users through the creation of an opportunity.

In the first stage, an opportunity consists of an abstract that summarizes the challenge, the research areas targeted, and optionally a deadline for proposals. If the solution seeker is applying for a grant, (s)he should inform its collaborators about the respective timeline. Furthermore, the user may provide an in-depth description of the challenge and specify the expected contribution of the partners, as well as their expected geographical location.

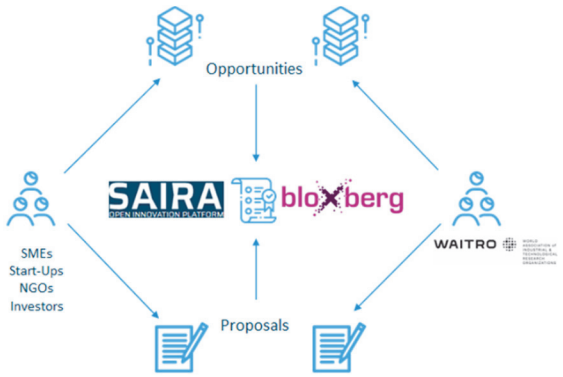

Fig. 1: SAIRA the matchmaking platform

When a SAIRA user finds an opportunity of interest and wants to contribute, (s)he can propose an idea towards tackling the opportunity. The proposal must include a detailed description on how to contribute, as well as information about the professional background of the author and his/her expertise. For initial clarifications, the user can contact the author of the published opportunity. When the user submits the proposal, the author of the opportunity receives an email notification and gets access to the proposal. Ultimately, the author of the opportunity may connect with the author of the proposal and start a collaboration by accepting the proposal.

The platform additionally offers the users a community panel where the profiles of platform users can be browsed, thus facilitating finding collaboration partners. During opportunity and proposal preparation, users can invite partners to their project and collaboratively develop their project idea.

SAIRA uses the Bloxberg blockchain to secure the submitted proposal against manipulation and to guarantee the authenticity and integrity of all registered data. Also, the acceptance and rejection of a proposal is protected by the bloxberg blockchain and respective transactions can be retrieved at any time.

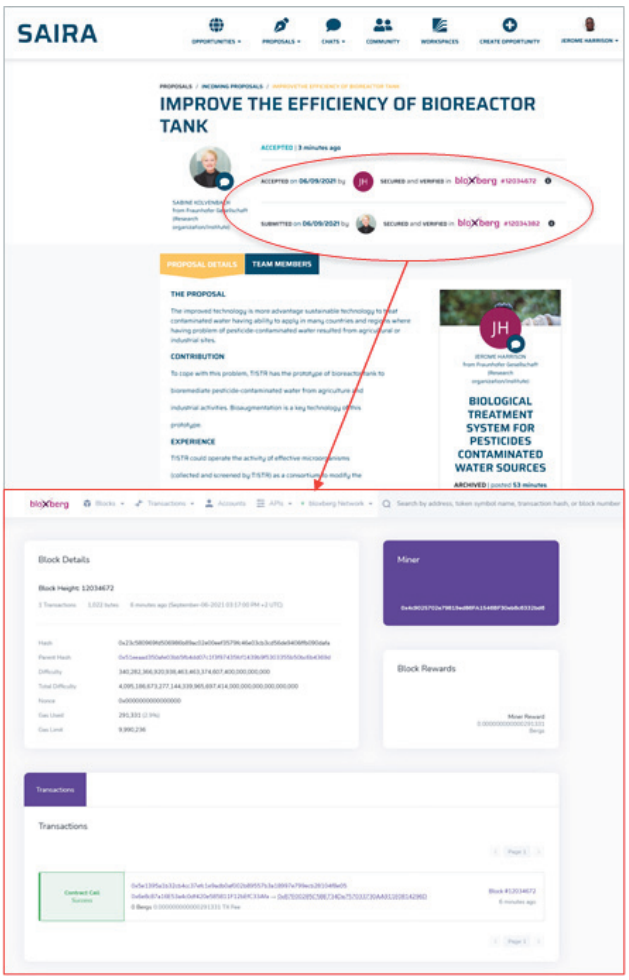

Fig. 2: Proposal submitted to an opportunity and secured in bloxberg

3. Platform Architecture

The SAIRA frontend has a responsive design; it is implemented in Angular and Bootstrap and integrated with the SAIRA backend and the bloxberg blockchain through a REST API.

SAIRA® is an adaptation and extension of the BSCW Shared Workspace System. BSCW [3] is continuously developed jointly by Fraunhofer Institute for Applied Information Technology FIT and Orbiteam GmbH & Co. KG [7] and has been successfully marketed by Orbiteam GmbH & Co. KG for more than 20 years.

The blockchain used to secure the application content is bloxberg, a worldwide network of research organisations that provides scientists with decentralized services for research collaboration. The network was launched in 2019 by the Max Planck Digital Library. Thanks to the blockchain properties of decentrality, coordinated consensus, and transaction validation, various services that are decentralized by nature are enabled, such as supporting research claims, paper peer review, research data certification, etc.

bloxberg is developed as a permissioned Ethereum blockchain and functions based on a Proof by Authority

consensus, i.e., the AuRa algorithm [8]. Ethereum is currently the most widely used blockchain technology, supports a relatively large number of decentralized applications (dapps) and has been proven to be resilient and stable against attacks.

4. Blockchain Integration

The blockchain backend of the platform fulfills the function of a notary. At its center, it has smart contracts that implement the business logic. Besides securing the hash of a contribution in the blockchain, the smart contracts provide functions to retrieve the stored content, both in its current and previous versions (cf. Table 1).

name	function
save	stores a proposal record in the blockchain
latest	retrieves the latest proposal record given a proposal id
versionCount	retrieves the proposal record that matches the proposal id and version index
pastVersion	retrieves the proposal record that matches the proposal id and version index
id	returns a list of proposal ids and version indexes that match the checksum provided

Table 1: The features implemented by the smart contracts

The main smart contract uses a storage contract for saving its data, which prevents any data loss in case of an update of contract's main functions. The storage contract provides a key-value storage for the basic data types by mapping the hash of the variable to its value. More complex data types, e.g., arrays, mappings, are stored using the same key-value mappings, in addition to which the name and size of the structure are likewise stored.

The smart contracts are deployed over a non-authority node to the bloxberg network dedicated to dapps. The interface to the blockchain functionality is realized by a REST API that forwards the requests to the main smart contract (cf. Figure 3).

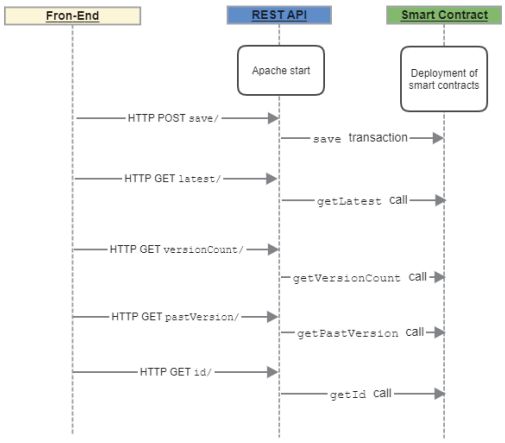

Fig. 3: A sequence diagram shows the request flow in the system

The smart contracts and the API are bundled as two containers in a docker-compose environment. The smart contracts are written in Solidity. Their compilation and deployment are performed using the web3 library. The REST API is run as Apache server and is implemented in Python using the Flask library.

With the advent of self-sovereign identity, extensions to the blockchain model can be implemented. The platform users can be assigned decentralized identifiers (DIDs) which wrap around the public/private key pairs that are used to sign content and for user verification. In return for submitting contributions to the platforms such as opportunities and proposals, verifiable credentials (VCs) can be issued by the platform to certify the user's contribution. The VCs are to be stored in the user's wallet and can be presented as evidence for the submitted content. The DIDs are stored in the ledger, so that the signature verification can be performed with public data (cf. Figure 4).

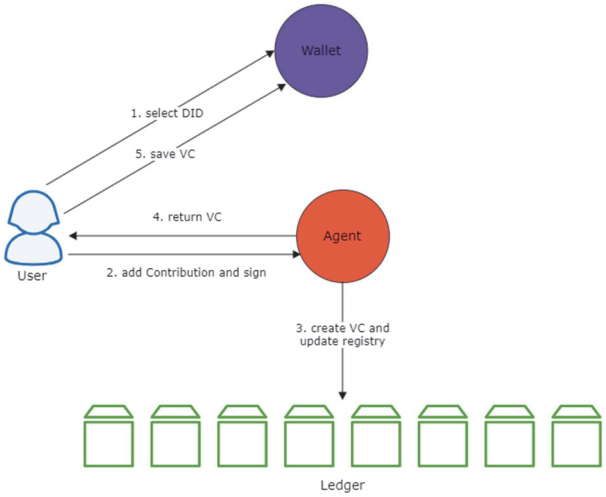

Fig. 4: SSI-enhanced model for SAIRA

5. Conclusion and Incentives to Join

The redesigned platform follows the over 50 success cases of small bilateral cross-border collaborations that were achieved with the previous platform version in 2019-2020. Since the relaunch in June 2021, more than 360 users have registered on SAIRA and more than 50 opportunities with innovative project ideas, local challenges, and collaboration needs have been published. Using a blockchain backend that backs up the proposals in one of the world's fastest growing research networks, bloxberg, SAIRA is aiming to add more features in the future in order to facilitate more matches and help advance the United Nations' Sustainable Development Goals.

WAITRO offers incentives to start using the new SAIRA platform, such as the WAITRO Innovation Award [5]. Two project teams who match on SAIRA get the chance to win 25.000 USD seed funding and training. This year's Innovation Award focuses on solutions that contribute to

food security and sustainable agriculture (SDG 2-Zero Hunger). Moreover, WAITRO provides support for consortia matched on SAIRA that are planning to submit proposals to the highly competitive Horizon Europe program by financing external reviewers who examine applications and offering guidance on research ethics and equitable partnerships [6].

Acknowledgements

The development of SAIRA was supported by the Fraunhofer Internal Programs under Grant No. Anti-Corona 114-600011 and by the German Federal Ministry of Education and Research.

References

[1] 'THE 17 GOALS | Sustainable Development'. https://sdgs.un.org/goals (accessed Sep. 26, 2021).

[2] 'WAITRO - The Global Innovation Family'. https://waitro.org/ (accessed Sep. 26, 2021).

[3] 'BSCW | Groupware for efficient teamwork and document management'. https://www.bscw.de/en/ (accessed Sep. 26, 2021).

[4] W. Prinz and A. T. Schulte, 'Blockchain and Smart Contracts. Technologies, research issues and applications', 2018, p. 25.

[5] 'WAITRO Innovation Award'. https://waitro.org/programs-services/waitro-innovation-award/ (accessed Sep. 26, 2021).

[6] 'WAITRO Project Support for Horizon Europe'. https://waitro.org/programs-services/horizon-europe-project-support/ (accessed Sep. 26, 2021).

[7] 'Unternehmen – BSCW | Groupware für effiziente Teamarbeit und Dokumentenverwaltung'. https://www.bscw.de/company/ (accessed Sep. 28, 2021).

[8] 'Aura Consensus Protocol Audit · poanetwork/wiki Wiki · GitHub'. https://github.com/poanetwork/wiki/wiki/Aura-Consensus-Protocol-Audit (accessed Sep. 28, 2021).

Developing a blockchain-based prototype for wind turbine fasteners

Andrei Ionita[1], Kristoffer Holm[2], René Chester Goduscheit[2], Per Hessellund Lauritsen[3], Wolfgang Prinz[1], Kim Nedergaard Jacobsen[4], Kristoffer Isbak Thomsen[5]

[1]Fraunhofer FIT, Schloss Birlinghoven 1, 53757 Sankt Augustin, Germany

[2]Aarhus University, Birk Centerpark 15, 7400 Herning, Denmark

[3]Siemens Gamesa Renewable Energy A/S, SGRE OF TE, Borupvej 16, 7330 Brande, Denmark

[4]APQP4Wind, Lysbrohøjen 24, DK-8600 Silkeborg, Denmark

[5]Vestas Wind Systems, A/S, Hedeager 428200 Aarhus N, Denmark

The wind energy sector is undergoing digitalization processes that span multi-tier supply chains of turbine components and wind farm maintenance, amongst others. In an industrial use case that includes Siemens Gamesa Renewable Energy, Vestas and APQP4Wind, the processes of producing, fastening, and servicing bolts in turbines are mapped to a digital model. The model follows the lifetime of turbine bolts from the manufacturing phase, to fastening in turbines and maintenance, until their replacement and recycling. The development of the digital model is iteratively addressed in a design science research approach, as the authors actively contribute to the project. Distributed ledgers (DLs) support the notary documentation of the bolts and turbines, from their registration phase to the assembly-, technical service verification- and recycling phases. The immutable and decentralized nature of DLs secures the data against tampering and prevents any changes taken unilaterally by engaging the service stakeholders and component providers in a blockchain consortium.

1. Introduction

The wind turbine industry contributes increasingly higher amounts of energy into the network grid and is a key pillar amongst renewable energy sources. As an example, in Denmark almost half of the power in 2019 was produced from wind [1]. At the same time, the wind industry is in a process of digitalization. The wind industry supply chain is going through a substantial consolidation in terms of reduction of the number of suppliers for the wind turbine manufacturers. Vertical, digital integration within the supply chain is instrumental in this consolidation process.

Blockchain, on the other hand, is amongst the technologies that are advancing digitalization and digital transformation alongside Internet of Things, Big Data, 3D printing, etc.

The contributions of this paper are as follows:

- A mapping of the bolt fastening use case to a digital model is developed by identifying the data and processes involved.
- A blockchain network with the focus on smart contracts that implement the established process functionality and manipulate the identified data records is conceptualized.
- Access roles for the users in the network that regulate the access permission to the various data resources are elaborated.
- The designed smart contracts are implemented in a test Ethereum-based blockchain network.

The structure of the paper is as follows. Following the introduction, the current research on related use cases is summarized; next, the use case investigated in the paper is described in detail and a digital model mapping is elaborated; following is a description of the blockchain concept alongside the reasons for which the technology was selected; next, the proof of concept implementation of the blockchain solution is being presented; the conclusion summarizes the digital transformation process and points out further possible improvements.

2. Related Work

The presented use case is part of the UnWind project that is funded by the Danish Industry Foundation [2]. The overarching goal of the project is to increase innovation in the wind turbine industry and its supply chain while strengthening cooperation between the involved parties, both wind turbine manufacturers and subcontractors. By using the blockchain technology, which has properties such as decentralization and transparency at its core, the collaboration between the network participants will increase by the implicit sharing of resources and participation in the network governance. Holm [3] elaborates on the maturity of the blockchain as technology and its adoption in the wind industry in the context of the UnWind project.

Some of the applications of the technology have been targeted at energy use cases and the smart grid [4][5] or digitalization in the wind industry as a whole [6]. Other studies have investigated adjacent topics to the one that this paper addresses, such as the quality control in the supply chain of wind turbine blades and its traceability

wins [7]. Worth mentioning is also the blockchain application to manage large amounts of data produced by offshore wind energy supply chains that achieves traceability and visibility [8].

3. Digital Model

The use case discussed in this paper follows the lifetime of bolts, from the creation- to recycling phase, as well as the maintenance process of fastening and replacing bolts in turbines.

3.1. Use Case

In the following section, the data and processes involved in this use case are described in detail.

A turbine bolt, or fastener, is designed to hold the turbine parts together and is a key element in the security of the turbine. We will further refer to a turbine-purposed bolt simply as bolt. Bolts are produced in batches of hundreds of pieces. The suppliers strive to maintain the same production quality for every bolt in a batch and provide quality documentation when delivering the bolts. Bolts are made from alloys such as brass and have a model identification. Typically used models are under the ISO 4014 standard [9].

The assembling of a turbine is performed both at the production site and at the wind farm site where it is commissioned. In the context of this use case, assembling refers to fastening of the bolts in the turbine parts, i.e., the rotor, nacelle, and tower. The turbine is commissioned to a customer, on whose site it is afterwards installed. The turbine assembling plan includes the required bolts and their respective positions in the turbine. The turbine model used is typically SG 14 [10].

Fig. 1: The SG 14-222 turbine model

The fastening of the bolts is performed by the service technicians. For one turbine, bolts from complete batches are used, if possible. The bolts are fastened by fixing them to a predefined pretension level. Documentation of the bolts used, their position in the turbine, pretension level, etc. is made by the service technicians. The maintenance and care of the fastened bolts is performed in samples at regular intervals, e.g., about 10% of the bolts 1-2 times per year, and consists of verifying the bolt pretension levels. If bolts have become loose, they are fastened at the initial pretension level. If they are found to be defect, the bolts are replaced with new ones that are taken from a different batch. As bolts from a batch are guaranteed by the suppliers to be of the same quality, further verifications of the bolts originating from the same batch is required. The risk of defects in other bolts from the same batch needs to be considered, as defect bolts may lead to accidents. When bolts reach the end of their lifetime, typically 25-30 years due to corrosion, they are replaced with new bolts and are recycled based on their material.

In the next section, the processes and data belonging to use case are identified. The process steps we identified are as follows: bolt and turbine registration, bolt fastening, maintenance, bolt replacement and recycling (cf. Figure 3).

3.2. Process Phases

When registering a bolt, its properties are entered and saved into the system, with the bolt getting assigned a unique identifier. To be able to identify and retrieve the bolt's id, a QR code is generated that encodes the necessary information, i.e., an URL, to retrieve the bolt from the system. The generated QR code is engraved on the head of the bolt in sufficiently large resolution (cf. Fig. 2), to include redundant information and compensate for the possible damages to the QR code.

Fig. 2: QR Code engraved on bolt

The turbine registration process is very similar to the bolt registration. The turbine is assigned an identifier by the system once its properties have been entered and saved in the system.

The action of fastening bolts is documented into the system by the service technicians, i.e., the bolt id, turbine id and turbine position are stored.

At regular time intervals, the service technicians will check the status of bolts samples and document the findings into the system, i.e., the found pretension levels and the new pretension levels after refastening.

When a bolt is found as defect during maintenance, the bolt is removed from the turbine and replaced with a new bolt from another batch that is appropriate to be fastened in that respective position in the turbine. The action is documented into the system, i.e., the faulty bolt id and its condition, together with the new bolt id. The old bolt is marked as defect and is set for recycling.

The replacement action is performed too when bolts have reached their service lifetime. The system notifies the responsible service technicians, which then retrieve the bold data records, climb on the respective turbine and replace the bolts. The condition and reason for the bolt replacement are documented and saved into the system.

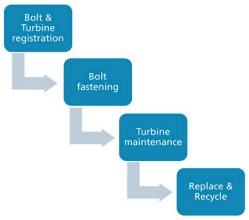

Fig. 3: The identified process phases

4. Blockchain Concept

The system that supports the above-described operations and stores the respective data needs to fulfill a series of properties:

- Store data in a database that all parties involved, e.g., bolt suppliers, turbine assembly, service technicians, traceability engineers, have access to.
- System implements functions that retrieve and locate bolts in turbines.

Moreover, all the parties involved would like to trust that:

- the data stored is not altered or deleted by any other party;
- the implemented functionality is correct, works the same for everyone and does not contain any bugs.

A traditional centralized client-server system with cloud storage would fulfill the first set of conditions, but would fail to offer hard guarantees for the second set of statements. The trust in the system is equivalent to trusting a central authority that offers the named services and stores the respective data. While having contractual agreements on the second set of statements may be a approach, the blockchain solution has a completely different approach.

A blockchain network is decentralized by nature and provides its members with the same rights of contributing to it. There are no parties that solely decide about the data or functionality in the system. In fact, the data cannot be altered or deleted by design, hence the risk of unilaterally manipulating the data is excluded from the start. Moreover, the functionality units in the blockchain, the smart contracts, are visible to all participants and can be checked for correctness and fairness prior to using the system. The blockchain satisfies the basic conditions from above as well. Data is stored in a hash-linked ledger that cannot be tampered with or, if appropriate, in designated databases. In terms of functionality, there is nothing that cannot be automated in smart contracts, as these use Turning-complete programming languages.

A suitable blockchain network would be public-permissioned, i.e., allows anyone to read, while only network members are allowed to write. The blockchain may use of the following types of consensus algorithms:

- a Byzantine Fault Tolerance consensus, e.g., Istanbul BFT [11], that guarantees the network survival even if 1/3 of the member nodes are dishonest;
- a Crash Fault Tolerance consensus, e.g., Raft [12], that guarantees protection against N/2 -1 offline nodes;
- a Proof of Authority consensus, e.g., Clique [13] or AuRa [14], that ensures that the network continues to operate as long as the majority of nodes are honest; it provides a better performance than BFT algorithms.

All of the above algorithms offer finality, i.e., there cannot be any forks in the ledger. The validator nodes participating in the consensus would be the parties involved in the process, e.g., bolt suppliers, turbine assembly, service technicians, traceability engineers. The network governance is to be agreed upon by the members. The governance regulates decisions when formulating and deciding on proposals, e.g., member eligibility criteria, addresses accountability of members for their actions, and introduces incentives to motivate members to act according to the network philosophy.

An addition to the described model is the introduction of access roles. Every participating party needs to have access to a certain amount of information in order to do its job, but seeing all the available information may have detrimental effects to company privacy and affect competition. Therefore, access roles have been established where read and write permissions are defined for all participants that match a certain role, e.g., bolt supplier, turbine assembly, service technicians, traceability engineers, etc. For example, bolt suppliers have full read and write access to the bolts that they own, while having no access whatsoever to other bolts that don't belong to

them. Likewise, the turbine assembly on site has full access for turbines records that they own and to the bolts fastened in the respective turbines. The service technicians have read access to the bolts and turbines that they service and limited access to the bolts of the rest of the turbines. They also have full read and write access to the maintenance data for the respective turbines. For the engineers responsible for tracing back bolts, the read access extends to all turbines that contain bolts from the batches used on-site.

5. Proof of Concept

The developed concept is implemented as a prototype decentralized application (dApp) that offers a web interface to the user. The dApp is written in Node.js and uses Express to set up a REST API that answers user requests.

The dApp communicates with a blockchain instance in the backend, where the smart contracts are deployed. There is one smart contract for bolt management, turbine management and maintenance management respectively. We use the Truffle framework to compile and deploy the smart contracts into the blockchain. The smart contracts are written in Solidity. The blockchain node is run with Ganache as test blockchain instance, which simulates an Ethereum-based blockchain node [14]. Additionally, an Interplanetary File System (IPFS) node is used to save the larger content, e.g., PDF documents or images, with the resulting IPFS CID, i.e., the SHA-256 content identifier hash [15], being anchored in the blockchain via the smart contracts.

6. Conclusion and Future Work

The processes surrounding the fastening of the bolts in turbines can be mapped to a digital model. The manufacturing and the fastening of bolts in turbines, as well as their maintenance until the end of the service lifetime can be specified as successive phases. The necessary data recorded in the respective phases has been identified as well. The blockchain technology suits the set requirements, as it offers a decentralized network designed for collaboration, an immutable data ledger that promotes transparency and offers traceability and is easily auditable. Additional access roles have been defined that protect company privacy and preserve competition amongst the parties involved.

An extension to the model would consist of adding self-sovereign identities to the actors involved. Bolts, turbines, bolt and turbine suppliers, and the service staff would receive decentralized identifiers (DIDs), which wrap around respective private/public key pairs generated for this purpose. The bolt documentation can be represented as verifiable credentials (VCs), where the issuers are the bolt suppliers. When fastened in the turbine, the bolts receive VCs that certify their successful fastening, whereas when they are verified by the service staff, VCs with technical reports are being issued. The DID data is to be stored on the ledger, while the VCs are be stored by agents representing the individual entities. This adds an extra layer of security to the entities that need to digitally sign their actions using their private keys. By outsourcing the VC data, the access roles will not rely solely on the smart contract logic, as the data is not on the blockchain and needs to be expressly shared by its owners.

Acknowledgements

This paper is based on the findings from the UnWind project, which is funded by the Danish Industrial Foundation.

References

[1] ‘Denmark sources record 47% of power from wind in 2019 | Reuters’. https://www.reuters.com/article/us-climate-change-denmark-windpower-idUSKBN1Z10KE (accessed Sep. 22, 2021).

[2] ‘UnWind - Blockchain i Vindmølleindustrien | Industriens Fond’. https://www.industriensfond.dk/unwind (accessed Sep. 20, 2021).

[3] HOLM, Kristoffer. Application of Blockchain in the Wind Industry. In: BPM (PhD/Demos). 2020. S. 61-66.

[4] Wang, Haitao, and Bin Wu. "Design of Wind Farm Information System Based on Blockchain Technology." IOP Conference Series: Earth and Environmental Science. Vol. 647. No. 1. IOP Publishing, 2021.

[5] Chartron, Sylvain, et al. "Digitalization potentials in supporting offshore wind logistics." Logistics 4.0 and Sustainable Supply Chain Management: Innovative Solutions for Logistics and Sustainable Supply Chain Management in the Context of Industry 4.0. Proceedings of the Hamburg International Conference of Logistics (HICL), Vol. 26. Berlin: epubli GmbH, 2018.

[6] ‘UiS Brage: Digitalization of Offshore Wind Farm Systems’. https://uis.brage.unit.no/uis-xmlui/handle/11250/2460309 (accessed Sep. 20, 2021).

[7] Yu, Hang, Senlai Zhu, and Jie Yang. "The Quality Control System of Green Composite Wind Turbine Blade Supply Chain Based on Blockchain Technology." Sustainability 13.15 (2021): 8331.

[8] Keivanpour, S., A. Ramudhin, and D. A. Kadi. "Towards the blockchain-enabled offshore wind energy supply chain." Proceedings of the Future Technologies Conference. 2018.

[9] ‘ISO 4014 - Hexagon head bolts with shank’. https://www.fasteners.eu/standards/ISO/4014/ (accessed Sep. 22, 2021).

[10] ‘Offshore Wind Turbine SG 14-222 DD I Siemens Gamesa’. https://www.siemensgamesa.com/products-and-services/offshore/wind-turbine-sg-14-222-dd (accessed Sep. 24, 2021).

[11] Moniz, Henrique. "The Istanbul BFT consensus algorithm." arXiv preprint arXiv:2002.03613 (2020).
[12] Ongaro, Diego, and John Ousterhout. "In search of an understandable consensus algorithm." 2014 {USENIX} Annual Technical Conference ({USENIX}{ATC} 14). 2014.
[13] 'EIP-225: Clique proof-of-authority consensus protocol'. https://eips.ethereum.org/EIPS/eip-225 (accessed Sep. 24, 2021).
[13] 'Aura Consensus Protocol Audit · poanetwork/wiki Wiki · GitHub'. https://github.com/poanetwork/wiki/wiki/Aura-Consensus-Protocol-Audit (accessed Sep. 24, 2021).
[14] 'GitHub - trufflesuite/ganache: A tool for creating a local blockchain for fast Ethereum development.' https://github.com/trufflesuite/ganache (accessed Sep. 24, 2021).
[15] 'Content addressing | IPFS Docs'. https://docs.ipfs.io/concepts/content-addressing/ (accessed Sep. 24, 2021).
[16] W. Prinz and A. T. Schulte, "Blockchain and Smart Contracts: Technologies, research issues and applications." (2018)

Is Blockchain the Next General Purpose Technology?

Michael Paul Kramer; Jon H. Hanf
Hochschule Geisenheim University, Kreuzweg 25, 65366 Geisenheim, Germany

While blockchain technology is still in an early stage of its development, it is already of surging economic importance. In the literature, blockchain is referred to as either being a disruptive, institutional, foundational, or general purpose technology. There is still no consensus about the economic theory that should apply for analyzing its economic effects. This article draws on use cases from the coffee supply chain to explore, which theories could potentially apply to an emerging blockchain economy.

Obwohl sich die Blockchain-Technologie noch in einem frühen Entwicklungsstadium befindet, gewinnt sie jedoch zunehmend an wirtschaftlicher Bedeutung. In der Literatur wird sie entweder als disruptive, institutionelle, grundlegende oder General-Purpose Technologie bezeichnet. Es besteht jedoch kein Konsens darüber, welche Wirtschaftstheorie für ihre Analyse herangezogen werden sollte. In diesem Artikel wird anhand von Anwendungsfällen aus der Kaffeelieferkette untersucht, welche Theorien potenziell auf die entstehende Blockchain Wirtschaft anwendbar sind.

1. Introduction

Technological innovation has been a major driver of economic growth. Digital technologies play a key role in the ongoing transformation of the economy, fundamentally changing the rules how value is being created. Blockchain technology is a key element in the continuing digital transformation of our economy. Blockchain and distributed ledger technology are oftentimes used as being interchangeable, albeit blockchain is a sub-category of the latter one. When referring to blockchain in this article we use it as an umbrella term representing the different platforms differentiating through governance types. Its immutable, distributed ledger is building the base of the emerging blockchain economy. It can be viewed as a meta-technology as it comprises of various existing technologies that are, intelligently combined, creating a new technology [1].

Blockchain can potentially transform agri-food supply chains enabling value transfer, increasing consumer trust, and reducing transaction costs. One of its key concepts is that on-chain governance mechanisms can be executed in cryptographically secured peer-to-peer networks without the need of a trusted central authority. Trust is being established through the immutability of data, cryptographical security, and consensus mechanisms that govern transactions. Different governance types and consensus algorithms operate in public, private, and consortium platforms [2]. Blockchain enabled tracking and tracing solutions have just started to be implemented in agri-food supply chain networks to provide consumers with trust attributes about the food products.

There is no common consensus as to which economic theory should be applied to research the economic effects of blockchain, let alone that different governance mechanisms exist depending on the platform type. In addition, blockchain evolves through various stages of maturity, incrementally adding functionality at each stage [3], which might result in applying different economic theories. Following Schumpeter's neo-classical notion and Christensen's disruptive innovation theory [4,5], it has been categorized as a disruptive technology [3]. Applying Coase's and Williamson's institutional economics it has been described as an institutional technology [6]. It has further been declared as a foundational [7] and also, as a general purpose technology [8,9].

The aim of this research is to analyze which economic framework applies to the blockchain technology while it matures through several development phases to explain its potential economic value.

2. Methodology

Following an extensive literature overview addressing blockchain technology in vertically coordinated agri-food supply chains, we have researched the application of blockchain in the coffee supply chain through qualitative interviews with experts that have gained operational experiences in using the technology. The results obtained have been applied to three use cases from the coffee industry which we will elaborate on in the discussion section. We admit that the chosen research methodology has certain disadvantages including but not limited to the limited number of use cases, the data obtained through interviews, and that the findings can only be applied to these specific cases.

3. Blockchain evolution over time

Invented in 2008, blockchain technology is still in its infancy phase [11]. It stores data in a distributed ledger and uses consensus mechanisms instead of a trusted central authority to verify transaction. Starting as the foundation of the single financial application bitcoin, a peer-to-peer crypto currency, it can be viewed both as a trust engine and a coordination mechanism for transactions. While this emerging technology has developed gradually over time, it is obvious that it has the potential

to disrupt the current mechanisms of economic transactions.

3.1 Phased approach

Blockchain is assumed to evolve gradually in three phases described as inspired, complete, and extended blockchain solutions [10]. The first phase of this evolution started shortly after the introduction of bitcoin[1] as an application of blockchain in 2009 [11]. Key attributes applying to the inspired phase are the distribution and constant synchronization of the ledger containing all transaction data at every participating node, public- and private-key cryptography for identity and encryption purposes, and hashing to create an immutable, chronologically ordered data ledger with transaction data, impossible to modify or delete.

The second evolutionary phase which is supposed to gain traction in the early 2020s adds tokenization and true decentralization as key attributes to create a blockchain complete solution. A token is the digital representative of a real asset proving the corresponding ownership. With tokenization a digital value of the asset is being created in order to reliably facilitate digital transactions. The tokenization of assets is a prerequisite for the application of smart contracts which was introduced by Ethereum in 2013. The third phase of its evolution is characterized by the integration of potentially disruptive technologies including but not limited to artificial intelligence, internet of things, and self-sovereign identity.

The technology is currently being explored by firms from various industries as its decentralized network topology and distributed architecture can solve transparency and trust issues in business processes. Decentralization can be characterized by the delegation of power or decision rights from a central authority to regional authorities. Still, the majority of current implementations represent a re-engineering of existing centralized processes [12]. Three different platform types exist today: public, private and consortium. These blockchain platform types are differentiating through their governance mechanisms, the access rights, and rights to read and write in the ledger.

3.2 Smart contracts and tokenization

Smart contracts have the potential to become the most successful application of blockchain. They have been first defined by Ethereum, followed by Binance, Cardano, Chainlink, Polkadot, and Stellar. Smart contracts are software programs that operate with fixed rules for automatically executing transactions based on a set of predefined conditions that have to be met and are coded in an electronic contract which has the potential to reduce ex-ante and ex-post transaction costs [13]. With the introduction of tokenization, smart contracts could not only further increase the transparency but also enable autonomous transactions. Key benefits of smart contracts are the increased transparency and trust in a decentralized system with no single ruling authority [14] and the reduction of ex-ante and ex-post transaction costs [15]. Smart contracts can be seen as coordination mechanisms applying an institutional perspective over coordination [16]. Tokens, the digital, alphanumerical representation of a physical asset, are the simplest form of a smart contract. In the supply chain smart contracts are enabling the tracking of products through time, manage ownerships, and authorize automatic payments. They could replace the trust that has been established by intermediaries so that untrusted parties can rely on the integrity of the transaction.

4. Institutional settings of blockchain

Blockchain has been approached through Schumpeter's neoclassical economics and through Coase's and Williamson's new institutional economics [6]. In addition, blockchain has been characterized as a foundational and general-purpose technology [17]. According to Lipsey a new general purpose technology does not start with a single invention at a specific date but rather evolves continuously. It also would not necessarily be accompanied by an immediately expected productivity gain. For managers it is important to understand if blockchain can be identified as a general-purpose technology to adapt the strategies of their firms early enough to best exploit its economic potential. We will elaborate in more detail on general purpose technologies in the subsequent chapter to provide an answer to the question: is blockchain a general purpose technology?

4.1 Neo-classical approach

Schumpeter as a representative of the neo-classical view emphasizes the size of the enterprise and the market structure as primary determinants of innovation, where innovation is the driver of modern economic activity. Schumpeter examines disruptive technologies as technologies which lower production costs and increase total factor productivity in existing economic operations which has "creative destruction" effects on firms and markets. Following Schumpeter, blockchain could be looked at as a new technology which increases productivity, inducing a destructive effect on firms, economy, and society. Clayton M. Christensen, as a result of his efforts in searching for the causes for the failure of enterprises, introduced the principle of disruption which describes the process of a small firm successfully challenging larger and established enterprises [5]. Disruptive technologies such as E-Mail or the compression format mp3 interrupt the success of established technologies and processes, eventually replacing them. In analogy, the cryptocurrency bitcoin could challenge the finance industry as email was challenging the postal industry. In their early stages disruptive technologies often can be

[1] Bitcoin can be viewed as a blockchain complete solution as it encompasses the five key characteristics

bulky and hard to handle. However, over time they gradually adapt to the established technologies eventually surpassing them. As blockchain is being implemented today in agri-food supply networks it can be viewed as a disruptive technology.

It is obvious that blockchain has the potential to replace existing technologies and business processes, but we value the effect as being far more severe as to simply view it as a technology that creatively disrupts existing business models. Blockchain has the potential to transform markets, governance, and society, creating novel use cases, innovative digital business models, and eventually new industries. In the first phase of its evolution however, it should be viewed as a single disruptive technology, as it still has close substitutes in eg. tracking and tracing where solutions are currently being provided by cloud-based offerings.

4.2 Institutional economics

Ronald Coase, the father of institutional economics, viewed the transaction as the predominant economic activity of firms [18]. While Coase focused on the cost of exchange where technological innovation lowers transaction costs, Williamson put his focus on the cost of entering into long-term contractual agreements, introducing the concept of ex-ante and ex-post transaction cost, thus excluding spot market transactions. As per transaction cost theory transaction costs are impacted by three human behaviors: opportunism, bounded rationality, and risk neutrality [19]. Humans act opportunistically, seeking to enforce their strategic objectives. Their decisions are limited by their cognitive abilities including but not limited to processing large amounts of data, their emotions, and the limited amount of time they have for making decisions without exploring all available alternatives or obtaining all relevant information which results in decision making based on incomplete information [19,20]. Due to the fact that assets are typically not homogeneous, Williamson introduced the concept of asset specifity. Hierarchically organized firms coordinate the three behavioral assumptions through governance mechanisms as well as managing the aspects of asset specificity. Following Williamson's theory, blockchain is being viewed as an institutional technology revolutionizing governance and competing with the traditional economy. Davidson elevates blockchain beyond just being a disruptive technology but rather as being "a new institutional technology of governance that competes with other economic institutions of capitalism, namely firms, markets, networks, and even governments" [6]. As the history of all transactions is transparently visible to all participating entities, ubiquitously available information enabled by the distributed ledger technology could also eliminate information asymmetries between business partners. Reducing information asymmetries between trading partners as well as humans limited decision-making capabilities through blockchain has the potential to reduce the costs occurred through bounded rationality and opportunism. However, not only the minimization of cost should be taken into account but also the quality and value of transactions. Eventually, blockchain will have an impact on the governance of organizations and firms introducing decentralized on-chain and off-chain governance. As it has the potential to reduce transaction costs and eliminating intermediaries, we conclude that in the second evolutionary stage it can be categorized an institutional technology applying the new institutional economics.

4.3 A foundational technology

There is also an approach to position blockchain technology as a foundational rather than a disruptive technology as one of the most important digital trends [21,22]. A common definition of what constitutes a foundational technology does not exist yet and even research on blockchain as a foundational technology addressing economic and business aspects is scarce [58]. Some broader definitions exist such as that foundational technology is being an important tool, a new product or service, or the building block of technological development that provides new foundations for the economy and society, or even a technology that enables progress [22,23]. A further indicator would be that the invention has been made by an individual as it has been the case with many innovations in the information technology age. However, the originator or group of originators have not been identified yet. Blockchain is not a new invention but rather a meta-technology which has been built as an open-source protocol intelligently combing various technologies. The definition of foundational technologies overlaps with those of general-purpose technologies and the borders are blurry. As blockchain potentially builds the foundation of a new token-based economy it could be categorized as a foundational technology at a later stage of its evolution. We conclude that it could potentially fall into the foundational technology category at a later stage of its development.

5. Blockchain as a general purpose technology

Historically inputs such as labor and capital have built the basis as primary forces of economic growth. Traditionally progress through technology has been viewed to progress incrementally albeit foundational innovations such as general purpose technologies lead to significant changes to the economy, society, and organizations. If blockchain technology could be viewed at as a general-purpose technology, it is proposed that its effects on the economy's facilitating structure could be compared to those resulting from the invention of true general purpose technologies such as the steam machine, electricity, and information and communication technology. Over the past 200 years those drastic innovations have driven the first three waves of the industrial revolution, which caused significant structural changes to the way a firm is managed and organized, to its governance, or even to the geographical location and concentration of

industries [24]. They significantly transformed production processes and lead to large-scale changes of economies and societies in the past [25,26]. Lipsey et al. conclude that a new general purpose technology does not start with a single invention at a specific date but rather evolves continuously and that it not necessarily would be accompanied by an expected productivity gain. Following Bresnahan and Trajtenberg and Lipsey [27, 24], Bekar et al. defined six attributes that characterize a general purpose technology [28]:

- an enabling technology that creates new use cases rather than providing a complete solution,
- productivity of research and development increases as a consequence of general purpose technologies,
- creating and cultivating productivity gains to the firm,
- enabling the invention of novel innovations that would not be possible without the technology,
- has multiple or single generic uses, and
- does not have close substitutes.

Bitcoin, which uses blockchain with its proof of work consensus mechanism to provide trust, was created as a single solution. However, with the introduction of Ethereum new capabilities such as smart contracts have been created based on the core technology. Meanwhile its applications have already been adopted by several industries including but not limited to agriculture, finance, health care, manufacturing, and logistics where provenance and traceability are amongst the fastest growing use cases [12]. We see the technology as an enabling technology that creates new use cases rather than providing a single complete solution.

Blockchain could lead to a productivity increase in research and development as a consequence of using a single digital ledger for chronological recording purposes that is shared among participants providing information symmetry. It has also the potential to create and cultivate productivity gains to the firm as long as urgent business problems are being addressed or novel business models are being built [12].

As demonstrated with Ethereum and other smart contract platforms blockchain enables novel business models in decentralized finance or through the provision of tokens that enable smart contracts to access external data, APIs, and traditional payment systems. As a result, blockchain enables the invention of novel innovations that would not be possible without the technology. It is also obvious that it has multiple or single generic uses such as the currently dominating crypto currency bitcoin. The last characteristic of a general purpose technology cannot be fulfilled by blockchain at its present maturity level. It still does have in many areas close substitutes resulting from a re-engineering of existing solutions [12].

Bekar, Carlaw, and Lipsey identified a total of 24 general-purpose technologies [24] which Lipsey condensed to 17 true transforming general-purpose technologies, which in the past lead to foundational changes in the economic, political, and social realms [17]. A recent research concluded that information and communication technologies could be viewed at as a general-purpose technology as well increasing the number to 18 [29].

Three general categories of general-purpose technologies have been identified which comprise of products, such as the steam machine, electricity, and information and communications technology, organizational such as mass and lean production, and process-related technologies such as printing all providing spill-over effects and enabling innovations in other sectors [23, 30]. As blockchain is a software protocol that is operating on the internet it could be viewed as an information technology. However, due to its unique capabilities of introducing new forms of governance and subsequently new forms of transactions it could be viewed as an organizational general-purpose technology.

With its inception it typically demonstrates cumbersome handling and basic functionalities similar to disruptive technologies, inhibiting early mass adoption. As they mature and penetrate the economy and society, they are widely used, enabling novel use cases and creating new business models. This process of diffusion of technology can take decades or even generations until the full potential of a general purpose technology develops. Although blockchain in its current evolution phase meets many of those characteristics it cannot yet be viewed as a general purpose technology since it still has close substitutes in certain applications such as tracking and tracing which can be provided by cloud-based solutions in the case of private and consortium type blockchain platforms. However, it does not have substitutes when acting as an enabler for the secure transfer of assets over the internet, enabling smart contracts and decentralized autonomous organizations. We therefor conclude that blockchain in the second evolutionary stage could be viewed at as a potential general purpose technology.

6. Blockchain in agri-food supply chains

The current agri-food supply chain systems are lacking transparency and are highly inefficient. It is estimated that two thirds of the final cost of the agricultural goods are needed to operate the supply chain [31]. Processes in the supply chain are also being impacted by the multitude of intermediaries.

Agri-food supply networks are typically managed centrally with a focal firm being responsible for the coordination of the network [32]. The objective of the network is to maximize its value by improving the overall efficiency by, for example, reducing the cost of transactions. Driven by recent food scandals consumers are expecting information about the origin of the products, which will in return increase the trust in the product and subsequently in the brand that is responsible for the coordination of the supply chain. The distinct requirements of agri-food supply chains are provision of provenance information, transparency of the food products in the supply chain, enabling rapid product recalls, and monitoring of transport and storage conditions, which could lead to an increase of the value of the supply chain network.

Traceability is becoming an increasingly urgent requirement and a fundamental differentiator in many supply chain industries including the agri-food sector [33] . In order to assess blockchain opportunities Carson performed an analysis of the use-cases for several industries including agriculture. The impact of blockchain proved to be very high in the agricultural supply chain while food safety and origin even surpassing the high impact level [33]. Gartner unveiled in a survey conducted in 2019 that the most successful use cases are those that address an urgent business need [12]. They also showed that provenance and traceability are amongst the fastest growing use cases.

7. Discussion on blockchain in coffee supply chains

The use cases we investigated are from the European coffee industry that source their coffee beans from African countries. The blockchain solutions have just recently been put into operation to primarily provide trusted provenance information and supply chain visibility with the objective to increase customer loyalty. In the agri-food industry the application of blockchain to the supply chain management can also increase trust by generating closer relationships between firms [34]. The blockchains we analyzed are being operated under private or consortium platform modes, which support the vertically coordinated agri-food ecosystem typically coordinated by a central authority [32]. All projects are permissioned, centralized solutions, where a single authority or a small group of stakeholders decide over access and control and verify transactions. Governance is being exerted traditionally in a form of regulation, which supports the achievement of the objectives of the firm.

Information about harvesting of goods, the roasting process, and shipping routes are currently being recorded and added manually to the blockchain ledger by the stakeholders; data of smallholders about harvest is being added at the first coffee bean collection point. The majority of the information can be transparently accessed by consumers through a QR (quick response) code which is printed on the coffee packages. While one firm, following a normative stakeholder management approach, has decided to create major parts of value in the country of origin, the other firms import green coffee beans for roasting and packaging in Europe. Firms also use the technology to manage the coffee supply chain and obtain forecasting information. However, tracking and tracing applications prevail in the use cases we investigated aiming to provide food credentials and trust attributes to consumers. The role of intermediaries is non-relevant as the autonomous transfer of assets has not been operationalized yet. Blockchain can be viewed as a competing technology to cloud-based tracking and tracing solutions providing supply chain transparency, cryptographically and chronologically chained data ledgers, as well as information symmetry.

Beyond the current use, other reasons for the implementation are adhering to sustainability requirements, reduction of pollution, and inclusion of smallholders in the coffee supply chain providing a direct farmer-consumer connection. One use case enables consumers to donate funds to “their” farmer as an appreciation for their engagement. By this, blockchain creates a direct connection between the first mile and last mile of the supply chain. Contracts, most importantly those with smallholders, are managed outside the blockchain where short term contracts for a one-year period prevail over long-term contracts, albeit this is the objective of the firms. The use of blockchain as a financial instrument, the settlement of transactions using crypto coins, tokenization of assets through non-fungible tokens, or implemented smart contracts to automate processes has been implemented yet. However, there are considerations to implemented those at a later stage. The predominant objective at the current maturity level is to transfer trust attributes of the food product to the consumer.

From the use cases we conclude that the technology has been implemented as an inspired blockchain solution, which could be analyzed through the neo-classical approach, as the novel technology replaces an existing technology and provides a better solution through immutability of transaction data and transparency across the supply chain. With the introduction of fungible, non-fungible tokens and smart contracts during phase 2 of the evolution, blockchain complete solutions could be materialized. Not only could the transparency in the supply chain further be increased but autonomous transactions based on electronic contracts could be operate on the blockchain creating the potential to reduce ex-ante and ex-post transaction costs, eliminate opportunism and bounded rationality. Hence, blockchain could be viewed as a new institutional technology. The economic effects should then be analyzed by applying Coase’s transaction cost theory.

While the current transaction cost theory emphasizes that centralization, hierarchies, and intermediaries reduce transaction costs, the application of blockchain calls for a new transaction cost theory as through the decentralization new governance mechanisms such as on-chain and off-chain governance emerge impacting transaction costs and introducing new groups of stakeholders. The technology introduces a concept of distributed trust which is pointing towards cooperation rather than to coordination in traditional supply chain settings.

8. Conclusion

The aim of this research was to analyze which economic framework applies to the blockchain technology to explain its potential economic value. From today’s point of view blockchain matures through three phases named blockchain inspired, complete, and extended solution incrementally adding functionality. We found that in the

short run the institutional economics of Coase and Williamson could be applied but due to the wide applicability and spill-over effects a more complex institutional approach should be taken. We also found that in the long run blockchain could be viewed as a potential general purpose technology where firms can build innovation strategies upon. We analyzed three use cases from the coffee supply chain and found that the current implementations fall into the category of blockchain inspired solutions which have the potential to replace existing solutions but on the other hand also have close substitutes. As a result, in the first phase of its evolution it can be viewed as a disruptive technology and the neo-classical approach could be applied. With the implementation of token- and smart contract-based solutions blockchain evolves to a complete solution. As the focus is then on transactions, blockchain in that second evolutionary stage has the potential to eliminate the behavioral assumptions opportunism and bounded rationality in transactions, as well as reducing information asymmetry. With the focus of reducing transaction costs, transaction cost economics as part of new institutional economics could be applied. In the subsequent phase of its evolution blockchain matures to an extended solution and it could be viewed as an organizational general-purpose technology as the combination of technologies could result in significant structural changes to the way a firm is managed and organized and consequently to its governance. However, in its current evolutionary phase operating in the agri-food supply chain it still has close substitutes.

As blockchain will continue to mature we suggest that it could develop even beyond being a general purpose technology. It has the potential to reinvent the exchange of assets and the way information is being provided transparently to stakeholders, eliminate intermediaries, as well as to significantly reduce transaction costs while providing trust in the economic activity. Due to its capabilities to democratize decision making and due to its ability to give the power over personal data back to users it can create new communities and decentralized marketplaces. As blockchain connects billions of unbanked people to the financial system through an internet-connected smartphone it can be viewed as a new mechanism for cooperation between stakeholders and coordination of economic activity.

Traditionally, the main objective of firms has been to maximize profits which enables them to pay increased dividends to shareholders, invest in research and development, and pay competitive salaries. In the blockchain economy gains are achieved through incentives, which build the basis for the blockchain platform, such as miner rewards and transaction fees and through the increase of funds. It is apparent that with the emergence of blockchain the economic activity is migrating from a database driven centralized to a distributed ledger-based decentralized blockchain economy. Based on novel forms of governance manifested as on-chain and off-chain governance, a new theory could emerge which we call decentralized crypto economics, explaining how the relationship between the institutional factors opportunism, bounded rationality, and asset specifity will be rearranged, replaced, or complemented to explain the economic effects of blockchain extended solutions.

References

[1] S. Kamble, A. Gunasekaran, H. Arha. Understanding the Blockchain Technology Adoption in Supply Chains-Indian Context. Int. J. Prod. Res. (2018), 57, 2009–2033.

[2] M.P. Kramer, L. Bitsch, J.H. Hanf. Blockchain and Its Impacts on Agri-Food Supply Chain Network Management. Sustainability 13(4) (2021): 2168.

[3] D. Furlonger, C. Uzureau. The real business of blockchain: how leaders can create value in a new digital age. Harvard Business School Publishing Corporation. Gartner, Inc. (2019).

[4] J.A. Schumpeter. Kapitalismus, Sozialismus und Demokratie. 2. Auflage, Berlin, 134ffS (1950).

[5] J. L. Bower, C.M. Christensen. Disruptive Technologies: Catching the Wave. Harvard Business Review, 43-44 (1995).

[6] P. Davidson, J. de Filippi, J. Potts. Blockchains and the economic institutions of capitalism. Journal of Institutional Economics (2018), Volume: 14, Issue: 4, Pages: 639-658, DOI: 10.1017/S1744137417000200

[7] K. Panetta. Gartner Top 10 Strategic Technology Trends for 2019 (2018).

[8] L. Pietrewicz. Blockchain: A Coordination Mechanism. ENTRENOVA Conference Proceedings. (2019); available at SSRN: https://ssrn.com/abstract=3490168 or http://dx.doi.org/10.2139/ssrn.3490168

[9] A. Kamilaris, A. Fontsa, F.X. Prenafeta-Boldú. The rise of blockchain technology in agriculture and food supply chains. Trends in Food Science & Technology, Volume 91 (2019); 640-652.

[10] D. Furlonger, C. Uzureau. The real business of blockchain: how leaders can create value in a new digital age. Harvard Business School Publishing Corporation. Gartner, Inc. (2019).

[11] S. Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System, N.p.: Bitcoin.org (2008).

[12] D. Groombridge. Unpacking Blockchain Myths From the Reality. Gartners Webinars. (2020). Gartner, Inc.

[13] M. Kõlvart, M. Poola, A. Rull. Smart Contracts. In: Kerikmäe T., Rull A. (eds) The Future of Law and eTechnologies. Springer, Cham. (2016). https://doi.org/10.1007/978-3-319-26896-5_7

[14] G. Zhao, S. Liu, C. Lopez, H. Lu, S. Elgueta, H. Chen, B.M. Boshkoska. Blockchain technology in agri-food value chain management: A synthesis of applications, challenges and future research directions. Computers in Industry. (2019) Elsevier B.V.

https://doi.org/10.1016/J.COMPIND.2019.04.002
[15] G. Ciatto, S. Mariani, A. Maffi, A. Omicini A. Blockchain-Based Coordination: Assessing the Expressive Power of Smart Contracts. Information. (2020). 11(1):52.
[16] C.K. Frantz, M. Nowostawski. From Institutions to Code: Towards Automated Generation of Smart Contracts. In Proceed-ings of the 2016 IEEE 1st International Workshops on Foundations and Applications of Self Systems (FAS*W), Augsburg, Germany, 12–16 September. (2016). 210–215.
[17] R.G. Lipsey. Transformative Technologies in the Past Present and Future: Implications for the U.S. Economy and U.S Economic Policy. ITIF Breakfast Forum (2007).
[18] R. Coase. The New Institutional Economics. The American Economic Review, 88(2), (1988).
[19] O.E. Williamson. The Economic Institutions of Capitalism: Firms, Markets, Relational Contracting. THE FREE PRESS, A Division of McMillan, Inc., New York, 30 (1985).
[20] M. Rutherford. Institutional Economics: Then and Now. Journal of Economic Perspectives, Volume 15, Number 3 (2001), 173–194.
[21] C.G. Harris. The risks and dangers of relying on blockchain technology in underdeveloped countries. IEEE/IFIP Network Operations and Management Symposium, Taipei (2018); 1-4. doi: 10.1109/NOMS.2018.8406330.
[22] M. Iansiti, K. Lakhani. The Truth About Blockchain. Harvard Business Review. Harvard University. Available online: https://hbr.org/2017/01/the-truth-about-blockchain (accessed 24 August 2021).
[23] J.L. Chameau, W.F. Ballhaus, H.S. Lin. Emerging and Readily Available Technologies and National Security: A Framework for Addressing Ethical, Legal, and Societal Issues. Washington (DC): National Academies Press (US); Foundational Technologies (2014). Available from: https://www.ncbi.nlm.nih.gov/books/NBK216326/
[24] R.G. Lipsey, K.I. Carlaw, C.T. Bekar. Economic Transformations: General Purpose Technologies and Long-term Economic Growth. Oxford: Oxford University Press (2005).
[25] E. Kane. Is Blockchain a General Purpose Technology? (2017); available at SSRN: https://ssrn.com/abstract=2932585 or http://dx.doi.org/10.2139/ssrn.2932585
[26] P.L. Rousseau. General Purpose Technologies. In: Durlauf S.N., Blume L.E. (eds) Economic Growth. The New Palgrave Eco-nomics Collection. Palgrave Macmillan, London (2010); https://doi.org/10.1057/9780230280823_11
[27] T. Bresnahan, M. Trajtenberg. General purpose technologies “Engines of growth?”. Journal of Econometrics, 65(1). (1995).
[28] C. Bekar, K. Carlaw, R. Lipsey. General purpose technologies in theory, application and controversy: a review. J Evol Econ 28, 1005–1033 (2018). https://doi.org/10.1007/s00191-017-0546-0
[29] H. Liao, B. Wang, B. Li, T. Weyman-Jones, T. ICT as a general-purpose technology: The productivity of ICT inthe United States revisited. Information Economics and Policy, vol. 36 (2016).
[30] M. Belitski, S.J. Desai. What drives ICT clustering in European cities? The Journal of Technology Transfer, 41(3), 430–450 (2016).
[31] M. Tripoli, J. Schmidhuber. Emerging Opportunities for the Application of Blockchain in the Agri-food Industry. FAO and ICTSD: Rome, Italy; Geneva, Switzerland, (2018).
[32] J.H. Hanf, K. Dautzenberg. A theoretical framework of chain management. Journal on Chain and Network Science 6 (2006): 79-94.
[33] C. Cost, F. Antonucci, F. Pallottino, J. Aguzzi, D. Sarriá and P. Menesatti. A Review on Agri-food Supply Chain Traceability by Means of RFID Technology. Food Bioprocess Technology 6 (2013): 353–366. doi:10.1007/s11947-012-0958-7.
[34] T. Aste, P. Tasca, T. Di Matteo. Blockchain Technologies: The Foreseeable Impact on Society and Industry. Computer, vol. 50, no. 09 (2017); 18-28

Towards a Typology of Blockchain-based Applications: A Conceptualization from a Business Perspective

Roger Heines[*], Tan Gürpinar[**]
[**]University of St. Gallen, CH-9000 St. Gallen
[**]TU Dortmund University, D-44227 Dortmund

Blockchain and other distributed ledger technologies are evolving into enabling infrastructures for innovative ICT-solutions. Numerous features, such as decentralization, programmability, and immutability of data, have led to a multitude of use cases that range from cryptocurrencies, tracking and tracing to automated business protocols or decentralized autonomous systems. For organizations that seek blockchain adoption, the overwhelming spectrum of potential application areas requires guidance reducing complexity and support the development of blockchain-based concepts. This paper introduces a classification approach to provide design and implementation guidance that goes beyond current textbook classifications. As an outcome, a typology for management and business architects is developed, before the paper concludes with an instantiation of existing use cases and a discussion of their classes.

1. Introduction

Blockchain technology (BC) represents one rising enabler with widely discussed capabilities for new types of information systems (IS) [1]. Known for the Bitcoin protocol and the underlying distributed ledger technology (DLT), this innovation provides an alternative way how transactions are digitally executed, recorded, and processed [2]. Before BC, only a centralized data management was able to ensure the validity of digital information [3]. Still, in most enterprise networks, trustworthy intermediaries are necessary to prevent the replication and manipulation of digital data. This leads to additional fees, complexity in IT-systems, security flaws as well as time consuming procedures [4].

When transferring a unique piece of digital property directly to a recipient, BC guarantees its safety and security without challenging the legitimacy of the transaction through a third party. Digital, programmable, and decentralized networks can be created with applicability to a countless number of services and processes [5], [6]. Despite many known benefits, it is still complex for companies, especially for non-technicians, to identify tangible application areas of BC for a potential adoption [7]. Where startups adopt emerging technologies much faster to create new business models, large organizations must consistently reconsider existing practices and legacy systems through a proactive identification and purposeful introduction of new technologies [8]. Although many initiatives try to establish a knowledge base, there is still a need towards a common understanding of BC for both business and IT [9].

A large number of studies and reports on use cases have been conducted and published. There is a substantial body of knowledge that mainly refers to grey literature from various sources, such as blogs, reports, and white papers [10]. There are few scientific contributions and articles that focus on a broader applicability of solutions. Some of them provide systematic literature reviews across multiple domains to conduct an overview about the current state of the art [11], [12], [13]. Others like Labazova et al. map requirements and technical features and propose a comprehensive use case overview of six areas, such as financial transactions, smart contracts, data management, storage, matching, and communication [14]. These works represent a reference point, but often lack generalizability. Also other classification schemes relate to empirical-driven taxonomies specifying technical features and trade-offs of such systems. The few theory-driven typologies are arbitrary without providing proper definitions or grounded criteria.

In order to develop a comprehensive classification scheme that is anchored in theory and provides a novel perspective on BC applicability, the paper aims to answer the following research questions:

- *RQ1: Which conceptual distinctions apply to Blockchain-based use cases?*
- *RQ2: How can Blockchain-based application areas be classified in practice?*

The remainder of this work is organized as follows. Section 2 gives a brief overview about the background and motivation of the paper highlighting the research gap and relevance. In section 3 the methodology and the development of the artifact are presented, where section 4 describes the relevant elements of the typology. Before the paper concludes with a summary and outlook in section 6, an overall discussion and an instantiation of the framework is conducted in section 5.

2. Theoretical Background

2.1. Blockchain Technology

DLT and BC are basically a new forms of database solutions that ensure the management and integrity of digitized transactions in a decentral manner [16]. The inherent technical features allow to build trust among unknown participants without the need for a third party [5], [13]. The verification process in existing structures on basis of conventional solutions represents a single point of failure and leads to time-consuming and costly reconciliation in operations that exacerbates negotiation and interaction between two entities [17].

DLT and BC replaces a single authorized ledger through a replication of records on countless nodes to shift trust from one entity towards multiple copies of a network. However, an additional decentralized mechanism is needed to manage which transactions are chosen and stored in case of a conflict. The so-called consensus algorithm determines the overall systemic state managing the propagation of transactions between equipotent peers of the network [18]. A practical concept for building trust among unknown participants has been implemented for the first time in form of the Bitcoin protocol [2]. The abilities to enable a fully public permissionless distributed ledger refers further to the immutability of data and the way information is distributed. Although DLT and BC may be implemented in various ways, the basic concept refers to four main pillars that combine years of research [2]:

- Peer-to-peer network: The topology enables the database structure for a distributed ledger and defines the network access and rights between entities in form of clients and nodes.
- Transactional logic: The protocol determines a secure communication to initiate changes and defines the distribution of records through digital signatures and additional mechanisms.
- Immutability of data: Transactions are stored and cryptographically sealed in consecutive data blocks interlinked on basis of hash functions to prior data.
- Consensus mechanism: Definition and joint execution of network rules to ensure validity and the systemic state of the network to synchronize the transactions within the shared ledger.

2.2. Decentralized Applications

Where Bitcoin was the first application that disrupted traditional payment structures, the term BC 2.0 refers broadly to the innovations beyond cryptocurrencies. Along with its evolving ecosystem, the BC 2.0 metaphor describes further the development of a whole new industry and the idea of a decentralized economy [5]. From a technical view, a comparison is often drawn to the internet and its TCP/IP protocol in terms of an underlying layer for the world wide web. This infrastructure has been used to build advanced web applications for providing internet-based services on top of it [19], [20].

As a specific feature of next generation BCs, smart contracts establish a whole new field of efficiency-driven applications. Originally relating to contractual agreements that are converted and digitized into algorithmic code, the protocol allows to automatically execute processes similar to contractual conditions. A smart contract is generally characterized by two aspects, autonomy and distribution across the network [5]. In general, a logical sequence in form of an “IF-statement” is necessary to formalize the relevant dependencies. Whether it is about automated processing in administration, invoicing for e-commerce, or machine-to-machine communication, the potentials are theoretically endless [5], [21]. Especially, the logistics sector with its supply networks and high transaction volumes is considered as a highly attractive market for these kinds of alternative ICT structures leading to a paradigm shift in the automation of interorganizational business interaction [18].

Being considered superior to conventional IS-solutions, many practitioners propose an implementation of BC and DLT for almost all sectors such as payment, transfer of voting rights, document management, supply-chain tracking, authentication services or even fully distributed autonomous organizations with an impact on many aspects in our society from environmental sustainability to healthcare or mobility [1], [22]. Based on successful pilots, many companies are encouraged to increase their involvements. More projects and partnerships are established to benefit from network effects, where the needs of the market meet demand, competition, and technical know-how. Although a return of investment is not expected in the short run, many companies take the risk to eventually benefit from improved operations, as well as better products and new business models in the future [23].

2.3. Related Work

A review of existing classifications within the IS-domain has identified a research gap that highlights the relevance for a new conceptual approach of classifying BC-based applications. Despite the growing interest of organizations, research on the applicability of BC-based solutions remains still limited [7]. Some early work provides new insight into the application design of BC-based smart contracts [24]. Other work investigates the usage of cryptocurrencies in practice [25], [26]. The focus lies either on business aspects of a specific application domain or addresses operational aspects of an implementation in a predefined industry sector [27]. Okada et al. use a classificatory approach to structure authority and incentive dimensions for joining permissionless BC-networks [28]. Ballandies et al. develop a taxonomy to map technical design features, such as cryptography and consensus, to evaluate implications on performance [29].

Where Mohsin et al. build a taxonomy on the authentication of network applications, Lemieux develops a typology on recordkeeping solutions [30], [31]. Beside a strong focus on computer science, the publications reflect only one-sided aspects of applicability [32].

Following this, Karim et al. conceptualize characteristics and applications to structure four fields of application areas on the basis of BC value propositions, namely as a development platform, smart contract utility, marketplace and as a trusted service [33]. However, the dimensions in terms of technological scope and platform access show only limited purpose for business practitioners. Also, Elsden et al. focus on a typology for BC applications by proposing seven categories. The different criteria are systematically derived from a business perspective. But in order to serve as a practical measurement tool, the proposed framework must provide a distinguishable categorization of cases [34], [14], [35]. Dependent on the target audience, the presented attributes should be easily understandable to distinguish features among application areas in practice [36]. Finally, it can be highlighted that especially grey literature provides a more comprehensive overview. Although these studies allow for a thorough understanding, the theoretical foundation is often not appropriate or missing at all.

3. Research Methodology

Different criteria can be utilized to categorize BC applications. However, there are two basic types of classifications that can be distinguished[28], [36]. Typologies are developed in a deductive manner on basis of conceptual and theory-driven work. Taxonomies are derived bottom up through inductive empirical-driven reasoning and attempt to cluster existing phenomena on basis of observable and measurable characteristics into mutually exclusive and exhaustive items [13], [36], [37]. Accordingly, it is appreciated to provide an alternative framework that does not solely rely on established variants. The tendency towards archetypal use cases and industries, such as track and tracing in logistics or payment in the financial sector, may lead to a dogmatism that inhibits a conceptualization of new interdisciplinary use cases.

Typologies, in contrast, are intended to provide a more abstract model and are characterized by two defined constructs, so called interrelated types and associated fundamental dimensions. These dimensions are based on the notion of an ideal type allowing in turn the definition of certain attributes [13]. As it appears that a theory-based classification is more aligned with the initial research objectives, the goal is to follow an approach that goes beyond an empirical analysis. By providing a new way to conceptualize BC- and DLT-based application areas, a classificatory framework in reference to the principles of typological reasoning is developed [14].

3.1. Foundations of Blockchain Technology

The proposed typology is subject to foundational implications of BC and DLT using deductive logic and reasoning. Relevant distinctions that define applicability have to be conceptually elaborated on basis of existing literature. To identify these elements, it is first necessary to describe a corpus that outlines similarities and differences in the definition of BC and DLT in terms of foundational premises (FP). In a second step, value drivers (VD) for a potential adoption of BC- and DLT-based use cases are derived by extending the work of Hofmann et al. [38]. By mapping what BC defines (FP) and why it is applied (VD), differentiated conclusions based on interdependencies between functionality and adoption can be drawn. These conclusions represent potential attributes, which are used for an instantiation of ideal types to develop a typology for BC-based applications. By addressing selected peer-reviewed-journals, conference proceedings in IS research, an explorative study on initial definitions, functionalities, and concepts of BC and DLT has been conducted.

Tab. 1: Overview of Foundational Premises

Foundational Premises	Selected References
FP1: DLT/ BC enable a distributed data storage and management	Beck et al. (2016) Dai & Vasarhelyi (2017) Hopf et al. (2018)
FP2: DLT/ BC represent a distributed computing system	Saito & Yamada (2016) Glaser (2017) Cong et al. (2017)
FP3: DLT/ BC is an IS to collect, process, store, and distribute information	Li et al. (2018) Hughes et al. (2018) Labazova (2020)
FP4: DLT/ BC enable decentralized global scale platforms and networks	Rückeshäuser (2017) Riasanow et al. (2018) Zavolokina et al. (2020)

Ultimately 37 publications have been considered to elaborate FPs that describe an underpinning theory in table 1. The exploratory study allows an aggregation of four superordinate premises. FP1 concludes all definitions describing BC as an infrastructure for value-transfer by storing and processing data in form of transactions [39], [40], [41]. FP2 extends this definition by aiming at the capabilities of BC to reach a byzantine-fault tolerance and multi-party-consensus to execute automated scripts via distributed state transitions [42], [43], [44]. Where FP3 provides an additional perspective on the IS-support of strategic, managerial, and operational activities, FP4 defines BC as a scalable platform layer for decentralized applications with the ability for autonomous process execution [45], [10], [46], [47], [48], [49]. Although the heterogonous definitions highlight the fuzzy boundaries of applicability, the conceptualized FPs serve as an initial basis for a more differentiated analysis.

3.2. A Blockchain Value Driver Perspective

Beside a functional view on BC in terms of four FPs, key value drivers are further derived from existing literature using the work of Hofmann et.al. [38]. The authors identified the transformative potentials on generic BC cases and applications to recognize the relevant domains that drive the adoption of blockchain capabilities. The findings were based on research conducted over several months, starting in June 2017, where mainly secondary sources, white papers, literature as well as websites have been acknowledged. In total, six VD were identified that represent main features of BC-based applications towards industry adoption and summarize superior characteristics to overcome pain points in existing ICT-solutions. As a result, the categories have been defined in accordance to "secure validation and protected ownership", "efficient resource allocation, scalability and interoperability", disintermediation and efficient interaction", "trusted automation of processes and contractual relations", "transparency and real-time information sharing" as well as "self-governance and democratization".

After outlining the relevant body of knowledge, it is of interest to add this perspective for a qualitative analysis and identify patterns between FPs and VDs. The goal is to allocate interdependencies and to assess the impacts of attributes on major conceptual elements. Table 2 shows the results of the evaluation, which was conducted during a focus group meeting with six representatives from the financial industry involving digital transformation managers, IT, and business architects as well as product managers. As part of a broader consortium research program on BC and DLT applications, it was not the goal to give an accurate estimation of impact levels, but rather to highlight interdependencies that offer applicable knowledge [50]. It has been revealed that different elements of the overall concept of BC address specific VD for adoption. It is possible to derive patterns and conclude relevant distinctions to develop two fundamental dimensions of the typology. Where BC represents a decentralized data storage system (FP1), the aspects for adoption strongly relate to secure validation and data protection. Defining BC as a distributed computing system (FP2), the trusted automation becomes highly relevant and extends functional capabilities beyond mere data processing. Although FP1 and FP2 partially relate to disintermediation, scalability and self-governance, transformational benefits in case of structural implications are mainly incidental driven. Accordingly, the instantiation of BC as a digital ICT structure (FP3) shows stronger implications on these kinds of drivers. The disintermediation of existing structures represents a more viable case for adoption. Where BC technology is operationalized on basis of a platform (FP4), basically all value drivers are potentially addressed.

The conceptualization of key dimensions and ideal types is based on the configurational complexity in the set of design choices between inherent technological abilities (FPs) and VDs. The analysis provides a first useful heuristic for a systematic foundation with relevant distinctions and attributes. Exhaustive and mutually exclusive classification principles can therefore be neglected to a certain extent [27].

4. A Typology of Blockchain-based Applications

4.1. Definition of Blockchain Dimensions

A need for the ideation of new application areas of BC and DLT can still be highlighted [23]. Therefore, an application-oriented classification is presented that is initially anchored in existing definitions of BC to provide useful distinctions from a business perspective. It differs from related work by determining the foundational impact and potential value proposition of BC-based applications from an industry-independent perspective. Accordingly, two dimensions are conceptualized to form a governance and process sophistication for a first differentiation. In combination with the foundational premises, an initial artefact in form a two-dimensional matrix is presented. In the following subsections the two fundamental dimensions of the typology are derived before a detailed description of classes, categories and labels takes place.

Governance sophistication

Similar to the infrastructure of the internet, BC enabled networks are created through the interconnection of data. Held on remote servers, the main difference lies in a replicated data basis, where BC is able to move the state of information directly into the system itself [43]. This global state allows to technically ensure a common, secure, and decentralized mechanism that represents the missing link for a so-called internet of value [5]. Trust is established between unknown participants in a decentralized network without the need of a third party [51]. Conventional transactions, on the contrary, are often centralized, controlled and verified through an additional instance. This verification ability is now shifted into the BC network leading to disintermediation of many structures. BC is not only capable to operate across organizational boundaries to facilitate access and transmission of transactional data, but also to exchange process states [24]. However, this architecture also leads to greater complexity. A difficulty lies in the peer-to-peer structure between equipotent participants. Its programmable logic is replicated, but in case of an error all computer nodes involved must consent to potential change. Once a BC-network is initiated, different actors have to agree upon one common protocol. Some real-world use cases show that disintermediation through BC is more relevant for certain application areas than for others. Therefore, a first dimension, the so-called governance sophistication, is introduced [52]. It refers to the level of complexity and interdependence of IT-management within organizations [53]. This understanding is ex-

tended by addressing how objectives of individual entities align to achieve economies of scale within a predefined network environment.

Process sophistication

Where the initial concept of Bitcoin lies in the disintermediation of existing monetary structures, a high governance sophistication of the system with its highly desired network effects can be observed [54]. On the contrary, the automated potential associated with smart processes and significantly changes the order of operations between participants in established governance structures [56], [57]. For that reason, a second dimension, the so-called process sophistication, is added to allow a categorization of application areas along attributes that aim to reduce transaction cost associated with automated execution and contracting.

Tab. 2. Interdependencies between Value Driver and Foundational Premises

(⊕: Less favorable, ⊕⊕: Favorable, ⊕⊕⊕: More favorable, ⊕⊕⊕⊕ Most favorable)

Value Driver according to Hofmann et al. (2018)		Foundational Premises: DLT/ BC enable a distributed data storage and management	DLT/ BC represent a distributed computing system	DLT/ BC is an IS to collect, process, store, and distribute information	DLT/ BC enable decentralized global scale platforms and networks
Foucs on processes	Secure validation and protected ownership	⊕⊕⊕	⊕⊕⊕⊕	⊕⊕⊕	⊕⊕⊕⊕
	Transparency and real-time information	⊕⊕	⊕⊕⊕	⊕⊕	⊕⊕⊕⊕
	Trusted automation and contractual relations	⊕	⊕⊕⊕⊕	⊕	⊕⊕⊕
Focus on structures	Disintermediation and efficient interaction	⊕	⊕⊕	⊕⊕⊕⊕	⊕⊕⊕⊕
	Direct ressource allocation, scalability & interoperability	⊕	⊕⊕	⊕⊕⊕⊕	⊕⊕⊕⊕
	Self-Governance and democratization	⊕	⊕⊕	⊕⊕⊕	⊕⊕⊕⊕

contract functionality is much more pronounced for industry applications, such as supply chain management, digital media, or track and tracing [20]. Not dependent on required network externalities, many processes can be radically improved on basis of a decentralized business logic. The rules and instructions that are initiated by predefined code stored on the BC offer enormous potential for many businesses. The consistency of transactional data is improved by the revision-proof storage capabilities of its replicated ledger and enables an automated execution of almost all pre-and post-processing tasks [24]. Once information has been confirmed, it is documented in an audit-proof manner and can be integrated into a wide variety of contexts. From a technological point of view, BC is a predestined tool for process optimization [16]. If a video file, for example, is imported into a platform once the corresponding audio rights are automatically processed on the BC, the entire control and monitoring processes can be omitted. The range of applications may easily be extended from logistics, over administration to real-time execution in combination with internet of the things (IoT), where whole workflows are triggered to initiate self-executing autonomous tasks [55]. The technology has a variety of effects on existing

4.2. Blockchain-based Application Areas

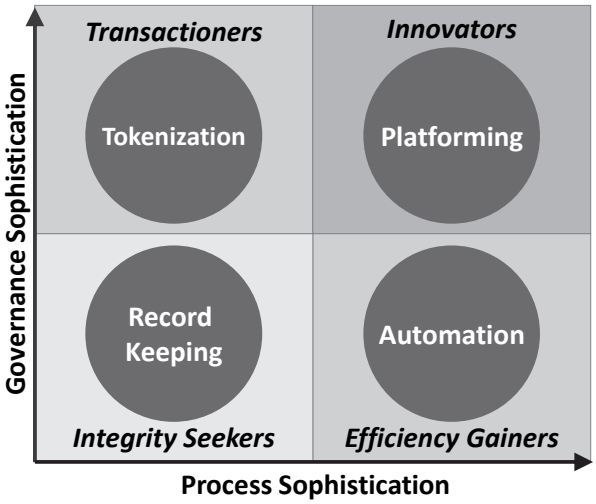

Fig. 1: A Typology of BC-based Applications

The presented typology in Fig. 1 consists of four categories and positions them across the proposed two key dimensions to group the different application areas according to their features and potentials within a 2x2 matrix. The first dimension refers to process sophistication, while the second relates to governance sophistication.

Starting with applications that are characterized by a lower degree of complexity, the grouping of BC-based solutions closes with the highest manifestation in both governance and process related attributes. With regards to the conceptual and descriptive nature of this artefact, it was not necessary to include additional sources and references.

Record Keeping

All records represented on a BC can basically be visible as well as track and traceable to all participants in the network. Every block consists of transactional data and cannot be manipulated or deleted. Only through consent of all participating nodes, a transaction might be reversed. As a result, BC allows a technical proof of data integrity based on immutability, transparency, and completeness at a certain point in time. This timestamping capability enables a wide range of documenting use cases to ensure the origin of any certificate in the area of compliance up to the automated checking of digitized records. If complete transparency is not desired, there is the possibility of a private BC to which only a limited number of users have access. The digital verification of documents or a tracking of objects held in registers represent an important economic factor. Not only auditing companies, auditors or certifiers are affected, but also manufacturers in the pursuit of their products. Companies that aim for business value in this application area can be defined as integrity seekers. Not primarily driven by network effects and scalability, an implementation results in quick and achievable benefits. Also characterized by a low level of smart contract functionality, the solution design is strongly facilitated in comparison to other application types. These use cases cover not only integrated recordkeeping systems in combination with conventional ICT, but also native on chain registries in terms of standalone platforms. However, the governance and process sophistication rise, when the recordkeeping abilities are encoded and executed among multi-stakeholder networks as part of a broader process workflow.

Automation

The technology can not only address inefficiencies in data sharing but also lead to a paradigm shift in the automation of business interaction. Conventional business process management is based on services that are handled internally within single functions and organizations. Automated business processes and workflows, on the contrary, can only be established, if a centralized repository of information is held between actors. Where a BC- and DLT-based solution creates a redundant repository through a fully distributed peer-to-peer system, multiple actors can exchange information while guaranteeing the integrity of the process. The rules and guidelines that define workflows on the BC are programmed into smart contracts in form of executable code segments. All specific steps are verified and enforced. Participants conforming with those rules can be ensured that the correct steps are being taken. This leads to a new way of seamless integration and real time auditing. Every party maintains data sovereignty without centralized control. A digitization of processes for increased efficiency strongly correlates with the complexity of smart contract functionality. Companies that seek process optimization through automated business process are defined as efficiency gainer with applications in trade finance and logistics leading the way to utilize the processual benefits of BC in form of the smart contract concept. As smart contracts are not just applications designed to perform a group of predefined functions, tasks, or activities, they represent an entirely new class of written code that spans various untrusted actors to be deployed and executed simultaneously in a distributed environment. Implementing complex smart contracts is therefore incredibly difficult and error prone that can lead to an increased process sophistication.

Tokenization

Regarding data integrity of BC, values can be stored that represent access rights, ownership of goods or intangible assets with specific characteristics to be transferred from one actor within the system to one another. This transfer capability is seen as the basis of the so-called internet of value to complement the centralized information architecture of today. Cryptocurrencies represent the most obvious applications, where ownership rights are securely and decentrally held within the ledger. A more innovative type of transaction record keeping is the so-called tokenization. It describes the digitalization of assets linking rights to real-world values for trading and settlement. Such systems differ from a native record keeping solution, as the transaction records are not only captured on chain, but enable a new digital representation of goods, rights, or services with specific characteristics in form of tradeable tokens. As the main goal lies not directly on efficiency gains through automated smart contracts, the application requires a minimal viable ecosystem in terms of network effects to ensure exchange and trade. Where cryptocurrencies, such as Bitcoins, show the ability to be interchanged with other assets of the same type, not fungible assets can be also represented through an indirect mechanism. Therefore, asset registries are linked to a digital currency on top of the BC-system. As a result, an asset can represent a piece of land, art, an old-timer, and anything else of value. Organizations that address tokenization capabilities, relate to so-called transactioners. The application area can further develop into a whole platform of copying and sharing for logging the origin and ownership of any value within a network.

Platforming

Due to the specific characteristics in terms of a distributed consensus, digital transfer of values, automation, and irreversible recordkeeping, BC has the potential to challenge entire business models of many organizations. It also offers the possibility to create new business

opportunities that were not possible or not economically viable before. The features of this innovation come by design meaning that the system inheres technical elements, such as cryptography, digital signatures, and peer-to-peer architecture, that logically support the development of business platforms and ecosystems in interorganizational company networks. Like an infrastructure for the provision and processing of data-driven business models, so called BC-enabled ecosystems constitute a next step in digitization to access new markets and to provide the foundation for a decentralized platform economy. The distributed consensus replaces the role of a trusted third party and ensures that all participants are not constrained by any central authority. As any business ecosystem requires to generate value for its users and customers, BC-enabled ecosystems achieve superior benefits through high structural as well as processual implications. Platforming allows to create marketplaces to directly match sellers and buyers allowing them to automate transactions through smart contracts. The open and scalable environment allows truly integrated peer-to-peer platforms for the shared economy where consumers increasingly become prosumers with no governing authority for providing accessible, disintermediated interaction. As the operationalization of these platforms is a fluent process, other application areas can easily develop into such infrastructures if the criteria for a minimal viable ecosystem are met. Due to many stakeholders and the high relevance of smart contract functionality in terms of a required business logic between many equipotent participants, an implementation comes with significant complexity. However, organization that strive for BC enabled platforms are defined as highly disruptive innovators.

5. Discussion

An investigation of industries that apply BC indicates that different characteristics of this innovation repetitively appear and show relevance for a scheme of interrelated application fields. Where tracking and tracing of products in logistics strongly relies on recordkeeping capabilities, analogies can be drawn to the retail sector where the origin of products within the value chain is also identified on basis of immutable and transparent transactional data. However, many empirical artifacts solely provide a one-sided perspective by grouping use cases according to their industry specific scope. This often leads to inconsistent classification attributes, such as financial or non-financial categories to name a few. The decisive aspect is that BC is of great relevance for many areas outside the financial sector and others than cryptocurrencies. To eliminate these redundancies and limitations, a deductive approach based on the classificatory principles by Meyer is chosen to explore new scenarios for applicability and to provide a new strategic tool for practitioners on basis of technological capabilities [14]. By Applying the concept of abstraction and theoretical grounding on the foundations of BC, the typology introduces why and how BC is addressed to allow a positioning with regards to governance and process sophistication.

It turns out that different types of solutions differently impact existing structures and processes leading to essential conceptual similarities for the conventional digital representation of economic transactions used today. From a practitioner's viewpoint, these similarities can be also interpreted as the initial motive to apply this technology, whether it is for recordkeeping, tokenization, automation, or the creation of BC-based ecosystems. Although, these categories can be understood as static and isolated groups, their attributes dynamically change. For instance, a recordkeeping solution within a minimal viable ecosystem of universities validating the origin of certificates. This system can slowly evolve into a multi stakeholder platform that includes other entities, such as companies and agencies, to check diplomas in application processes. In this case, the framework should rather provide an indication for an application area, than to provide an accurate categorization. The two-dimensioned based frame of reference provides an underlying logic that reduces the complexity and helps to simplify the vast field of BC-based use cases.

Tab. 3: Instantiation of BC-based Applications

	Record Keeping	Automation	Tokenization	Platforming
Cryptocurrencies	-	-	10	2
Asset Management	1	1	4	-
Custody	-	-	4	-
Token Issuance	-	-	5	-
Smart Contracts	-	3	-	-
Data Management	3	-	-	-
Reporting	2	-	-	-
Banking Infrastructure	-	2	-	2
Identity Management	-	1	-	4
Total in %	**14%**	**16%**	**52%**	**18%**

To exemplify the typology, the four classes are initially applied to characterize a sample of Swiss BC and DLT-FinTechs in Tab. 3. The data was retrieved from Crunchbase where the search for "Blockchain", "Distributed Ledger" and "FinTech" resulted in 47 hits. Through a website desk research, individual service offerings have been analyzed, grouped, and mapped according to the predefined categories. If multiple services are offered, only core services are considered. Three FinTechs have been further omitted due to indefinable use cases. Interestingly, more than 50% percent of all offerings in Switzerland relate to tokenization. Only 18% specialize on platforming, whereas 16% focus on process optimization. Record keeping solutions are also underrepresented with 14%, assuming that these applications strongly compete with conventional ICT. According to the complexity of BC-solutions, it must be considered that exhaustive and mutually exclusive classification principles

have been neglected to a certain extent. Although the findings probably reflect an industry specific focus and indicate application areas in a specific domain, the practicability of this framework has further to be validated through a broader empirical-to-conceptual iteration in various industries.

6. Conclusion and Outlook

This work provides a typology for BC-based applications across two dimensions and four categories, as it explains why and how use cases can be approached. On basis of a brief study, a research gap has been addressed to provide an orientation and guideline to better understand applicability from a business perspective. As such, it contributes to the existing body of knowledge within the BC domain serving as a strategic and conceptual tool for the development and implementation of new BC solutions in organizations. By addressing which useful distinctions can be applied to classify use cases into application areas, the overall research question has been answered through the definition of two attributes. Where governance sophistication aims at applications that initially impact structures in terms of disintermediation, process automation is mainly driven by solutions that primarily gear towards BCs smart contract functionality in terms of an effective process redesign. As a combination of BCs ability to affect both, processes and structures, a two-dimensional framework has been elaborated. Eventually, four categories have been defined, namely recordkeeping, tokenization, automation, and platforming. By introducing a comprehensible, compact, and easy to use strategic tool for decision making that is anchored in existing theory, a knowledge gap for academia at the intersection of disruptive potentials and real-world use cases for practice can be closed. In the context of this work, an extensive validation is still outstanding. As this initial frame of reference reduces the complexity in the vast field of BC-applications, validation is pivotal to improve potential ambiguity and inconsistencies between the categories. Apart from the formal verification using existing theories and definitions of BC in the existing literature, further testing is appreciated with focus groups and various blockchain implementations that exist. Therefore, it cannot be claimed that the proposed classification is complete nor stops the need for further research at this intersection. Nevertheless, it can be stated by non-digital experts that the artefact enables people to discuss the topic and supports the initial purpose. Following this, it provides a first reference point and represents an important step to understand and formalize use cases in a new way to explore scenarios that are not dependent on existing variants anymore.

Acknowledgements

The work was funded by the Ministry of Economic Affairs, Innovation, Digitalization and Energy of the State of North Rhine-Westphalia.

References

[1] R. Beck, M. Avital, M. Rossi and J.B. Thatcher, "Blockchain technology in business and information systems research", Business & Information Systems Engineering 59(6), 2017, 381-384.

[2] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", Whitepaper, 2008.

[3] A.M. Antonopoulos and G. Wood, Mastering Ethereum: Building Smart Contracts and Dapps, O'Reilly Inc., 2018.

[4] J.L. Zhao, S. Fan and J. Yan, "Overview of business innovations and research opportunities in blockchain and introduction special issue", Financial Innovation 2(28), 2016.

[5] M. Swan, Blockchain: Blueprint for a New Economy, O'Reilly Inc., 2015.

[6] G. Hileman, M. Rauch, "Global Blockchain Benchmarking Study", Cambridge Centre for Alternative Finance, 2017.

[7] M. Rossi, C. Mueller-Bloch, J. Thatcher and R. Beck, "Blockchain Research in Information Systems Current Trends and an Inclusive Future Research Agenda", Journal of the Association for Information Systems 20(9), 2019, 1388-1403.

[8] C. Christensen, The Innovator's Dilemma: The Revolutionary Book that Will Change the Way You Do Business, HarperCollins, 2003.

[9] B. Düdder, V. Fomin, T. Gürpinar, M. Henke, M. Iqbal, V. Janavičienė, R. Matulevičius, N. Straub, H. Wu, "Interdisciplinary Blockchain Education: Utilizing Blockchain Technology from Various Perspectives", Frontiers in Blockchain, 2021.

[10] L. Hughes, Y.K. Dwivedi, S.K. Misra, N.P. Rana, V. Raghavan and V. Akella, "Blockchain research, practice and policy: Applications, benefits, limitations, emerging research themes and research agenda", International Journal of Information Management 49, 2019, 114-129.

[11] T. Guerpinar, G. Guadiana, P. Ioannidis, N. Straub, M. Henke, "The Current State of Blockchain Applications in Supply Chain Management.", 2021.

[12] T. Guerpinar, M. Brueggenolte, D. Meyer, P. Ioannidis, M. Henke, "Blockchain Technology in Procurement - A Systematic Literature Mapping", Proceedings Blockchain Autumn School, 2020.

[13] N. Große, T. Guerpinar, M. Henke, "Blockchain-Enabled Trust in Intercompany Networks Applying the Agency Theory", Blockchain and Internet of Things Conference, 2021.

[14] O. Labazova, T. Dehling and A. Sunyaev, "From Hype to Reality: A Taxonomy of Blockchain Applications", 52nd Hawaii International Conference on System Sciences, 2019.

[15] R. Adams, Perceptions of Innovations: Exploring and Developing Innovation Classification, Cranfield, 2003.

[16] N. Große, D. Leisen, T. Guerpinar, R. Schulze Forsthoevel, M. Henke, M. tenHompel, "Evaluation of

(De-)Centralized IT Technologies in the Fields of Cyber- Physical Production Systems", Conference on Production Systems and Logistics, 2020.
[17] E. Bertino and R. Sandhu, "Database Security – Concepts, Approaches and Challenges", IEEE Transactions on Dependable and Secure Computing 2(1), 2005, 2-19.
[18] M. Mainelli and A.K.L. Milne, "The Impact and Potential of Blockchain on the Securities Transaction Lifecycle", SWIFT Institute Working Paper No. 2015-007, 2016.
[19] E.K. Clemons, R.M. Dewan, R.J. Kauffman and T.A. Weber, "Understanding the information-based transformation of strategy and society", Journal of Management Information Systems 32(2), 2017, 425-456.
[20] M. Iansiti and K. Lakhani, "The Truth about Blockchain", Harvard Business Review 95(1), 2017, 118-127.
[21] V. Buterin, "A Next-Generation Smart Contract and Decentralized Application Platform", Whitepaper, 2013.
[22] K. Gammon, "Experimenting with blockchain: Can one technology boost both data integrity and patients' pocketbooks?", Nature Medicine 24, 2018, 378-381.
[23] 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", Business & Information Systems Engineering 59(6), 2017, 385-409.
[24] B. Egelund-Müller, M. Elsman, F. Henglein and O. Ross, "Automated execution of financial contracts on blockchains", Business & Information Systems Engineering 59(6), 2017, 457-467.
[25] Y. Li, T. Marier-Bienvenue, A. Perron-Brault, X. Wang and G. Pare, "Blockchain Technology in Business Organizations: A Scoping Review", 51st Hawaii International Conference on System Sciences, 2018.
[26] F. Holotiuk, F. Pisani, J. Moormann, "The Impact of Blockchain Technology on Business Models in the Payments Industry", 13th International Conference on Wirtschaftsinformatik, 2017, 912-926.
[27] T. Guerpinar, S. Harre, M. Henke, F. Saleh, "Blockchain Technology - Integration in Supply Chain Processes", Hamburg International Conference of Logistics, 2020.
[28] H. Okada, S. Yamasaki and V. Bracamonte, "Proposed classification of blockchains based on authority and incentive dimensions", 19th International Conference on Advanced Communication Technology, 2017, 593-597.
[29] M. Ballandies, M. Dapp and E. Pournaras, "Decrypting Distributed Ledger Design - Taxonomy, Classification and Blockchain Community Evaluation",arXiv:1811.03419, 2018.
[30] A.H. Mohsin, A.A. Zaidan, B. Bahaa, O. Albahri, A Albahri, M.A. Alsalem and K.I. Mohammed, "Blockchain Authentication of Network Applications: Taxonomy, Classification, Capabilities, Open Challenges, Motivations, Recommendations and Future Directions", Computer Standards & Interfaces 64, 2019.
[31] V. Lemieux, "A typology of blockchain recordkeeping solutions and some reflections on their implications for the future of archival preservation", IEEE International Conference on Big Data, 2017, 2271-2278.
[32] F. Glaser, L. Bezzenberger, "Beyond Cryptocurrencies - A Taxonomy of Decentralized Consensus Systems", 23rd European Conference on Information Systems, 2015.
[33] K. Sultan, U. Ruhi and R. Lakhani, "Conceptualizing Blockchains: Characteristics & Applications", 11th IADIS International Conference Information Systems, 2018.
[34] C. Elsden, A. Manohar, J. Briggs, M. Harding, C. Speed and J. Vines, "Making Sense of Blockchain Applications: A Typology for HCI", Conference on Human Factors in Computing Systems, 2018, 1-14.
[35] S. Gregor, "The Nature of Theory in Information Systems", MIS Quarterly 30, 2006, 611-642.
[36] K.D. Bailey, Typologies and Taxonomies: An Introduction to Classification Techniques, Sage Inc., 1994.
[37] D.C. Hambrick, "Taxonomic Approaches to Studying Strategy: Some Conceptual and Methodological Issues", Journal of Management 10(1), 1984, 27-41.
[38] E. Hofmann, R. Heines and Y. Omran, Foundational premises and value drivers of blockchain-driven supply chains in: Supply Chain Finance, Kogan Page, 2018, 225-255.
[39] R. Beck, J.S. Czepluch, N. Lollike and S. Malone, "Blockchain: The gateway to trust-free cryptographic transactions", 24th European Conference on Information Systems, 2016.
[40] J. Dai and M.A. Vasarhelyi, "Toward Blockchain-Based Accounting and Assurance", Journal of Information Systems 31(3), 2017, 5-21.
[41] S. Hopf, C. Loebbecke and M. Avital, "Blockchain Technology Impacting Property Rights and Transaction Cost Regimes", 24th Americas Conference on Information Systems, 2018.
[42] K. Saito and H. Yamada, "What's So Different about Blockchain? - Blockchain is a Probabilistic State Machine", IEEE 36th International Conference on Distributed Computing Systems Workshops, 2016, 168-175.
[43] F. Glaser, "Pervasive Decentralisation of Digital Infrastructures: A Framework for Blockchain enabled System and Use Case Analysis", 50th Hawaii International Conference on System Sciences, 2017.
[44] L.W. Cong, Z. He and J. Zheng "Blockchain Disruption and Smart Contracts", SSRN Electronic Journal, 2017.
[45] Y. Li, T. Marier-Bienvenue, A. Perron-Brault, X.

Wang and G. Pare, “Blockchain Technology in Business Organizations: A Scoping Review”, 51st Hawaii International Conference on System Sciences, 2018.
[46] O. Labazova, “Towards a Framework for Evaluation of Blockchain Implementations”, International Conference on Information Systems, 2019.
[47] N. Rückeshäuser, “Typology of Distributed Ledger Based Business Models”, 25th European Conference on Information Systems, 2017, 2202-2217.
[48] T. Riasanow, R.J. Floetgen, D.S. Setzke, M. Böhm and H. Krcmar, “The Generic Ecosystem and Innovation Patterns of the Digital Transformation in the Financial Industry”, 22nd Pacific Asia Conference on Information Systems, 2018.
[49] L. Zavolokina, R. Ziolkowski, I. Bauer and G. Schwabe, “Management, Governance and Value Creation in a Blockchain Consortium”, MIS Quarterly Executive 19, 2020.
[50] A. Back, G. Von Krogh and E. Enkel, “The CC Model as Organizational Design Striving to Combine Relevance and Rigor”, Systemic Practice and Action Research 20(1), 2007, 91-103.
[51] A.Y.L. Chong, E.T.K. Lim, X. Hua, S. Zheng and C. Tan, “Business on Chain: A Comparative Case Study of Five Blockchain-Inspired Business Models”, Journal of the Association for Information Systems 20(9), 2019, 1308-1337.
[52] M. Zachariadis, G. Hileman and S.V. Scott, “Governance and control in distributed ledgers: Understanding the challenges facing blockchain technology in financial services”, Information and Organization 29(2), 2019,105-117.
[53] S. Haes and W. V. Grembergen, Strategic IT Governance and Alignment in Business Settings, IGI Global, 2016.
[54] M. Vasek, M. Thornton and T. Moore, “Empirical Analysis of Denial-of-Service Attacks in the Bitcoin Ecosystem”, International Conference on Financial Cryptography and Data Security, 2014, 57-71.
[55] K. Christidis and M. Devetsikiotis, “Blockchains and Smart Contracts for the Internet of Things”, IEEE 4(1), 2016.
[56] T. Gürpinar, N. Straub, S. Kaczmarek, and M. Henke. “Blockchain-Technologie Im Interdisziplinären Umfeld.” ZWF, 114, (10): 605–9, 2019, https://doi.org/10.3139/104.112117.
[57] N. Große, D. Leisen, T. Gürpinar, R. Schulze-Forsthövel, M. Henke, and M. ten Hompel. “Evaluation of (De-)Centralized IT Technologies in the Fields of Cyber-Physical Production Systems.”, CPSL, 2020.

Rollen und Aufgaben Interdisziplinärer Projektteams zur Blockchain-Integration im Unternehmensumfeld

Tan Gürpinar*, Timucin Korkmaz**, Michael Henke*
*Technische Universität Dortmund, D-44227 Dortmund
**Fraunhofer Institut für Materialfluss und Logistik, D-44227 Dortmund

Bei der Einführung von Blockchain-Lösungen im Unternehmensumfeld sind zahlreiche Unternehmensfunktionen und Mitarbeiter unterschiedlicher Disziplinen involviert, deren Zusammenarbeit zum einen notwendig sind, zum anderen jedoch auch zahlreiche Herausforderungen hervorrufen. Relevante Rollen und Disziplinen werden in diesem Paper identifiziert und beschrieben, um Handlungsempfehlungen für die interdisziplinäre Zusammenarbeit und somit zur erfolgreichen Integration von Blockchain-Lösungen in Unternehmen und insbesondere unternehmensübergreifenden Geschäftsbeziehungen zu entwickeln. Auf Basis existierender Blockchain-Projekte werden die Rollen „Management und Finanzen", „Supply Chain Management" und „IT und IT-Sicherheit" fokussiert und entlang eines Vorgehensmodells zur Integration mit konkreten Rollenbeschreibungen und Aufgaben beschrieben.

1. Einleitung

In globalen Wirtschaftsbeziehungen nehmen Kooperation und Wettbewerb im Sinne einer Koopetition zu erreichen, um die nächste Stufe der Innovation zu [1], [2]. Dezentrale Technologien, wie die Blockchain-Technologie (BCT), gewinnen an Bedeutung, da sie demokratische und nachvollziehbare Beziehungen zwischen mehreren Organisationen herstellen können und für Transparenz und Vertrauen sorgen [3]. Die BCT etabliert sich dabei als Forschungsgegenstand in verschiedenen wissenschaftlichen Disziplinen, da sie Merkmale aus den Bereichen verteilte Systeme, bzw. Peer-to-Peer-Netzwerke, Kryptografie und anderen Technologien vereint und das Versprechen mit sich bringt, die Art und Weise zu verändern, wie unternehmensübergreifende Geschäftsprozesse durchgeführt werden [1], [4].

Die Einführung der BCT in bestehende Geschäftsprozesse ist mit weitreichenden strategischen Auswirkungen und komplexen Herausforderungen für Unternehmen verbunden und kann nur durch Bereichs-übergreifende Zusammenarbeit sowie die Integration verschiedener Disziplinen gemeistert werden [5]. Um Innovation und effektive interdisziplinäre Teamarbeit zu fördern, wird interdisziplinäre Kompetenz immer wichtiger. Der Fokus liegt dabei auf der Integration und Synthese unterschiedlicher Perspektiven und Methoden zur Lösung von komplexen Problemen [1]. Das interdisziplinäre Setting bringt sowohl Chancen, wie schnelle Entscheidungsfindung, kognitive Vielfalt und erhöhten Innovationsgehalt bzw. Kreativität, als auch Risiken wie mangelnde Offenheit gegenüber anderen Disziplinen, Kommunikationsbarrieren und Konfliktpotenziale [1].

In Blockchain-Integrationsprojekten führen die Beziehungen zwischen internen und unternehmensübergreifenden Akteuren häufig zu den genannten Herausforderungen. In diesem Fall haben die Akteure Schwierigkeiten, ein gemeinsames Verständnis über Ziele, Fähigkeiten und Anforderungen der Blockchain-Integration zu erreichen, und es fehlt eine gemeinsame Fachsprache und einheitliche Diskussionsbasis [5]. Um solche Projekte zum Erfolg zu führen, sollten zukünftige Projektteilnehmer "interdisziplinäre Kompetenz" entwickeln und damit in die Lage versetzt werden, in interdisziplinären Settings zu arbeiten [1]. Kachalov et al. [6] definieren interdisziplinäre Kompetenz als die Fähigkeit und Bereitschaft, das Wissen mehrerer Disziplinen entsprechend den Anforderungen der beruflichen Tätigkeit anzuwenden. Das Verständnis für interdisziplinäre Kommunikation und die Demonstration der psychologischen Bereitschaft, das Wissen der relevanten Bezugsdisziplinen anzuwenden, sind dabei Schlüsselelemente [6].

In diesem Paper werden auf Basis aktueller Blockchain-Projekte vorherrschende Disziplinen und Rollen identifiziert, beschrieben und hinsichtlich ihrer Aufgaben im Blockchain-Projekt sowie des Zusammenspiels mit anderen Rollen analysiert. Zudem wird eine Vorgehensweise zur Einführung der BCT unter Berücksichtigung der zuvor identifizierten Disziplinen erarbeitet.

2. Theoretischer Hintergrund

2.1 Blockchain im Unternehmensumfeld

Die Blockchain Technologie hat sich aus dem Wunsch heraus entwickelt elektronische Zahlungen direkte von einem Teilnehmer zu einem anderen transferieren zu können, ohne dabei von einem Intermediären abhängig zu sein [7]. Erfüllt wird diese Anforderung indem ein Peer-to-Peer-Netzwerk Kontrollmechanismen realisiert, welche für die Entstehung und Aufrechthaltung eines Single-Point-of-Truth sorgt.

Es entsteht ein Mechanismus, der den Teilnehmern des Netzwerks sicherstellt, dass die in ihr vorgehaltenen Daten nicht kompromittiert sind. Das notwendige Vertrauen in die gegenüberliegende Entität, um Transaktionen sicher durchzuführen, wird verlagert auf die zugrun-

deliegende Technologie [3]. Aktuelle Blockchain-Implementierungen sind nicht nur in der Lage Transaktionen zu handhaben, sondern auch komplexere Daten und verteilt Logiken. Daher kann die Blockchain Technologie im Unternehmenskontext immer da eingesetzt werden, wo es einer Zuverlässigen und manipulationssicheren Datenpersistenz bedarf. Insbesondere die permissioned Blockchains, welche für eine geschlossene Betreibergruppe gedacht sind, bieten große Vorteile sowohl in der Performance als auch in der Möglichkeit der Verwaltung der jeweiligen Rechte, zum Beispiel durch Zugangsbeschränkungen. Im Gegensatz zu permissionless Blockchains, wie dem Bitcoin, welcher für jeden, sowohl als Nutzer mittels eines Wallets, als auch als Betreiber (Miner) durch einen Fullnode, frei zugänglich ist, können permissioned Blockchains so konfiguriert werden, dass die Inbetriebnahme eines neuen Nodes einem Genehmigungsverfahren unterliegt und Daten nur selektiv geteilt werden [9], [10].

2.2 Funktionsweise und Unterschied zu traditionellen Systemen

Der Einsatz der Blockchain Technologie erfordert ein technisches Umdenken in den Unternehmen. Zwar forcieren auch andere technologische Neuerungen wie zum Beispiel die Cloud-Technologie eine Abkehr von traditionellen monolithischen Strukturen hin zu verteilten Systemen, im Grunde wird jedoch nur eine Funktion aus der lokalen IT-Infrastruktur in ein verteiltes System ausgelagert. Daher ist es möglich Funktionen wie z.B. den Datenspeicher oder die Berechnungskapazität, auszulagern und bedarfsgerecht von einem gekapselten System – der „Cloud" – abzurufen. Die Blockhain-Technologie nutzt jedoch ihre eigene zugrundeliegenden, verteilte IT-Infrastruktur und lässt sich daher nicht ohne Weiteres anstelle bestehender Systemkomponenten einsetzten.

Satoshi Nakamoto legt bereits 2008 für die erste Blockchain eine Peer-to-Peer-Infrastruktur fest. Diese besteht aus einem verteilten Netzwerk aus sogenannten Nodes [11]. Diese Nodes sind in der Lage sowohl Dienstleistungen anzubieten, als auch in Anspruch zu nehmen und besitzen unter anderem auch die Möglichkeit sich zu synchronisieren. Diese Prinzipien lassen sich soweit auch auf andere Blockchain-Implementierungen übertragen. Insbesondere braucht es eine Synchronisation des Status, der über die Nodes redundant und verteilt verwalteten Daten. Jedes Mal wenn neue Informationen in die Blockchain aufgenommen werden sollen, muss eine Synchronisation und eine Einigung über den neuen Status erreicht werden. Diese Aufgabe übernehmen die Konsensmechanismen und bilden einen essentiellen Unterschied zu traditionellen Systemen [12].

Einzelne Datensätze werden als so genannte Transaktionen zu Blöcken zusammengefasst und mittels Hashfunktion mit einem digitalen Fingerabdruck versehen. Dieser Hashwert fließt als erstes Datum in den nachfolgenden Block mit ein und stellt damit eine Referenz zum Vorgänger dar. Ein Block enthält also immer den Hash seines Vorgängers, seine Nutzdaten und seinen Hashwert über den gesamten Datensatz, so entsteht eine Kette aus Blöcken – eine Blockchain [13]. Die Eigenschaften von Hashfunktionen, welche in der Mathematik und Kryptografie schon hinreichend betrachtet wurden, stellen dabei sicher das nachträgliche Manipulationen fast unmöglich werden [14]. Diese Eigenschaft ist nochmals durch die Synchronisations- und Konsensmechanismen der jeweiligen Blockchain-Implementierung abgesichert. Denn selbst wenn ein Node in der Lage wäre, seinen eigenen Datenbestand zu ändern, hätte dieser allein Schwierigkeiten dies in einem verteilten Netzwerk durchzusetzen. Denn eine Statusänderung des Netzwerkes kann nur erreicht werden, wenn ein Konsens über diesen erzielt wird. Abhängig von der gewählten Blockchain-Implementierung sind die Nodes darauf ausgelegt die Mehrheitsentscheidungen im Netzwerk mitzutragen [12]. Dies lässt die Vermutung aufkommen, dass ein Blockchain-Netzwerk sicherer ist, wenn es hirneichend viele Nodes gibt und diese idealerweise im Hoheitsbereich unterschiedlicher Rechtsträger sind, bzw. nicht kooperieren, um dem Netzwerk zu schaden [4].

2.3 Zusammenarbeit in Projektteams

Das Zusammenkommen der aufgezeigten technischen Besonderheiten der Blockchain Technologie sowie deren zahlreichen Anwedungsdomänen lassen die Schlussfolgerung zu, dass Experten unterschiedlicher Fachbereiche bei der Planung und Umsetzung einer Blockchain-Lösung benötigt werden. Bereits Frodeman und Klein sowie Brassler und Dettmers beschreiben, dass Experten in Projektteams in der Lage sein sollten Informationen, Daten, Techniken, Werkzeuge, Konzepte und/oder Theorien aus zwei oder mehr Disziplinen zu integrieren, um bei der Umsetzung unterschiedliche Interessen zu berücksichtigen und Probleme zu bewältigen. Auf diese Weise könnten komplexe Problemstellungen gelöst werden, bei denen es unwahrscheinlich ist, dass sie mit isolierten disziplinären Mitteln gelöst werden könnten [15], [16].

Eine Möglichkeit ein derartiges interdisziplinäres Team zu formen, bietet das überarbeitete Modell nach Tuckman [17], in dem die Formung eines Teams in 5 Sequenzen unterteilt wird (siehe Abb. 1). Hier lernt das Team seine eigenen Grenzen sowie die Interessen der anderen Teammitglieder kennen und bildet grundlegende Regeln (Forming). Anschließend folgt eine konfliktbereite Sequenz, in der die Teammitglieder ihre eigenen Interessen positionieren - zunächst ohne die Sichtweisen der anderen Teammitglieder zu berücksichtigen (Stoming). Die Akzeptanz anderer Betrachtungsweisen und Interessen ist kombiniert mit der Einführung von Rollen und Normen in der darauffolgen-den Sequenz (Norming). In der vierten Sequenz stellt das Team sodann eine hochfunktionale Einheit dar, die instrumentarisch funktionieren kann, um bestehende Problemstellungen zu lösen (Performing). Wenn ein Team dieses

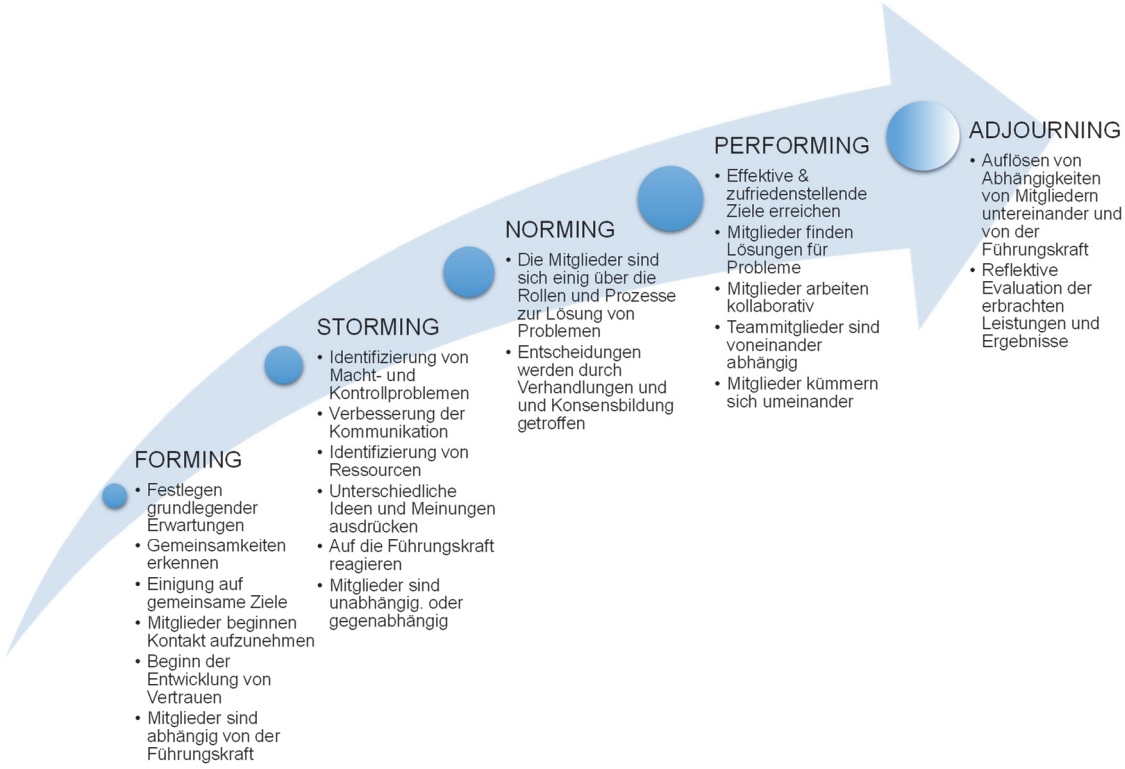

Abbildung 1: Entwicklungssequenzen in Kleingruppen i.A.a. Tuckman, B. W. (1977)

Stadium erreicht hat ist es in der Lage über die Grenzen der isolierten Disziplinen und der jeweiligen disziplinären Kulturen hinaus zu denken.

Das interdisziplinäre Arbeiten kann durch das Kommunizieren und Wahrnehmen der eigenen und anderer Disziplinen, Methoden oder Gegenstände angeregt werden. Dies kann zur Entwicklung eines "interdisziplinären Denkstils" führen [18]. 1977 ging B.W. Tuckman selbst auf aktualisierte Erkenntnisse ein und fügte seinem Modell noch die 5. Phase „Adjourning“ hinzu. In dieser Phase entkoppeln sich die Teammitglieder von den entstandenen Strukturen und Abhängigkeiten und lösen dadurch das Teamgefüge wieder auf. Hier gehört es auch dazu auf die erbrachte Leistung und die erreichten Ziele zurückzuschauen. Diese Phase unterscheidet sich auch von den vorgehenden, da diese das Ende bildet und keine weitere Phase folgt, wohingegen nach jeder anderen Phase eine weitere folgt. Für die vorherigen Phasen sind auch iterative Abläufe – wie bspw. an das Performing anschließendes Forming – vorgesehen.

3. Methodisches Vorgehen

Zur Identifikation relevanter Disziplinen, Rollen und entsprechender Aufgaben in Blockchain-Projekten wurden Fallstudien der aktiven Blockchain-Großprojekte „Tradelens“ [19] und „Foodtrust“ [20] analysiert und durch Informationen von den Webseiten sowie YouTube-Kanälen ergänzt. Auf Basis der Erkenntnisse wurde das in einer vorangegangenen Veröffentlichung entwickelte Blockchain-Integrationsmodell [10] weiterentwickelt und die entsprechenden Phasen des Modells mit Verantwortungen und Zuständigkeit je Disziplin und Rolle versehen sowie beschrieben. Die Projekte Tradelens und Foodtrust dienten hierbei als exemplarische Blockchain-Projekte für den Bereich des Supply Chain Managements, da sie bereits verhältnismäßig weit fortgeschritten sind und Fallstudienmaterial herausgeben.

Das Projekt Tradelens wurde im Januar 2018 gestartet. Die Gründungspartner des Projekts sind das IT-Unternehmen IBM und das Logistik- und Transportunternehmen Maersk. Tradelens ist eine Supply Chain Plattform und möchte den Informationsaustausch und die Zusammenarbeit über die Lieferkette hinweg ermöglichen. Hierbei sollen alle Stakeholder der Lieferkette in das System eingebunden werden. Die Plattform soll allen Stakeholdern einen sicheren und nahtlosen Austausch von Echtzeit-Lieferketteninformationen, Versandmeilensteinen, Ladungsdetails, Handelsdokumenten und Sensordaten ermöglichen. Durch den Einsatz der Blockchain Technologie kann die Manipulationssicherheit und Überprüfbarkeit gewährleistet werden. In einer zwölfmonatigen Testphase konnte ermittelt werden, dass die Versandzeit der Partner um bis zu 40% gesunken ist. Im Laufe der Zeit konnte Tradelens mehr als 300 Organisationen für ihr Projekt als Partner gewinnen. Zu den Partner gehören mehr als achtzig Hafen- und Terminalbetreiber, die Zollbehörden von unter anderem den Niederlanden, Saudi-Arabien, Singapur und Australien und diverse Transport-, Spediteur und Logistikunternehmen. Mittlerweile arbeiten ebenfalls fünf der sechs größten Reedereien mit Tradelens. Insgesamt wurden mehr als

42 Millionen Containersendungen auf der Plattform verarbeitet. Aktuell bewältigt Tradelens mehr als zwölf Millionen Sendungsereignisse pro Woche. Ebenfalls werden mehr als 100.000 Versanddokumente pro Woche bearbeitet und sicher gespeichert.

Die Idee der Plattform Food Trust wurde im Jahr 2016 von IBM vorgestellt. Die offizielle Testphase startete im August 2017. Am 8. Oktober stellte IBM daraufhin Food Trust offiziell vor. Seitdem kooperiert IBM mit vielen großen Unternehmen aus der Lebensmittelbranche. Unter den Partnern befinden sich unter anderem Nestlé, Walmart Inc. und Carrefour. IBM möchte durch das Projekt die Lieferkette effizienter gestalten. Hierbei sollen alle Stakeholder innerhalb der Lieferkette von der Nutzung profitieren. Durch die Nutzung einer gemeinsamen Plattform ist es möglich, jeden Schritt in der Lieferkette manipulationssicher nachzuverfolgen. Dadurch sind Informationen zum aktuellen Standort, Zertifizierungs-, Prüf- und Temperaturdaten jederzeit innerhalb von Sekunden einsehbar. Anhand dieser Informationen soll es möglich sein, die Lieferkette besser analysieren zu können und diese daraufhin zu optimieren. Ebenfalls stellen diese Daten sicher, dass die Qualitätsstandards der Lebensmittel über die gesamte Lieferkette eingehalten werden. Dadurch wird die Transparenz stark gesteigert und das Vertrauen gestärkt. Um einen möglichst einfachen Einstieg zu gewährleisten, setzt Food Trust auf das Modell Software-as-a-Service. Hierdurch benötigen Teilnehmer nur eine Internetverbindung und einen Browser, um die Funktionen von Food Trust zu nutzen. Ebenfalls ist es möglich, durch APIs das ERP-System einfach zu integrieren und Daten einfach in das Netzwerk hochzuladen. Aktuell können Firmen Food Trust nutzen, um ihre Effizienz zu steigern, den Versand von Lebensmitteln zu verfolgen, Verschwendung zu minimieren und die Qualität mittels Zertifikaten zu verifizieren und nachzuweisen.

4. Ergebnisse

4.1 Rollen in Blockchain Projekten

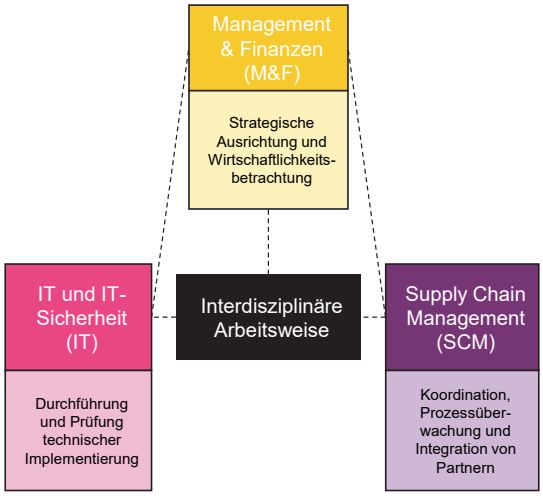

Abbildung 2: Rollen in Blockchain-Projekten

Management & Finanzen

Die Rolle Management & Finanzen gibt während des Aufsetzens und der Einführung eines Blockchain-Projekts eine klare strategische Ausrichtung für das Geschäftsmodell vor und führt darüber hinaus entsprechende Wirtschaftlichkeitsbetrachtungen durch. Darauf aufbauend fungiert die Rolle als Projektadministrator, der dafür verantwortlich ist, dass der gesetzte Soll-Zustand erreicht wird und eine reibungslose Kommunikation innerhalb des interdisziplinären Teams gesichert ist. Von der Rolle wird gefordert, dass sie kurzfristig das Unternehmensergebnis absichert und gleichzeitig einen Beitrag zur langfristigen Unternehmensstrategie leistet.

Als relevante Aufgaben ergeben sich die folgenden:

- Berücksichtigung von unternehmensübergreifendem Risikomanagement
- Prüfung einer Verankerung der Ziele des Blockchain-Projekts mit übergeordneten Unternehmenszielen
- Festlegung einer Governance und somit Definition von Regeln, Rollen und Verantwortlichkeiten (z.B. Lese- und Validierungsrechte)
- Prüfung der Einzahlung des Blockchain-Projektes auf die Kultur und Strategie des Unternehmens unter Berücksichtigung der Compliance
- Prozess-Management und Soll-/Ist-Vergleiche
- Workflow-Management und Definition von KPIs zur Performance-Messung
- Sinnhaftigkeitsprüfung und Wirtschaftlichkeitsbetrachtung des Gesamtprojektes

Supply Chain Management und Einkauf

Die Rolle des Supply Chain Management (SCM) ist im Rahmen des Projekts für die Koordination der verschiedenen Prozesse zuständig. Aufgrund der vielen Schnittstellen zu diversen internen Abteilungen und Partnerunternehmen, nimmt das SCM die Rolle des Bindeglieds zwischen den am Projekt beteiligten Geschäftsbereichen und weiteren Supply-Chain-Teilnehmern ein. Je nach Phase des Projekts variieren die damit verbundenen Aufgaben von der Incentivierung externer Partner zur Partizipation am Projekt bis hin zur fortlaufenden Koordination nach der Implementierung. Darüber hinaus trägt das SCM durch umfassende Prozesskenntnisse in nahezu sämtlichen Phasen maßgeblich zur Gestaltung des Blockchain-Konzepts bei und wird daher häufig nicht nur als Koordinator, sondern auch als Business Architekt der Lösung bezeichnet. Aufgrund der großen Einflussnahme auf diverse Abteilungen und dem abteilungsübergreifenden Prozessverständnis kann das SCM in einigen Bereichen als verlängerter Arm des Managements interpretiert werden. Unternehmensintern

befindet sich das SCM demnach zwischen der strategischen und operativen Ebene. Die Einkaufsabteilung ist innerhalb des Projektes für die Koordination der externen Schnittstellen zu den Zulieferern des Unternehmens zuständig und wird in diesem Fall dem SCM zugehörig angesehen. Diese weitreichende Expertise in der fachlichen Ausgestaltung des Prozesses wird insbesondere benötigt, um die Ziele und Umsetzungsstrategien für die IT und IT-Security vorzugeben. Häufig müssen vertragliche Regelungen, Geschäftsprozesse oder manuelle Vorgänge erst digitalisiert werden. Da wo dies nicht direkt geht, müssen intensive Absprachen mit der IT stattfinden, so dass passende Workarounds erarbeitet werden können.

Es ergeben sich die folgenden Aufgaben beim Aufsetzen und der Einführung von Blockchain-Lösungen:

- Umsetzung der vom Management vorgegebenen Maßnahmen auf Prozessebene
- Sammeln und aufbereiten von Prozess-relevanten Ist-Daten
- Entwurf und Aufbereitung der Soll-Prozesse für IT und IT-Security
- Unterstützung der Management-Ebene durch Prozess-Know-how und dem Verständnis des Zusammenwirkens einzelner Abteilungen
- Beitrag zur Erarbeitung eines Ablaufplans für die Einführung von Blockchain-Lösungen und des damit verbundenen Progress-Monitorings
- Zusammenstellen von abteilungsintern und externen Anforderungen an das neue blockchainbasierte Konzept
- Unterstützung bei der Auslegung des Konzepts durch andere Unternehmensbereiche oder Supply Chain Partner
- Beitrag zum Berechtigungsmanagement und zur Datenverwaltung im Blockchain-Netzwerk
- Integration der Zulieferer und den damit verbundenen Aufgaben durch die Einkaufsabteilung und Einigung auf wesentliche Standards, um die Interoperabilität zu gewährleisten

IT und IT-Security

Die Rolle IT und IT-Security ist zentraler Ansprechpartner für die operative Ausgestaltung der Blockchain-Plattform und somit zuständig für die technische Implementierung. Die Rolle ist Ansprechpartner bei Rückfragen zu technischen Spezifikationen, intern sowie extern, und unterstützt die Abteilungen SCM und M&F bei der Planung und Organisation mit Informationen zu technologischen Grundlagen. Über die Vermittlung von Grundlagenwissen hinaus, berät die IT den Bereich M&F hinsichtlich der Anforderungsprofile zur weiteren Personalplanung in der IT und ist gemeinsam mit dem Bereich SCM zuständig für den Aufbau und Transfer des Blockchain-spezifischen Wissens innerhalb des Netzwerkes. Weiterhin prüft die IT-Abteilung die technologische Machbarkeit der vom SCM geplanten Prozesse, koordiniert den fortlaufenden Abgleich zwischen operativem Implementierungsfortschritt und der Gesamtprojektplanung und befindet sich hierzu im ständigen Austausch mit den Bereichen SCM und M&F. Die für das Gesamtprojekt erfolgsentscheidende Aufgabe der IT ist es, die zielführende Erhebung und Verarbeitung aller über die Plattform genutzten Daten, die Sicherheit dieser Daten sowie deren rechtskonforme Nutzung, entsprechend der Data Compliance und länderspezifischen Gesetzgebung, innerhalb des Blockchain-Netzwerkes technisch zu ermöglichen.

Die spezifischen Aufgaben können wie folgt zusammengefasst werden:

- Planung auf welche Art und Weise Daten im Blockchain-Netzwerk erfasst werden (Blockchain-Devices)
- Planung wie die Daten gespeichert, verwaltet, geteilt und genutzt werden sollen
- Planung und Kalkulation des IT-Budgets
- Anforderungen für die zielführende und effiziente Vernetzung aller Stakeholder definieren
- Informationstechnische Aspekte aufbereiten, Aufwandsprognose der Implementierung erstellen und bei Rückfragen beraten
- Implementierung einer nachhaltigen Smart Data Governance sowie eines standardisierten Datenaustauschformats
- Entwurf von verschiedenen Nodes und entsprechenden Interfaces für verschiedene Stakeholder
- Programmieren, ausgestalten und einrichten der Smart Contracts
- Aufbereitung von technischen Trainingsmaßnahmen für alle Partner und Kunden, sowie Ausgestaltung der Inhalte und Unterlagen für das Training
- Die Performance und Kapazitäten sowie die Auslastung der Blockchain-Lösung steuern, evaluieren und optimieren
- Die Sicherheit der Plattform und aller vollzogenen Transaktionen gewährleisten
- Sicherheitsrisiken, die speziell in Blockchain-basierten Anwendungen auftreten, identifizieren, daraus Sicherheitsanforderungen ableiten und entsprechende Maßnahmen ergreifen

- Den Datenschutz gemäß der konsortiumsweiten Vorgaben und der technischen Möglichkeiten umsetzen
- Eingliedern der BC-Governance in die innerbetriebliche IT-Governance
- Aufklärung zu den Blockchain-spezifischen Abläufen und die Gewährleistung der Daten-/Prozesssicherheit

4.2 Vorgehen zur Blockchain-Integration

Auf Basis der gewonnen Rollen-spezifischen Erkenntnisse kann die strukturierte Integration einer Blockchain-Lösung in bestehende Geschäftsprozesse entlang des Integrationsmodells in Abb. 3 beschrieben werden. Entwickelt wurde die Grundstruktur des Modells bereits in 2020 [10]. In der folgenden Erweiterung sind die sechs Integrations-Phasen des Modells Rollen-spezifisch beschrieben. Außerdem wird auf das Zusammenspiel der jeweiligen Rollen eingegangen und in einer neuen Spalte „Rollen" dargestellt.

Phase 1: Damit die Blockchain-Lösung möglichst reibungslos in bestehende Unternehmensprozesse integriert werden kann, startet die erste Phase zunächst mit einer Aufnahme der Projekt-Rahmenbedingungen. Die Rolle M&F ist dafür verantwortlich zu überprüfen, ob eine Blockchain-Integration für den gegebenen Use Case überhaupt sinnvoll ist und entscheidet über die Ressourcen, die für die Planung und Konzeptionierung des Blockchain-Netzwerkes aufgebracht werden sollen. Dafür ist eine Abstimmung mit dem SCM und Einkauf notwendig - insbesondere, um ein für den Anwendungsfall sinnvolles Partnernetzwerk festzulegen. Des Weiteren liefert das SCM weitere Informationen zur Realisierung des Anwendungsfalls, indem bspw. überprüft wird, ob eine einheitliche Datenbasis oder Versionsverwaltung zwischen den Partnern benötigt wird, oder ob bestehende Verfahren ausreichen. Darüber hinaus muss die Rolle M&F klar begründen können, warum ein solches Innovationsprojekt für das Unternehmen sinnvoll ist (z.B. Wettbewerbsvorteil gegenüber anderen Marktteilnehmern). Dazu gehört auch, die bereits erkennbaren Nutzenversprechen und potenziellen Herausforderungen des Projekts zu identifizieren. Dies sollte in einem engen Austausch mit den anderen Abteilungen aus dem interdisziplinären Team erfolgen. Dabei erhält die Rolle M&F Informationen zu erkennbaren Nutzenversprechen (z.B. Nachvollziehbarkeit und lückenlose Dokumentation der Lieferkette) insbesondere vom SCM und Mitarbeitern der betroffenen Geschäftspro-

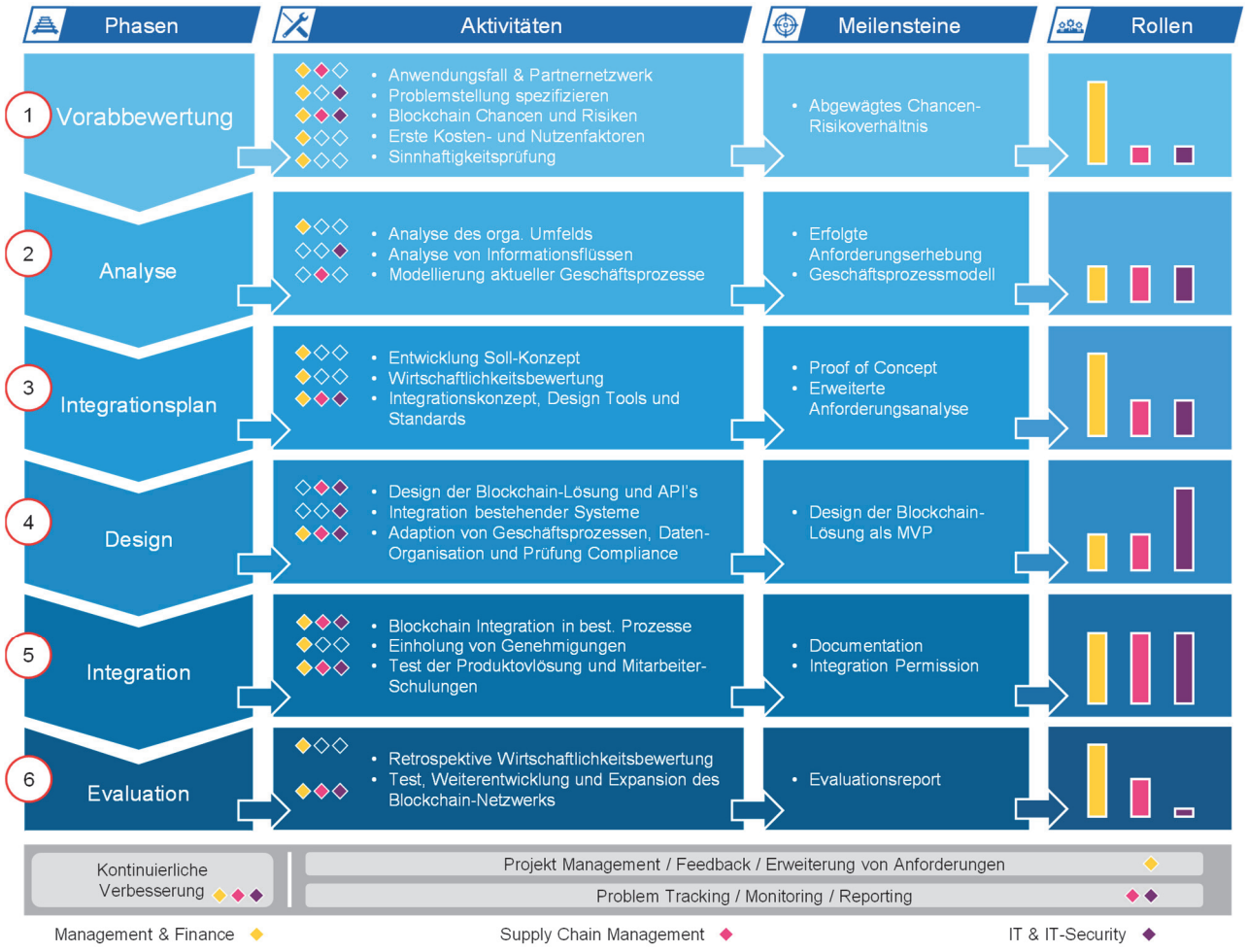

Abbildung 3: Blockchain-Integrations-Modell

zesse. Seitens der IT werden insbesondere die Herausforderungen und potentielle Kosten der technischen Umsetzung beleuchtet. Zum Abschluss der ersten Phase sollte eine Strategie für die Integration der BCT festgelegt sein, und die Dringlichkeit bzw. der Business Impact des Projektes klar unter den interdisziplinären Teammitgliedern kommuniziert werden.

Phase 2: Basierend auf der festgelegten Strategie und dem formulierten Business Impact setzt sich das Projektteam in der Analysephase mit den bestehenden Geschäftsprozessen auseinander, definiert Anforderungen und evaluiert verschiedene Implementierungsansätze unter Berücksichtigung privater und konsortialer Blockchain-Frameworks sowie zugehöriger Konsensmechanismen. Um ein vollständiges Bild des aufzubauenden Unternehmensnetzwerkes zu erhalten, analysiert die Rolle M&F sowie SCM die organisatorische Umgebung und diskutiert die Mitwirkung der Partner. Alle relevanten Akteure sind hinsichtlich ihres Nutzens für das Netzwerk zu untersuchen und es ist festzustellen, wie diese in ihren jeweiligen Geschäftsmodellen einen Mehrwert generieren oder als Kunden an der Plattform partizipieren können. Die Aufarbeitung von finanziellen Informationen ist von besonderer Bedeutung, da Ökosysteme wie Blockchain-Plattformen, ausgeprägten Netzwerkeffekten unterliegen. Das SCM modelliert betroffene Geschäftsprozesse und bietet somit die Grundlage, um vorhandene Pain Points durch das blockchain-basierte Konzept zu adressieren. Darüber hinaus ist das Geschäftsprozessmodell eine essentielle Voraussetzung für die Planung der aufzusetzenden IT-Infrastruktur und das entsprechende Datenmodell. Die IT entscheidet sich auf dieser Basis für die Einführung eines bestimmten Blockchain Frameworks. Die Entscheidung über das spezifische Framework beeinflusst schlussendlich die genaue Ausgestaltung der zukünftigen Prozesse sowie die Kostenseite der Wirtschaftlichkeitsbetrachtung.

Phase 3: In der folgenden Phase sollten sowohl Ziele als auch der letztendliche Soll-Zustand des blockchain-basierten Konzepts festgelegt werden. Involviert ist hier insbesondere die Rolle M&F, die aus gesamtunternehmerischer Sicht vorgibt, dass bspw. nach den ersten sechs Monaten bereits 80% der in Schritt zwei analysierten Prozesse papierlos laufen und mehr als 60% der Zulieferer in das Blockchain-Netzwerk integriert werden sollten. Die Zielerreichung wird während des Projektverlaufs kontinuierlich überwacht. Darüber hinaus findet an dieser Stelle – da nun sowohl Ist- als auch Soll-Prozesse analysiert wurden, eine Wirtschaftlichkeitsbewertung statt. Als Ergebnis dieser Phase sollte von der IT-Abteilung ein Prototyp des Blockchain-Netzwerks mit minimalem Funktionsumfang entwickelt worden sein (Bspw. kann dieser einen konkreten Geschäftsprozess abbilden). Dieser Prototyp wird für die interne Organisation verwendet, um ein besseres Verständnis für das Innovationsprojekt zu erlangen. So kann die Rolle SCM frühzeitig weitere modifizierte Anforderungen für die spätere Lösung identifizieren (z.B. Detaillierungsgrad der Bestellvorgänge und Kundendaten). Entscheidend ist abschließend, dass die Machbarkeit und Wirtschaftlichkeit des Projektes sichergestellt ist, sodass für die Entwicklung ein größeres Budget freigegeben, werden kann.

Phase 4: Die Design-Phase ist die letzte Phase vor der vollständigen Umsetzung und Integration der Blockchain-Lösung und besteht in erster Linie in der Ausgestaltung des zuvor entwickelten Konzepts, indem sämtliche vorgelagerten Entscheidungen und Analysen zu einem vollständigen Bild zusammengefügt werden. Die Rolle des SCM als Business Architekt und Koordinator kommt während dieser Phase besonders zum Tragen, da Informationen von verschiedenen Abteilungen und den betroffenen Schnittstellen kombiniert werden müssen. Die IT fokussiert hierbei die technische Entwicklung, als auch Integration der Software-Inkremente in bereits bestehenden Informationssystemen. Alle in den vorherigen Phasen als positiv betrachtete Aspekte müssen nun in enger Abstimmung mit dem SCM durch die IT in die Blockchain-Landschaft integriert werden. Das M&F muss definieren, für welche funktionalen Abläufe Smart Contracts in Erwägung gezogen werden und wie die vereinfachend bezeichneten „Wenn-Dann-Konditionen" gestaltet werden (z.B. Leistungen für Zahlung, Zahlungsmethode und -intervalle, etc.). Bei der Gestaltung der Smart Contracts müssen deren Funktion überprüft werden. Insbesondere muss die Logik im Smart Contract dem abzubildenden Geschäftsvorgang entsprechen. Hier muss wie bei fast allen zu digitalisierenden Vorgängen in Abstimmung mit den anderen Bereichen geprüft werden, ob Prozesse 1-zu-1 digitalisiert werden können und falls das nicht geht, ob der Prozess oder das digitale Abbild angepasst werden muss. Ganz im Sinne des interdisziplinären Vorgehens sollten auch die Stakeholder berücksichtigt werden, die die neuen digitalen Prozesse handhaben müssen. Immer wiederkehrende Vorgänge zum Beispiel der Produktionsversorgung sowie die Beschaffung von typischen Verschleiß- und Ersatzteilen, die regelmäßig erneuert werden müssen, bieten sich für die Verwendung eines Smart Contract-Konzepts im Rahmen der Blockchain-Plattform an. Im Zusammenhang mit dem Design der BCT-Lösung muss außerdem die Einhaltung gesetzlicher Vorschriften beachtet werden. Die Umsetzung einer Blockchain-Lösung erfordert die Berücksichtigung von zahlreichen Compliance-Anforderungen. Darüber hinaus gilt es, branchenspezifische Regularien des jeweiligen Industriezweigs zu berücksichtigen sowie nationale und internationale gesetzliche Vorschriften einzuhalten, die zwischen den Blockchain-Teilnehmern variieren können.

Phase 5: In der Integrationsphase wird die entwickelte Blockchain-Lösung umgesetzt und getestet. Ziele dieser Phase ist es die Blockchain-Lösung als ganzheitliche Lösung in die Geschäftsprozess mit zu integrieren. Da die BCT ihre vorteilhaften Eigenschaften zum Teil aus ihrer Infrastruktur (P2P-Netzwerk) bezieht müssen manche

technischen Aspekte von Anfang an mit umgesetzt werden. Daher kann es Sinn machen zwar nicht alles auf einmal umzusetzen (Top-Down-Ansatz), aber es könnte von Vorteil sein einzelne Prozesse im Ganzen oder zumindest in abgeschlossenen Sequenzen in Smart Contracts zu überführen. Die zur Integration der BCT in die Systeme aller Partner notwendigen Genehmigungen der Partner werden von der Rolle M&F eingeholt. Einen erheblichen Einfluss auf die Bereitschaft der Partner, am Blockchain-Netzwerk teilzunehmen, wird die Argumentation von M&F haben, wie sich eine Teilnahme auf die individuellen Ziele der Partner auswirkt. Für diese Aufgabe wird die M&F-Abteilung auf die Zuarbeit der Bereiche SCM und IT angewiesen sein, welche die Argumentationskette durch fachliche und operativ relevante Information bekräftigt. Bei der Umstellung auf Smart Contract gestützten Prozesse muss darauf geachtet werden das die Integrität der bestehenden Geschäftsdaten nicht verloren geht. Dies erfordert erneut eine enge Zusammenarbeit mit dem Bereich SCM, der für die Prozessgestaltung des Anwendungsfalls sowie die Definitionen der Kommunikationsschnittstellen verantwortlich ist. Eine wesentliche Rolle in der Integrationsphase spielt weiterhin das interne sowie Partnerübergreifende Training, um die Blockchain-basierten Lösungen korrekt anwenden und Auswirkungen verstehen zu können . Um ein nachhaltiges und zielführendes Training zu gewährleisten, werden sowohl das SCM als auch die IT entsprechend ihrer Bereiche alle notwendigen Informationen zusammentragen müssen. Die interne Veranlassung des Trainings sowie das Angebot für externe Teilnehmer zur Verfügung zu stellen, ist anschließend die Aufgabe von des Managements.

Phase 6: Die letzte Phase des Ablaufplans besteht in der Evaluation des entwickelten Konzepts und dessen Einführung. Vor allem die dritte Wirtschaftlichkeitsbetrachtung ist ein zentraler Aspekt in dieser Phase, da retrospektiv auch quantitative Methoden für die Analyse genutzt und dementsprechend aussagekräftigere Ergebnisse bezüglich des Projekterfolges und möglichen Problemfaktoren erzielt werden können. Hierfür müssen die Verantwortlichen der Rolle M&F zunächst den Umfang des Evaluations-Reports inklusive geeigneter KPIs und Zielgrößen festlegen. Einige Kennzahlen, vor allem prozessbasierte Indikatoren, werden vom SCM ermittelt und für die Weiterverarbeitung aufbereitet. Im Rahmen der Auswertung der Ergebnisse sollte M&F die Notwendigkeit für weitere Datenanalysen und Verbesserungen bewerten und diese gegebenenfalls einleiten. Für das Unternehmen sollten vor allem die Auswirkungen der Blockchain-Lösung auf Prozesszeiten (z.B. Order Processing Time, Aufwand für Customer Service) und die Fortschritte basierend auf verbesserten Tracking- und Tracingmöglichkeiten untersucht werden. Außerdem sollte durch die M&F-Rolle das Feedback aller Beteiligten der interdisziplinären Projektteams eingeholt und evaluiert werden – optimaler Weise in regelmäßigen Zyklen parallel zum Projektfortschritt und in einer größer angelegten Runde der sechsten Phase. Letztendlich kann durch die genannten Tätigkeiten eine kontinuierliche Verbesserung und Unterstützung aller Kernaspekte im Ablaufmodell gewährleistet werden.

5. Fazit und Ausblick

In Projekten zur Integration von Blockchain-Lösungen im Unternehmensumfeld kann das Bilden von interdisziplinären Projektteams dazu verhelfen, die zahlreichen Perspektiven von Blockchain-Anwendungsfällen zu berücksichtigen und den Einsatz von Produktivlösungen zu forcieren. In aktuellen Blockchain-Projekten, die in Unternehmensnetzwerken eingesetzt werden, konnten insbesondere drei relevante Rollen unterschiedlicher Disziplinen identifiziert werden: Management und Finanzen; Supply Chain Management und Einkauf; IT und IT-Sicherheit. Während das Management insbesondere die strategische Ausrichtung des Projektes festlegt und kontrolliert sowie die Sinnhaftigkeit und Wirtschaftlichkeit der Lösung betrachtet, dient die Rolle des Supply Chain Managements als unternehmensübergreifender Koordinator und überwacht die Integration der Partner sowie die entsprechenden Prozesse. Die IT und IT-Sicherheit ist hauptsächlich bei der Planung, Durchführung und Absicherung der technischen Implementierung involviert.

Auf Basis der identifizierten Rollen wurde ein Vorgehensmodell zur gestützten Integration von Blockchain-Lösungen in bestehende Geschäftsprozesse weiterentwickelt und Rollen-spezifisch beschrieben. Es wurde deutlich, dass in den meisten Prozessschritten mindestens zwei Rollen gleichzeitig zu involvieren sind und eine enge Vernetzung der Rollen zwingend gegeben sein muss. Außerdem wurde deutlich, dass viele Randaspekte, wie bspw. Governance und Compliance in ihren Aufgabenumfängen nicht unterschätzt werden sollten und womöglich für sich eigenständige Rollen darstellen können. Methoden der interdisziplinären Zusammenarbeit konnten zudem auf den Blockchain-Bereich angewendet und adaptiert werden.

In dieser Arbeit wurden zwei Referenzprojekte begutachtet und zur Wissensgenerierung genutzt, wodurch keine Verallgemeinerung für den Bereich des Supply Chain Managements erzeugt werden kann. In zukünftigen Forschungsvorhaben ist zu empfehlen, weitere Projekte in die Berücksichtigung einfließen zu lassen und empirisch zu validieren. Optimaler Weise sollten Blockchain-Integrationsprojekte von Beginn an begleitet und unterschiedliche, involvierte Rollen (bspw. unter Zuhilfenahme der Delphi-Methode) interviewt werden.

Danksagung

Beteiligt an der Ideengebung und Umsetzung im Rahmen von Fallstudien aus dem Bereich der Erdölindustrie waren die folgenden Teilnehmer des LFO Blockchain-Labors 2020 der TU Dortmund: Leon Baumgartner, Lennart Berg, Jonas Beyer, Christian Becker, Leon Brake-

meier, Silas Fischer, Nils Hoppe, Maximilian Kempa, Benjamin Krah, Florian Möller, Lukas Paßmann, Helin Pehlivan und Vanessa Zander.

Die Autoren bedanken sich bei allen Teilnehmern für ihren wertvollen Beitrag sowie bei dem Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen für die Unterstützung als Fördermittelgeber.

References

[1] B. Düdder, V. Fomin, T. Gürpinar, M. Henke, M. Iqbal, V. Janavičienė, R. Matulevičius, N. Straub, H. Wu, Interdisciplinary Blockchain Education: Utilizing Blockchain Technology From Various Perspectives. Frontiers in Blockchain. 3. 58, (2021).

[2] M. Henke, Strategische Kooperationen im Mittelstand: Potentiale des Coopetition-Konzeptes für kleine und mittlere Unternehmen (KMU), Verl. Wiss. & Praxis. Zugl. München, (2002).

[3] N. Große, T. Gürpinar, M. Henke, Blockchain-Enabled Trust in Intercompany Networks Applying the Agency Theory, Blockchain and Internet of Things Conference, (2021).

[4] T. Gürpinar, N. Straub, S. Kaczmarek, M. Henke, Blockchain-Technologie Im Interdisziplinären Umfeld." ZWF, 114 (10), (2019), 605–9.

[5] D. Laufs, P. Sandner, Implementing blockchain projects in banks, in: Banking & Financial Services Policy Report, (2020), 39

[6] N. Kachalov, ,A. Kornienko, R. Kvesko,,S. Kvesko, Y. Chaplinskaya, Interdisciplinary competences and their status role in the system of higher professional education. Proc. Soc. Behav. Sci. 206, (2015) 429–433.

[7] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System. (2008).

[8] T. Gürpinar, G. Guadiana, P. Ioannidis, N. Straub, M. Henke, The Current State of Blockchain Applications in Supply Chain Management., Association for Computing Machinery, (2021).

[9] N. Große, D. Leisen, T. Gürpinar, R. Schulze Forsthövel, M. Henke, M. ten Hompel, Evaluation of (De-) Centralized IT Technologies in the Fields of Cyber-Physical Production Systems, Conference on Production Systems and Logistics, (2020).

[10] T. Gürpinar, S. Harre, M. Henke, F. Saleh, Blockchain Technology – Integration in Supply Chain Processes, Hamburg International Conference of Logistics, (2020).

[11] H-G. Fill, A. Meier (eds.): (2020), Blockchain. Grundlagen, Anwendungsszenarien und Nutzungspotenziale, Springer Fachmedien Wiesbaden, (2020).

[12] K. Adam, Blockchain-Technologie für Unternehmensprozesse. Sinnvolle Anwendung der neuen Technologie in Unternehmen, Springer Berlin Heidelberg, (2020).

[13] Subramanian, N, Chaudhuri, A & Kayıkcı, Y. Blockchain and Supply Chain Logistics. Evolutionary Case Studies, Springer International Publishing; Imprint Palgrave Pivot, Cham., (2020).

[14] P. Rogaway, T. Shrimpton, Deterministic Authenticated-Encryption: A Provable-Security Treatment of the Key-Wrap Problem, Eurocrypt, (2006).

[15] R. Frodeman, J. T. Klein, The Oxford Handbook of Interdisciplinarity. 1. publ. in Paperback. Oxford: Oxford Univ. Press, (2012).

[16] M. Brassler, J. Dettmers , How to Enhance Interdisciplinary Competence. Interdisciplinary Problem-Based Learning versus Interdisciplinary Project-Based Learning. Interdisciplinary Journal of Problem-Based Learning, (2017).

[17] B. Tuckmann, M. Jensen, Stages of Small-Group Development Revisited, Group & Organisation Management, (1977).

[18] S. Lerch, Interdisziplinäre Kompetenzen, Waxmann Verlag, Münster, (2017).

[19] Tradelens-Projekt, https://www.tradelens.com/, abgerufen: 31.08.2021

[20] Food-Trust-Projekt, https://www.ibm.com/de-de/blockchain/solutions/food-trust, abgerufen am: 31.08.2021

Entwicklung eines industriellen Blockchain-Netzwerkes

Erik Neumann
Hochschule Mittweida, Technikumplatz 17, 09648 Mittweida

Mit der zunehmenden Vernetzung von Unternehmen wächst auch das Potenzial für Cyberangriffe, Spionage und Sabotage in Produktionsnetzwerken. Netzwerke, die auf Blockchain-Technologien aufbauen, können einige dieser Risiken abmildern, insbesondere solche, die Datenmanipulation betreffen. Dieses Paper befasst sich mit der Architektur und Implementierung eines unternehmensübergreifenden Blockchain-Netzwerks zur manipulationssicheren und ausfallsicheren Speicherung von produktionsbezogenen Daten und deren Verteilung innerhalb eines globalen Netzwerks. Dazu werden zunächst die Anforderungen an ein solches System erläutert. Darauf aufbauend wird die Architektur eines Blockchain-Knotens beschrieben und der Nutzen des Systems anhand eines Anwendungsfalls dargestellt.

As companies become more interconnected, the potential for cyberattacks, espionage, and sabotage in production networks continues to grow. Networks building on blockchain technologies can mitigate some of these risks, especially those concerning data manipulation. This paper details the architecture and implementation of a cross-company blockchain network for the tamper-proof and resilient storage of production-related data and its distribution within a global network. To this end, the requirements for such a system are first explained. Based on this, the architecture of a blockchain node is described and the utility of the system is presented via a use case.

1. Einleitung

Der technologische Fortschritt der letzten Jahre hat es Unternehmen ermöglicht, ihre Produktionssysteme schrittweise zu digitalisieren und zu vernetzen. Mithilfe dieser Vernetzung können mehrere Unternehmen entlang einer Wertschöpfungskette ihre Produktion aufeinander anpassen und effizienter zusammenarbeiten [1]. Durch die stärkere Vernetzung und Digitalisierung vergrößert sich jedoch auch die Gefahr durch Cyberkriminalität. So wurde zwischen 2019 und 2020 ein rund 20-prozentiger Anstieg bei den Delikten der „*Datenveränderung*“ und „*Fälschung beweiserheblicher Daten*“ [1] verzeichnet, dabei waren die Ziele zumeist große Unternehmen [2][3].

Insbesondere die Manipulation von produktionsnahen Daten stellt für die Sicherheit von kritischen Infrastrukturen eine erhöhte Gefahr dar. Werden beispielsweise Produktionsdaten manipuliert, kann die Nachverfolgbarkeit von Fehlern innerhalb der Produktion zu einem späteren Zeitpunkt nicht mehr gewährleistet werden. Dies kann zu einer Gefährdung der Bevölkerung führen, falls Fehler beispielsweise bei Automobilteilen oder pharmazeutischen Produkten auftreten.

Um eine Lösung für dieses Problem zu erforschen, wurde das Projekt „safe-UR-chain“ 2019 vom Bundesministerium für Bildung und Forschung gefördert [4], darin arbeiten Unternehmen mit Expertise in der Fertigungsindustrie mit Forschungseinrichtungen[2] gemeinsam an einem Blockchain-Simulator zur Erprobung innerhalb eines Wertschöpfungsnetzwerkes. Die Entwicklung des Blockchain-Netzwerkes wird dabei von der Hochschule Mittweida getragen. Dieses Netzwerk soll es ermöglichen, Daten manipulationssicher speichern zu können. Dafür sollen einzelne Unternehmen jeweils private Blockchains verwenden, die sich gegenseitig absichern. Dabei werden die unternehmensinternen Blockchains regelmäßig die Hashes ihrer aktuellen Blöcke austauschen. Mithilfe dieser Hashes kann die Existenz von Daten innerhalb der jeweiligen Blockchains später belegt werden, ohne dass die gesamten Daten preisgegeben werden müssen.

2. Anforderungen

Da die Blockchain-Software innerhalb eines industriellen Umfeldes zum Einsatz kommen soll, muss sie bestimmten Anforderungen gerecht werden. Diese Anforderungen wurden insbesondere in Zusammenarbeit mit den Industriepartnern ausgearbeitet. Einige der Anforderungen wurden auf Basis der unternehmensinternen Infrastruktur entwickelt und betreffen Limits, die beispielsweise durch die Konfiguration von Firewalls und dem Firmennetzwerk entstehen. Andere betreffen die Kommunikation innerhalb des Blockchain-Netzwerkes, sowie die Blockchain selbst. Diese Anforderungen entspringen hauptsächlich Überlegungen über die Sicherheit des Systems, sowie der Grundidee, einzelne Netzwerkteilnehmer nur mit für sie unbedingt notwendigen Daten in Kontakt kommen zu lassen. Die wesentlichen Anforderungen an das System sind im Nachfolgenden aufgeführt:

[1] Deliktsbezeichnungen gekürzt

[2] https://safe-ur-chain.de/about

- Die Netzwerkinterne Kommunikation erfolgt über TCP/IP
- Die Kommunikation über Unternehmensgrenzen hinaus erfolgt über HTTPS
- Das Blockchain-Netzwerk baut sich selbstständig auf
- Beim Netzwerkaufbau kommen keine Broadcast-nachrichten zum Einsatz
- Nachrichten innerhalb des Netzwerkes werden signiert
- Neue Nodes synchronisieren die Blockchain automatisch
- Das Fehlen von Nutzdaten darf den Block-Hash nicht beeinflussen

3. Node-Architektur

Auf Basis dieser Anforderungen wurde die Software der Blockchain-Nodes entwickelt. Diese Software teilt sich in verschiedene Module, die den Fokus des restlichen Kapitels bilden.

3.1. Blockchain

Das zentrale Modul der Node-Software bildet Funktionen der Blockchain ab. Es wurde auf den drei Ebenen der Transaktionen, Blöcke, sowie der eigentlichen Blockchain implementiert.

Transaktionen stehen in der untersten Ebene der Blockchain-Hierarchie, sie enthalten die eigentlichen Nutzdaten, die vom Netzwerk gespeichert werden sollen. Um jegliche Art von Daten aufnehmen zu können, bieten Transaktionen das *payload*-Feld, in dem Daten als Bytes abgelegt werden können. Der Datentyp wird vom *contents*-Feld repräsentiert und für die Deserialisierung der Daten verwendet. Um die Herkunft der Daten anzuzeigen, wird ihr Hash-Wert von der Node, die sie aufgenommen hat signiert und im *signed_hash*-Feld abgespeichert. Mit dieser Information können die Nutzdaten nun auch aus der Transaktion entfernt, später aber auch wieder zugeordnet werden. Transaktionen, die keine Nutzdaten mehr enthalten werden als *stripped* bezeichnet und können zur Einsparung von Bandbreite bzw. für die Geheimhaltung sensibler Daten verwendet werden. Zusätzlich zum signierten Hash erhält jede Transaktion zum späteren Auffinden eine eindeutige Identifikationsnummer. Diese wird deterministisch aus dem signierten Hash der Nutzdaten, sowie dem Zeitstempel der Transaktion erzeugt (dieser ist in den Metadaten enthalten). Zusätzlich können im Feld *tags* Schlagwörter hinterlegt werden, die eine effiziente Suche nach Transaktionen ermöglichen. Sie geben den Nutzern des Systems eine Möglichkeit, Transaktionen beispielsweise mit intern verwendeten Teilenummern oder Maschinenkennungen zu versehen.

```rust
pub struct Transaction {
    pub id: Vec<u8>,
    pub tags: Vec<String>,
    pub signed_hash: SignedData,
    pub contents: TransactionV1Contents,
    pub payload: Vec<u8>,
    pub stripped: bool,
    pub meta: TransactionMetaData,
}
```

Abbildung 1: Datenstruktur für eine Transaktion

Mehrere Transaktionen werden zu Blöcken zusammengefasst, dafür wird eine Merkle-Tree-Struktur [5] verwendet, bei der in unterster Ebene die IDs der Transaktionen stehen, da diese IDs unabhängig davon sind, ob die Transaktion Nutzdaten enthalten oder nicht, erhält der Merkle-Tree immer den gleichen Root-Hash, selbst wenn einige oder alle der Transaktionen frei von Nutzdaten sind.

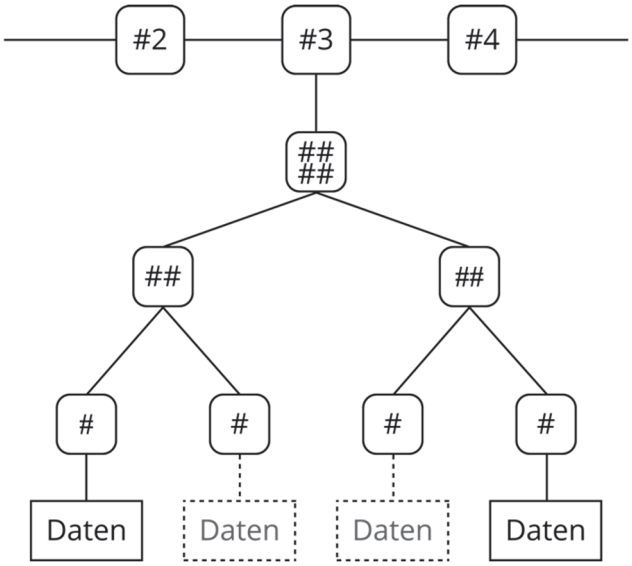

Abbildung 2: Merkle-Tree mit einigen fehlenden Nutzdaten und der Verknüpfung von dessen Root-Hash mit einem Block

Zusätzlich zu dieser Baumstruktur enthalten Blöcke auch *Header*, diese Datenstruktur enthält einige Metadaten, wie den Zeitstempel und die Block-Höhe, sowie Felder, die eingesetzt werden, um die Blockerzeugung nach den Regeln verschiedener Konsensverfahren zu erlauben. So können die Felder *difficulty*, *nonce* und *signatures* in unterschiedlichen Konsensverfahren verschiedene Rollen einnehmen. Dies ermöglicht es den Unternehmen, in ihrer lokalen Blockchain ein Konsensverfahren einzusetzen, das speziell auf ihren Anwendungsfall angepasst ist. Zum Testen dieser Funktionalität wurden *Proof of Work*, *Proof of Elapsed Time*, sowie ein Verfahren, bei dem Blöcke valide werden, wenn sie von ausreichend vielen Nodes signiert wurden, implementiert.

```rust
pub struct BlockHeader {
    pub timestamp: u128,
    pub previous_digest: Vec<u8>,
    pub difficulty: Difficulty,
    pub nonce: Vec<u128>,
    pub height: usize,
    pub merkle_root: Vec<u8>,
    pub signatures: Vec<SignedData>,
}

pub struct Block {
    pub header: BlockHeader,
    pub data: MerkleTree,
    hash: Option<Vec<u8>>,
}
```

Abbildung 3: Datenstrukturen für einen *Block* und dessen *Header*

Die Datenstruktur für Blöcke beinhaltet zusätzlich ein Feld für den Block-Hash. Dieser wird im Netzwerk nicht übertragen und von jeder Node selbst erzeugt, indem der Hash des Headers gebildet wird (in diesem ist der Root-Hash des Merkle-Trees enthalten).

Die oberste Ebene der Blockchain-Struktur wird als Baum-Struktur abgebildet, in der neue Blöcke an ihren jeweiligen Vorgänger angehangen werden. Um die korrekte Blockchain zu erzeugen, bzw. um Forks aufzulösen, verwendet diese Baumstruktur je nach Konsensverfahren eine Scoring-Funktion, mit der jeder Block eine Punktzahl erhält, diese Punktzahl, sowie die Summe der Punktzahlen der Vorgängerblöcke wird von jedem Element der Baumstruktur gespeichert. Um nun die korrekte/längste/gültige Kette zu bilden, wird das Ende mit der höchsten Punktzahl gesucht und dessen Vorgänger werden aufgelöst. Die Baumstruktur kann ebenfalls verwaiste Blöcke[3] aufnehmen, diese werden automatisch in die Kette integriert, sobald ihr Vorgänger hinzugefügt wird. Diese Funktion ist rekursiv implementiert, damit auch Ketten von verwaisten Blöcken korrekt an die Blockchain angehangen werden.

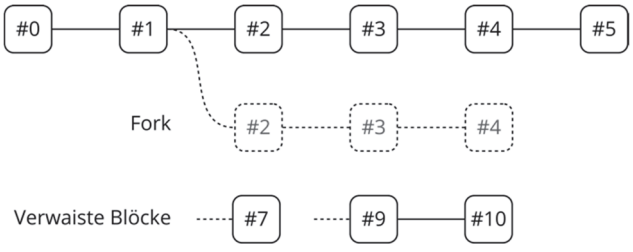

Abbildung 4: Baumstruktur zur Speicherung von Blöcken mit der „korrekten“ Kette (oben), einer Fork (mittig) und verwaisten Blöcken (unten)

Um diese Datenstrukturen zu speichern und für die Software verfügbar zu machen, wurde ein Speicher auf Basis einer Dateisystem-Datenbank entwickelt, der die Ebenen der Blockchain-Struktur widerspiegelt und einen Datenabruf in konstanter Zeit ermöglicht. Zusätzlich wurde aus dieser Speicherstruktur ein Interface abgeleitet, das es Unternehmen ermöglicht, ihre eigenen Speicherlösungen an die Node-Software anzuschließen.

3.2. Datenaufnahme

Das Datenaufnahmemodul bietet ein generisches Interface mit dem Daten in das System eingespeist werden können. Über dieses Interface können Daten entweder als reine Rohdaten oder als Bündel aus Roh-und Metadaten übertragen werden. Die eingegangenen Datensätze werden dann von der Blockchain-Node signiert und in Transaktionen eingearbeitet, die in die Blockchain geschrieben werden. Unternehmen können mithilfe dieses Interfaces ihre eigenen Protokolle mit beliebiger Logik umsetzen.

Für dieses Interface wurden bereits drei Implementierungen geschrieben. Die erste erlaubt die Aufnahme von Daten direkt aus dem Dateisystem. Dabei wird lediglich ein Verzeichnis auf neue Dateien überwacht, sobald diese erkannt werden, wird ihr Inhalt eingelesen und daraus Transaktionen erstellt. Die zweite Implementierung wurde als Gegenstelle zu einem proprietären Kommunikationsprotokoll von einem der Projektpartner entwickelt. Dieses Protokoll erlaub die Aufnahme von verschlüsselten Nutzdaten mit Metadaten direkt von den Maschinen des Partners. Mit dem Interface für die Datenaufnahme lassen sich beliebige Netzwerkprotokolle einbauen, so ermöglicht die dritte Implementierung die Übertragung von Dateien über HTTP, damit können Nutzdaten beispielsweise über den Dateiupload in einem Webbrowser an die Blockchain-Node übergeben werden.

3.3. Netzwerk

Die bisher beschriebenen Module bieten die grundlegenden Datenstrukturen für die Blockchain, sowie eine Möglichkeit, Daten in diese aufzunehmen. Das Netzwerk-Modul ermöglicht es, diese Funktionalitäten im Netzwerk zu verteilen. So werden aufgenommene Daten in das Netzwerk geschickt und dort von Nodes die Blöcke erzeugen aggregiert. Die erzeugten Blöcke müssen ihrerseits auch im Netzwerk verteilt und auf den empfangenden Nodes an die Blockchain angefügt werden.

Um diese Funktionen bereitzustellen, bietet das Netzwerkmodul eine interne API, über die andere Prozesse ausgehende Nachrichten an das Netzwerkmodul übergeben und eingehende Nachrichten vom Netzwerkmodul abrufen können. Die Logik, die innerhalb des Moduls für den Aufbau und Erhalt des Netzwerkes zuständig ist, wurde vom restlichen System abgekapselt.

[3] Blöcke die vor ihrem Vorgänger empfangen wurden

Der Netzwerkaufbau darf laut den bereits genannten Anforderungen nicht auf Broadcast-Nachrichten aufbauen. Darum erhalten Nodes beim ersten Start eine Liste von anderen Nodes, die mit hoher Wahrscheinlichkeit online sind. Diese Nodes werden als Seed-Nodes bezeichnet. Das Netzwerkmodul einer neu gestarteten Node beginnt damit, Nachrichten an die Seed-Nodes zu schicken, die eine Anfrage nach deren Liste von bekannten Nodes enthält. Nach Erhalt dieser Liste, schickt das Netzwerkmodul die gleiche Anfrage auch an die nun bekannten Nodes, bis eine gewisse Mindestanzahl an bekannten Nodes erreicht ist.

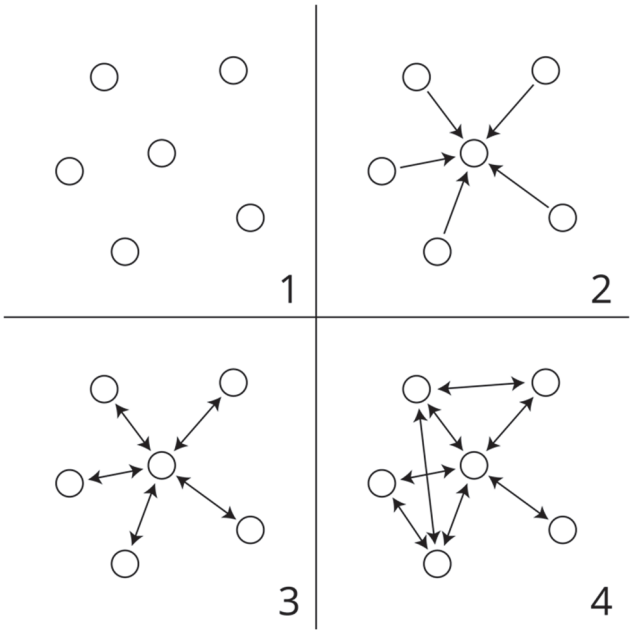

Abbildung 5: Schrittweiser Netzwerkaufbau mit Hilfe einer Seed Node; 1) Keine Verbindungen; 2) Unidirektionale Verbindungen zur Seed-Node (Anfragen); 3) Erste bidirektionale Verbindungen zwischen Nodes; 4) Verbindungen zwischen Nodes die sich durch Informationen der Seed Node finden konnten

Nodes streben danach, eine dauerhafte Verbindung zu einigen anderen Nodes aufrechtzuerhalten. Diese werden zufällig aus der Liste der bekannten Nodes ausgewählt und regelmäßig erneuert. Damit soll die zufällige oder böswillige Abschottung von Nodes verhindert werden.

3.4. Kryptographie

Alle Transaktionen und Netzwerk-Nachrichten werden von den Nodes signiert. Dafür erhalten Nodes je ein Schlüsselpaar aus einem öffentlichen und privaten Schlüssel. Diese Schlüssel werden in der aktuellen Implementierung durch ein hierarchisch-deterministisches Verfahren [6] erzeugt und beispielsweise durch einen Administrator auf die Nodes verteilt. Der erweiterte öffentliche Schlüssel ist allen Nodes bekannt, damit können neue Nodes dem Netzwerk beitreten, ohne dass ihr öffentlicher Schlüssel bekanntgegeben werden muss, andere Nodes können dieses mithilfe des erweiterten öffentlichen Schlüssels, sowie der Kennung der neuen Node erzeugen.

Die Logik für die Kryptographie wurde in ein separates Modul gekapselt, dieses bietet Funktionen zum Signieren, Hashen und Verschlüsseln von Daten. Die Verschlüsselung wurde dabei über ein das *Elliptic Curve Integrated Encryption Scheme* [7] umgesetzt. In diesem hybriden Verschlüsselungsverfahren wird der öffentliche Schlüssel des Empfängers zum Verschlüsseln eines temporären, symmetrischen Schlüssels genutzt, mit dem die Nutzdaten verschlüsselt werden. Damit können Nodes ohne zusätzliches Setup verschlüsselte Nachrichten untereinander austauschen.

3.5. Processing

Innerhalb der Node fallen viele verschiedene Aufgaben an. So müssen beispielsweise empfangene Blöcke verarbeitet, fehlende Blöcke angefragt und Transaktionen erstellt werden. Diese Aufgaben werden innerhalb der Node vom Processing-Modul verarbeitet. Dieses Modul gibt Warteschlangen für Aufgaben frei, die von einer konfigurierbaren Anzahl von *Worker*-Threads abgearbeitet und die anderen Module weitergegeben werden.

Zusätzlich hat dieses Modul die Aufgabe, regelmäßige Überprüfungen zum Zweck von Instandhaltungsarbeiten der lokalen Blockchain durchzuführen. Beispielsweise werden lokal erzeugte Transaktionen so lange gespeichert, bis sie in der Blockchain des Netzwerkes auffindbar sind. Falls Transaktionen nach einer gewissen Zeit nicht in die Blockchain aufgenommen wurden, reiht das Modul eine erneute Verteilung im Netzwerk ein. Zusätzlich wird regelmäßig geprüft, ob die lokale Blockchain auf dem aktuellen Stand des Netzwerkes ist, dafür werden Blockchain-Status Nachrichten im Netzwerk, sowie das Alter des aktuellsten lokalen Blockes herangezogen. Sollte festgestellt werden, dass die lokale Blockchain nicht mehr aktuell ist, werden Anfragen an das Netzwerk eingeleitet. Über diesen Mechanismus synchronisieren sich auch Nodes, die zum ersten Mal gestartet werden.

3.6. Architektur

Die in diesem Kapitel beschriebenen Module arbeiten in sechs Funktionsgruppen zusammen, die gemeinsam die Blockchian-Node bilden:

Gruppe	Aufgabe(n)
Netzwerk	Netzwerkverwaltung; Kommunikation mit anderen Nodes
Blockchain	Zusammenfassung von Blöcken zur Blockchain
Blockerzeuger	Sammlung von Transaktionen; Erzeugung neuer Blöcke
Speicher	Speicherung und Bereitstellung von Blockchain, Blöcken und Transaktionen
Datenaufnahme	Entgegennahme von Roh- und Metadaten

Processing	Bearbeitung von Aufgaben und Umsetzung von Datenströmen zwischen den anderen Funktionsgruppen

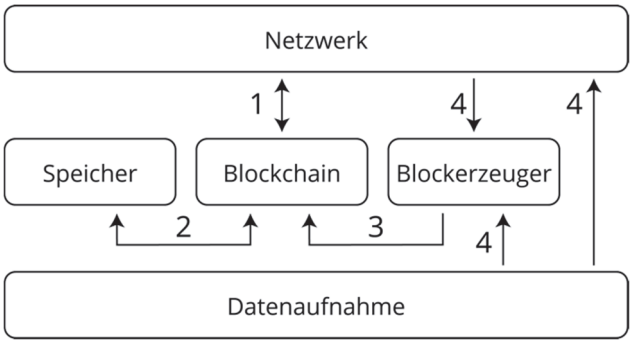

Abbildung 6: Funktionsgruppen und Datenströme zwischen ihnen (Processing); 1) Blöcke und Anfragen nach Daten; 2) Blockchain + alle assoziierten Daten; 3) Blöcke; 4) Transaktionen

4. Netzwerk-Architektur

Das Gesamtnetzwerk lässt sich in zwei Ebenen aufteilen: die lokale Ebene beinhaltet die einzelnen Netzwerke der Unternehmen, die von den Blockchain-Nodes gebildet werden. Und die globale Ebene, über die diese lokalen Netzwerke Informationen austauschen können.

4.1. Lokales Netzwerk

Das lokale Netzwerk besteht aus mehreren Blockchain-Nodes, wie sie in Kapitel 3 beschrieben worden. Um dieses Netzwerk besser an die spezifischen Anforderungen einzelner Unternehmen anpassen zu können, werden bei einigen Nodes die Funktionsgruppe „Blockerzeuger" und „Speicher" abgeschaltet bzw. anders konfiguriert. Durch die Abschaltung des Blockerzeugers können Nodes auf Hardware mit weniger Rechenleistung betrieben werden, da die rechenaufwändige Aufgabe des Zusammensetzens von Transaktionen in Blöcke wegfällt. Und durch die angepasste Konfiguration der Speicher-Funktionsgruppe kann die Speicherung einiger oder aller Transaktionsnutzdaten umgangen werden. Damit können Nodes auf Hardware mit deutlich weniger Speicher betrieben werden.

Es ergeben sich vier verschiedene Node-Typen:

	Blockerzeuger	Speicher
Full Node	Aktiviert	Alle Nutzdaten
Blockerzeuger Node	Aktiviert	Teilweise/Keine Nutzdaten
Archiv Node	Deaktiviert	Alle Nutzdaten
Thin Node	Deaktiviert	Teilweise/Keine Nutzdaten

Durch den gezielten Einsatz dieser Node-Typen können Netzwerke genau an die verfügbare Hardware und den Anwendungsfall angepasst werden. So könnten Thin Nodes innerhalb einer Fabrik direkt an Maschinen die Produktionsdaten aufnehmen und diese an Blockerzeuger Nodes schicken. Die entstehende Blockchain kann dann für den Langzeitspeicher in einem Cluster von Archiv-Nodes gespeichert und von diesen für andere Applikationen zur Verfügung gestellt werden.

4.2. Globales Netzwerk

Auf der Ebene des globalen Netzwerkes tauschen lokale Netzwerke Daten untereinander aus. Dafür werden eine oder mehrere Instanzen eines Message Brokers genutzt, der projektintern aufgrund seiner Funktionsweise als „Post Office" bezeichnet wird. Dieser Broker nimmt verschlüsselte Nachrichten von allen Netzwerken entgegen, sammelt diese und schickt sie auf Anfrage an das Zielnetzwerk der Nachrichten. Die Verschlüsselung der Nachrichten erfolgt über das bereits beschriebene Hybridverfahren, sodass nur Nodes im Zielnetzwerk die Nachrichten entschlüsseln können. Damit wird sichergestellt, dass Nachrichten, die über den Broker versandt werden, nicht von außen mitgelesen werden können.

Die wesentlichen Nachrichten, die Netzwerke austauschen, sind Block-Hashes. Diese werden verwendet, um die Daten innerhalb der lokalen Blockchains von den anderen Teilnehmern des globalen Netzwerkes „gegenzeichnen" zu lassen. Dafür werden empfangene Block-Hashes aus fremden Netzwerken innerhalb eines lokalen Netzwerkes als Transaktion in die Blockchain aufgenommen. Sobald der Hash eines Blockes, der einen anderen Block-Hash als Transaktion enthält in einem anderen Netzwerk in die Blockchain aufgenommen wird, kann an beiden Blockchains bis zu diesem Zeitpunkt keine Veränderung mehr vorgenommen werden, selbst wenn dies vom Konsensverfahren erlaubt würde. Wenn dieses Verfahren von mehreren Unternehmen regelmäßig angewandt wird, werden die Blockchains ineinander „verstrickt". Abbildung 7 veranschaulicht den Prozess.

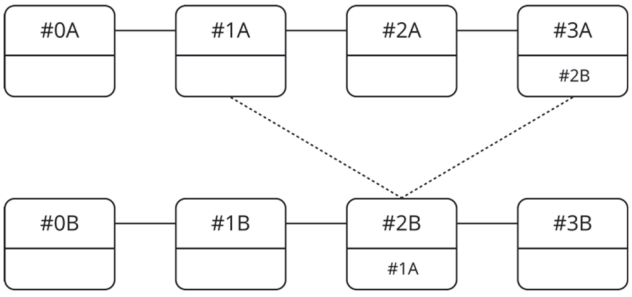

Abbildung 7: „Verstrickte" Blockchains zweier Netzwerke; Die oberen Bereiche der Blöcke enthalten die Blocknummer, die unteren die Hashes von Blöcken externer Blockchains

Der Umgang mit Forks in einem oder mehreren der Netzwerke, sowie ein effizienter Beweis über die Existenz von Daten in einer so verstrickten Blockchain sind Gegenstand laufender Forschung.

5. Anwendungsfall

Ein Anwendungsfall für das System besteht in der Rückverfolgung eines fehlerhaften Produktes. In diesem Anwendungsfall produziert Unternehmen **A** Bauteile, die von Unternehmen **B** verbaut werden. Dabei protokolliert **A** die eigene Produktion sowie eine Qualitätsprüfung auf seiner lokalen Blockchain und gibt die betreffenden Transaktions-IDs mit dem Versand weiter. Unternehmen **B** protokolliert diese IDs beim Wareneingang, und die Montage der eigenen Produkte auf seiner Blockchain.

Sollte im Produkt ein Fehler auftreten, der sich nicht auf die Montage von **B** zurückführen lässt, kann die Preisgabe der Ergebnisse der Qualitätskontrolle von Unternehmen **A** gefordert werden. Die Informationen in dieser Transaktion sind auf Seite von Unternehmen **B** durch die beim Wareneingang erhaltenen Transaktions-IDs nachvollziehbar und können durch die „Verstrickung" der Blockchains zeitlich eingeordnet werden. Wenn festgestellt wird, dass das Bauteil zum Zeitpunkt der Qualitätskontrolle fehlerfrei war, kann davon ausgegangen werden, dass es während des Transportes beschädigt wurde. Andernfalls kann Unternehmen **A** den Fehler weiter zurückverfolgen und für eine Entschädigung sorgen.

6. Ergebnisse

Das beschriebene Netzwerk ist mit Ausnahme der in 4.2 benannten Funktionen, die noch erforscht werden, vollständig implementiert und erfüllt die genannten Anforderungen. Als besonderes Ergebnis ist die Sicherheit zu nennen, mit der die Integrität von Daten innerhalb der Blockchain über Netzwerkgrenzen hinweg belegt werden kann.

Die Node-Software wurde in der Programmiersprache Rust[4] implementiert und umfasst zum Zeitpunkt des Schreibens dieses Papers annähernd 8000 Zeilen Code, die zu einer ausführbaren Binärdatei mit einer Größe von 13,9MB[5] kompiliert werden. Durch die geringe Größe der Binärdatei und den überschaubaren Quellcode kann die Software für viele Anwendungsgebiete verwendet und angepasst werden. Aktuelle Integrationstests zeigen einen Transaktionsdurchsatz von über 100 Transaktionen pro Sekunde.

Im weiteren Projektverlauf soll ein Sicherheitsaudit des Systems, sowie eine Evaluation durch die testweise Anwendung bei den Industriepartnern durchgeführt werden. Erste Tests, darunter die Erprobung eines Testnetzes über mehrere Monate wurden erfolgreich ausgeführt.

Förderhinweis

Das Vorhaben wird mit Mitteln des Bundesministeriums für Bildung und Forschung im Rahmen der Bekanntmachung „Zivile Sicherheit – Kritische Strukturen und Prozesse in Produktion und Logistik" unter den Förderkennzeichen 13N15150 bis 13N15153 gefördert.

Literaturverzeichnis

[1] Siemens. The Digitalization Productivity Bonus, 2017, 7-9.

[2] Bundeskriminalamt. Cybercrime Bundestagsbild 2020, 2021, 3-11.

[3] Statista. Polizeilich erfasste Fälle von Cyberkriminalität im engeren Sinne in Deutschland von 2007 bis 2020 [Online; aufgerufen am 30.08.2021] https://de.statista.com/statistik/daten/studie/295265/umfrage/polizeilich-erfasste-faelle-von-cyberkriminalitaet-im-engeren-sinne-in-deutschland/

[4] Bundesministerium für Bildung und Forschung. Sicherheit und Nachverfolgbarkeit in zivilen Produktions- und Wertschöpfungsnetzwerken durch Blockchain (safe-UR-chain), 2019 [Online; aufgerufen am 30.08.2021] https://www.sifo.de/files/Projektumriss_safe-UR-chain.pdf

[5] Merkle, R., Protocols for Public Key Cryptosystems, 1980 IEEE Symposium on Security and Privacy, 1980, 125–127

[6] Bitcoin Core Team. BIP 32 [Online; aufgerufen am 30.08.2021] https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki

[7] ECIES Developers. eciesrs [Online; aufgerufen am 30.08.2021] https://github.com/ecies/rs

[4] https://www.rust-lang.org

[5] Die Größe bezieht sich auf die Version für Unix-basierte Betriebssysteme

Faktoren für das Verständnis und die Nutzungsintention der Blockchain-Technologie

Josephine Halama, Nicole Ebert, Sebastian Mach
TU Chemnitz, Institut für Psychologie, Wilhelm-Raabe-Straße 43, 09120 Chemnitz

Während Blockchain großes Potenzial bietet und erste Anwendungen bereitstehen, ist eine der größten Nutzungsbarrieren von Blockchain-Anwendungen, dass Novizen Blockchain nicht verstehen. In der vorliegenden Onlinestudie (N = 68) wurden daher unterschiedliche Lernmaterialien (neutral vs. interessant) genutzt, um Novizen Blockchain näher zu bringen. Weiterhin wurde untersucht, ob das Interesse am Thema, der Bildungsstand, das Alter oder das Geschlecht einen Einfluss auf die Nutzungsintention, das subjektiv eingeschätzte oder das objektive Verständnis haben. Interesse, Alter und Bildung standen im Zusammenhang mit dem Verständnis, die Nutzungsintention unterschied sich hingegen nur bei unterschiedlichem Interesse. Zudem kommt die Studie zu dem Schluss, dass ein mangelndes subjektives Verständnis die eigentliche Nutzungsbarriere darstellt, nicht jedoch ein mangelndes objektives Verständnis. Des Weiteren weist die Studie auf Personengruppen hin, die einen anderen Informationsbedarf aufweisen, um von Blockchain bzw. der Digitalisierung allgemein zu profitieren.

1. Einleitung

Blockchain wird als eine der innovativsten Technologien des 21. Jahrhunderts mit einem hohen Potential für technische und gesellschaftliche Veränderungen angesehen [1]. Neben der bekanntesten Anwendung, den Kryptowährungen wie Bitcoin oder Ethereum, gibt es zahlreiche weitere Anwendungsfelder wie die Energiebranche, Produktion und Logistik, Medizin oder Bildung, bei denen der Einsatz der Blockchain vielversprechend ist [2]. Während dieses Potential unter Blockchain-ExpertInnen vieldiskutiert ist, ist die Technologie unter der Allgemeinbevölkerung, sogenannten Blockchain-Novizen, noch recht unbekannt [3].

Einer breiten Nutzung von Blockchain-Anwendungen stehen zahlreiche Barrieren entgegen. Bei einer induktiven Inhaltsanalyse relevanter Publikationen wurden sechzehn Barrieren identifiziert, wie z. B. mangelndes Vertrauen oder eine mangelnde Benutzerfreundlichkeit [1]. Die wichtigste Barriere stellte das fehlende Verständnis der Technologie dar. Die Relevanz der Technologie, deren Vorteile und das Potential für die Anwendungsfälle würden somit nicht ausreichend erkannt. Blockchain wurde häufig auch als zu komplex eingestuft, um die Aufmerksamkeit der Allgemeinbevölkerung auf sich zu ziehen [1].

Die vorliegende Studie beschäftigt sich mit der Frage, ob und wenn ja, wie Blockchain-Novizen die Technologie, deren Potential sowie mögliche Anwendungen möglichst einfach vermittelt werden können. Zur Beantwortung dieser Forschungsfrage sollen Theorien und Methoden der psychologischen Forschung genutzt werden.

Die kognitionspsychologischen Grundlagen, wie Menschen lernen, existieren bereits seit den 1960er-Jahren. Im Mehrspeichermodell (Bild 1) wird angenommen, dass wir eine Vielzahl von Informationen unserer Umwelt zunächst über das sensorische Register aufnehmen, diese aber nur für Sekundenbruchteile darin aufrechterhalten können [4]. Informationen, denen wir Aufmerksamkeit schenken, gelangen in das Kurzzeitgedächtnis (auch als Arbeitsgedächtnis bezeichnet). Dort findet die Verarbeitung von Informationen statt und der Informationsaustausch mit dem Langzeitgedächtnis erfolgt. Zudem kann eine Reaktion auf die Information ausgelöst werden.

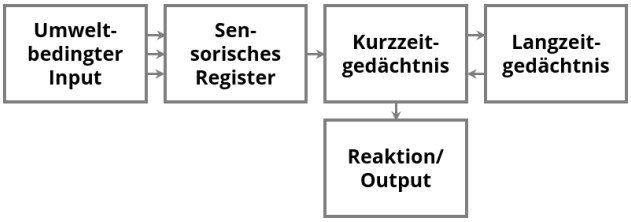

Bild 1. Mehrspeichermodell [4], eigene Darstellung

Wenn Menschen etwas (über Blockchain) lernen, findet demnach zunächst eine Verarbeitung der Informationen im Kurzzeitgedächtnis statt und es erfolgt eine Überführung in das Langzeitgedächtnis, den dauerhaften Wissensspeicher. Besonders gut gelingt eine solche Überführung, wenn neue Informationen an bereits bekannte Wissensstrukturen, sogenannten Schemata, anknüpfen können [5]. Während das Langzeitgedächtnis über eine sehr große Kapazität verfügt, ist die Kapazität des Kurzeitgedächtnisses begrenzt und sollte daher durch eine gezielte Aufmerksamkeitslenkung unterstützt werden.

Auf die Erkenntnisse über die Funktion unseres Gedächtnisses baut auch die Cognitive Load Theory auf [6, 7]. Sie trifft Aussagen darüber, wie Menschen lernen und wie eine optimale mentale Belastung, der Cognitive Load, erzielt werden kann, um ein größtmögliches Verständnis des Lernmaterials zu erreichen. Dazu wird angenommen, dass ein Lernprozess in drei verschiedene, additiv verknüpfte Komponenten geteilt ist: Den Intrinsic Load, den Extraneous Load und den Germane Load (Bild 2). Der Intrinsic Load wird durch die Komplexität des Lernmaterials und individueller Eigenschaften der lernenden Person bestimmt. Wenn die Person beispielsweise über ein hohes Vorwissen zum Lerninhalt verfügt

(ExpertInnen), wird es für sie leichter sein, an bestehende Wissensstrukturen anzuknüpfen. Der Extraneous Load ist die mentale Belastung, die vom Lernmaterial ausgeht. Je nachdem wie kompliziert oder einfach das Lernmaterial gestaltet ist, steigt oder fällt diese mentale Belastung. Zudem sollte das Lernmaterial interessant gestaltet werden, da ein höheres Interesse zu einem höherem Lernerfolg führt [8, 9]. Der Germane Load beschreibt den Prozess des Verstehens und beinhaltet damit den mentalen Aufwand, der benötigt wird, um einen Inhalt zu erfassen. Wenn diese Loads gut aufeinander abgestimmt sind, kann eine optimale Lernleistung erzielt werden. Ist die mentale Belastung insgesamt hingegen zu groß, kommt es zu einem Overload [7], der zu einem sogenannten Blackout führen kann.

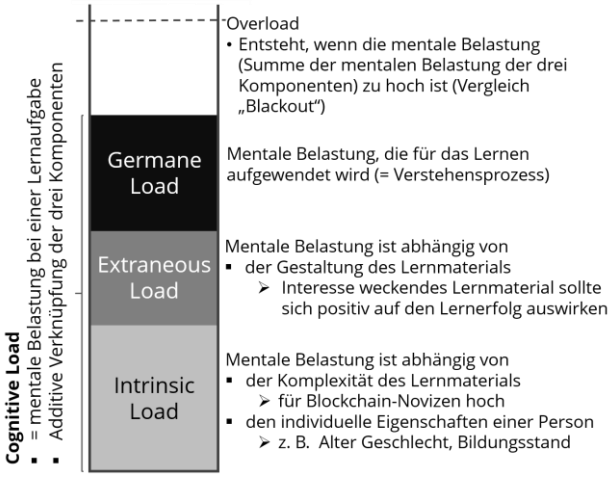

Bild 2. Übertragung der Cognitive Load Theory auf das Erlernen von Blockchain-Inhalten

Bezieht man diese Erkenntnisse auf das Erlernen der Blockchain, ergibt sich folgende Ausgangssituation: Für den Germane Load, das Verstehen des Erlernten, sollte möglichst viel mentale Kapazität zur Verfügung stehen, damit Personen möglichst viel über Blockchain lernen. Die Gestaltung des Lernmaterials (Extraneous Load) sollte in einem möglichst geringen Aufwand resultieren, Blockchain zu verstehen. Lernmaterial sollte für Novizen demnach möglichst leicht verständlich gestaltet werden. Zudem dürfte sich ein Interesse weckendes Lernmaterial über Blockchain positiv auf das Verständnis auswirken, da das Interesse an einem Thema den Lernerfolg erhöht [8, 9]. Der Intrinsic Load, wird zum einen durch die Komplexität des Lernmaterials bestimmt: Für Blockchain-Novizen ist diese intrinsische Belastung hoch, weil es sich bei Blockchain um ein komplexes Thema handelt [1]. Zum anderen wird der Intrinsic Load durch Eigenschaften der Person beeinflusst. Es wird einer Person leichter fallen, neue Informationen über Blockchain zu lernen, wenn sie gut an bereits bestehende Schemata anknüpfen kann. Dies sollte für Blockchain-Novizen mit einem höheren Bildungsstand leichter sein als für Personen mit einem geringeren Bildungsstand.

Auch das Alter einer Person könnte einen Einfluss darauf haben, inwieweit eine Person über passende Wissensstrukturen verfügt, um beim Erlernen von Blockchaininhalten daran anknüpfen zu können. Personen, die mit digitalen Inhalten aufgewachsen sind, sogenannte Digital Natives [10], verfügen in der Regel über ein höheres Verständnis digitaler Technologien. Beim Erlernen von Inhalten über Blockchain könnten sie dieses Wissen (z. B. über die Organisation digitaler Datenbanken oder die Funktionsweise verschiedener Speichermedien) nutzen, um ihr neu erworbenes Wissen daran anzuknüpfen. Personen, die ohne digitale Angebote aufgewachsen sind, sogenannte Digital Immigrants, fällt es in der Regel schwerer, digitale Inhalte oder Funktionsweisen digitaler Geräte zu erlernen. Die Unterscheidung in Digital Natives und Digital Immigrants kann aufgrund des Geburtsjahres erfolgen. Personen, die vor 1980 geboren sind, gelten als Digital Immigrants, jüngere Personen als Digital Natives [11]. Diese Zweiteilung sollte allerdings nur als Orientierung betrachtet werden und kann im Einzelfall durchaus falsch sein.

Eine weitere Eigenschaft, die dem Intrinsic Load zuzuordnen ist und einen Einfluss auf die Lernleistung haben könnte, ist das Geschlecht. Allerdings gibt es bei dieser Variable keine Evidenz dafür, dass Frauen oder Männer, Lernmaterialien zum Thema Blockchain objektiv leichter verstehen könnten, da es im Mittel keine Intelligenzunterschiede zwischen den Geschlechtern gibt, Männer lediglich in den Extremgruppen häufiger vertreten sind [12]. Mögliche Unterschiede im objektiven Verständnis zwischen den Geschlechtern sollten durch das gleichzeitige Auftreten anderer Variablen erklärbar sein, wie z. B. das Interesse oder das Vorwissen. Unterschiede im subjektiven Verständnis beim Erlernen von Inhalten über Blockchain sind zwischen Männern und Frauen jedoch vorstellbar. So zeigte beispielsweise eine Untersuchung zu Fertigkeiten am Computer [13], dass sich die objektive Leistung zwischen Männern und Frauen nicht unterschied, Frauen ihre Leistung jedoch subjektiv schlechter einschätzten. Eine Erklärung dafür könnten Geschlechtsstereotype sein, durch die Frauen im technischen Bereich als weniger kompetent wahrgenommen werden [14] und es dadurch auch zu einer geringeren Einschätzung der Leistung der in der Studie kam [13].

Aus den aufgeführten Überlegungen zum Intrinsic Load leitet sich die zweite Forschungsfrage ab: Gibt es Personengruppen, denen es schwerer fällt, Inhalte über Blockchain zu erlernen und damit möglicherweise weniger von den Potentialen der Technologie profitieren? Zudem stellt sich die Frage, ob ein geringeres Verständnis auch mit einer geringeren Nutzungsintention verbunden ist. Wenn, wie eingangs beschrieben [1], ein geringeres Verständnis mit einer geringeren Wahrnehmung des Potentials assoziiert ist und dies die wichtigste Nutzungsbarriere darstellt, sollte die Intention zur Nutzung bzw. zur Beschäftigung mit der Technologie ebenfalls geringer sein. Aus diesem Grund beschäftigt sich die vorliegende

Studie neben dem subjektiven und objektiven Verständnis auch mit der Nutzungsintention von Blockchain. Dabei soll untersucht werden, ob die Variablen, die einen möglichen Einfluss auf das subjektive und objektive Verständnis haben (Interesse, Bildungsstand, Alter und Geschlecht), auch im Zusammenhang mit der Nutzungsintention stehen.

Zur differenzierten Beantwortung der Forschungsfragen werden folgende Hypothesen (H) abgeleitet:

H1: Das subjektiv eingeschätzte Verständnis der ProbandInnen ist nach der kognitiven Auseinandersetzung mit der Blockchain-Technologie größer als vorher.

H2: ProbandInnen mit hohem Interesse am Thema Blockchain weisen nach einer kognitiven Auseinandersetzung mit der Technologie ein größeres subjektives (H2a) und objektives (H2b) Verständnis auf und geben eine höhere Nutzungsintention (H2c) an als ProbandInnen mit niedrigem Interesse.

H3: ProbandInnen mit einem höheren Bildungsstand weisen nach einer kognitiven Auseinandersetzung mit der Technologie ein größeres subjektives (H3a) und objektives (H3b) Verständnis auf und geben eine höhere Nutzungsintention (H3c) an als ProbandInnen mit einem geringeren Bildungsstand.

H4: Jüngere ProbandInnen weisen nach einer kognitiven Auseinandersetzung mit der Technologie ein größeres subjektives (H4a) und objektives (H4b) Verständnis auf und geben eine höhere Nutzungsintention (H4c) an als ältere ProbandInnen.

H5: Frauen weisen nach einer kognitiven Auseinandersetzung mit der Technologie ein geringeres subjektives Verständnis (H5a) und eine geringere Nutzungsintention (H5c) auf als Männer. Für das objektive Verständnis wird kein Unterschied zwischen Männern und Frauen erwartet (H5b).

H6: Das Verständnis der Blockchain-Technologie und deren Nutzungsintention zeigen einen großen Zusammenhang.

2. Methode

2.1 Design

Das mehrfaktorielle und multivariate Experiment wurde als Onlinestudie durchgeführt. Die erste unabhängige Variable, die manipuliert und den ProbandInnen zufällig zugewiesen wurde, war das Interesse an der Blockchain-Technologie, das durch unterschiedliche Lernmaterialien erzeugt wurde (neutral vs. interessant; between-subjects-Design). Des Weiteren wurden die Variablen Bildungsstand, Alter und Geschlecht quasi-experimentell (alle im between-subjects-Design) erhoben und deren Zusammenhang mit den abhängigen Variablen untersucht. Als abhängige Variablen dienten das subjektive und das objektive Verständnis der Blockchain-Technologie sowie die Nutzungsintention. Das subjektive Verständnis der Blockchain-Technologie vor der Präsentation des Lernmaterials, die Zeit, die ProbandInnen auf der Seite des Lernmaterials verbracht hatten, die Aufmerksamkeit der ProbandInnen und die User Experience des Lernmaterials wurden als Kontrollvariablen erfasst.

2.2 Stichprobe

ProbandInnen wurden über E-Mail-Verteiler der TU Chemnitz und persönliche Kontakte zur Studienteilnahme aufgefordert. Es nahmen insgesamt 80 Personen an der Studie teil. Davon wurden 12 Personen aus verschiedenen Gründen aus der Analyse ausgeschlossen (fünf mit hohem Vorwissen zum Thema Blockchain; fünf die weniger als eine Minute auf der Seite des Lernmaterials verbracht hatten; eine, die angab sich das Lernmaterial „*gar nicht aufmerksam*“ angeschaut zu haben und eine Person, die fast alle Fragen unbeantwortet ließ). Die Gesamtstichprobe für die Analyse betrug daher $N = 68$. Alle Versuchspersonen sprachenfließend Deutsch. Die ProbandInnen waren durchschnittlich 34 Jahre alt ($M = 33.77$, $SD = 15.34$, Range: 18-62 Jahre). Dreiviertel der ProbandInnen waren weiblich (75.0%, männlich: 25.0%, divers: 0%). Die Hälfte der ProbandInnen gab als höchsten Bildungsabschluss das (Fach-) Abitur an (50.0%, Hauptschulabschluss 1.5%, Realschulabschluss 23.5%, (Fach-) Hochschulabschluss 23.5%, ohne Angabe: 1.5%).

2.3 Untersuchungsmaterial

Zur Manipulation der unabhängigen Variable, dem Interesse an Blockchain, wurden Lernmaterialien entwickelt, die sich in ihrer Formulierung (neutral vs. interessant) unterschieden. In der neutralen Bedingung wurde keine Bewertung der Inhalte vorgenommen und es erfolgte keine persönliche Ansprache der ProbandInnen. Der Lerntext in der interessanten Bedingung enthielt hingegen solche Bewertungen, persönliche Ansprachen der ProbandInnen und Inhalte waren teilweise als rhetorische Fragen formuliert. Zwei Beispiele für solche unterschiedlichen Formulierungen sind: 1. neutral: „*Eine Möglichkeit zur Lösung stellt eine neue Technologie dar: die Blockchain.*“ vs. interessant: „*Eine vielversprechende Technologie, die die Lösung dieser Probleme sein könnte, ist Blockchain.*“; 2. neutral: „*Jedoch hat Blockchain neben den Vorteilen auch Nachteile.*“ vs. interessant: „*Können Sie sich vorstellen, dass so eine geniale Erfindung auch Nachteile haben kann?*“. Abgesehen von diesen Stilmitteln waren die beiden Lerntexte gleich und mit drei unterstützenden Bildern versehen (Beispiel siehe Bild 3).

Die Lerntexte enthielten folgende Informationen, die sprachlich möglichst einfach für Novizen aufbereitet waren: Herleitung zum Thema Blockchain (Digitalisierung), allgemeine Funktionsweise von Blockchains, Rolle der Hash-Funktion, Bitcoin, Smart Contracts und potenzielle Nachteile.

Für den Manipulationscheck wurde das Interesse an Blockchain mit drei Items erfasst, z. B. „*Die Beschäftigung*

mit der Blockchain-Technologie finde ich spannend.“ (Antwortskala: 1 = „*stimme überhaupt nicht zu*“ bis 7 = „*stimme vollkommen zu*“).

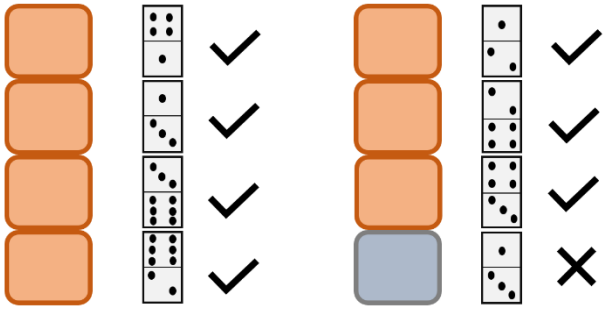

Bild 3. Beispielbild aus dem Lernmaterial, das eine Analogie zum Spiel Domino nutzt, um Blockchain zu erklären

Für die quasi-experimentelle Erfassung der Variablen Geschlecht, Alter und Bildungsstand wurde jeweils ein Item zu Beginn der Studie erhoben.

Das subjektive Verständnis wurde über das Item „*Wie gut schätzen Sie Ihr Wissen zum Thema Blockchain ein?*“ (Antwortskala: 1 = „*überhaupt nicht gut*“ bis 7 = „*sehr gut*“) vor und nach der Präsentation des Lernmaterials erfasst. Dabei diente das subjektive Verständnis vor dem Lernmaterial (prä) als Ausschlussvariable: ProbandInnen die angaben, mindestens ein mittleres Vorwissen (> 3) zu haben, wurden aus der Analyse ausgeschlossen. Das subjektive Verständnis nach der Präsentation des Lernmaterials (post) diente als abhängige Variable.

Für das objektive Verständnis wurden neun Wissensfragen zum Thema Blockchain entwickelt, die durch die Inhalte des Lernmaterials zu beantworten waren. Bei diesen Fragen handelte es sich um Single-Choice-Fragen, bei denen eine von vier Antwortalternativen richtig war. Um die Hypothesen zum objektiven Verständnis überprüfen zu können, wurde ein Punktwert berechnet, bei dem für jede richtig beantwortetet Frage ein Punkt vergeben wurde. Damit waren Ausprägungen von null bis neun für das objektive Verständnis möglich.

Die Nutzungsintention wurde über das Item „*Es ist zum jetzigen Zeitpunkt wahrscheinlich, dass ich mich in meiner Freizeit mit Blockchain beschäftige.*“ (Antwortskala: 1 = „*stimme überhaupt nicht zu*“ bis 7 = „*stimme vollkommen zu*“) erhoben.

Für die Erfassung der User Experience wurde der Fragebogen UEQ-S verwendet [15]. Dieser erfasst zum einen die Pragmatische Qualität, welche Aspekte wie die Durchschaubarkeit, die Effizienz oder die Steuerbarkeit beinhaltet und misst, wie gut eine Anwendung objektiv dazu geeignet ist, eine Aufgabe zu erfüllen. Zum anderen umfasst sie die Hedonische Qualität, bei der angegeben wird, wie viel Spaß die Anwendung macht und wie ansprechend diese ist.

Zudem wurde die Aufmerksamkeit der ProbandInnen kontrolliert, indem gefragt wurde „*Wie aufmerksam haben Sie sich das Lernmaterial angesehen?*“ (Antwortskala: 1 = „*gar nicht aufmerksam*“ bis 5 = „*sehr aufmerksam*“).

2.4 Durchführung

Die Onlinestudie wurde mit der Fragebogensoftware LimeSurvey durchgeführt. Zu Beginn erhielten ProbandInnen ausführliche Studieninformationen und Informationen zum Datenschutz und stimmten diesen bei Einverständnis zu. Danach folgte die Erhebung demographischer Angaben (Bildung, Alter, Geschlecht) sowie die subjektiven Einschätzungen zum Interesse (prä) und dem Verständnis (prä) von Blockchain. Anschließend wurde das Lernmaterial (neutral oder interessant) präsentiert. Danach gaben die ProbandInnen an, wie aufmerksam sie sich das Lernmaterial angesehen hatten. Als nächstes schätzten die ProbandInnen die Benutzerfreundlichkeit (User Experience) des Lernmaterials ein und machten Angaben zum Interesse am Thema Blockchain (post), der Nutzungsintention und dem subjektiven Verständnis von Blockchain (post). Den Abschluss der Studie bildeten die objektiven Wissensfragen. Dabei wurden die ProbandInnen explizit darauf hingewiesen keine zusätzlichen Informationsquellen für die Beantwortung der Fragen zu verwenden, um die Rückschlüsse über die Qualität des Lernmaterials nicht zu verzerren. Die Umfrage dauerte durchschnittlich 27 Minuten (M = 26.55, SD = 17.51). Zudem wurde erfasst, wie lange ProbandInnen auf der Seite des Lernmaterials verbrachten, um die Personen aus der Analyse auszuschließen, die sich das Lernmaterial nicht oder kaum angesehen hatten (< 1 Minute).

3. Ergebnis

3.1 Subjektives Verständnis (H1)

Bei den Berechnungen zur ersten Hypothese wurde überprüft, ob sich das subjektiv eingeschätzte Verständnis prä vom subjektiven Verständnis post unterschied. Wie die grafische Darstellung im Bild 4 bereits vermuten lässt, konnte ein signifikanter und großer Effekt festgestellt werden (t-Test für abhängige Stichproben: $t(65) = -9.90$, $p < .001$, $d = 1.39$). Im Mittel gaben die ProbandInnen vor der kognitiven Auseinandersetzung mit dem Lernmaterial ein subjektives Verständnis von $M = 1.24$ ($SD = 0.47$) und $M = 2.94$ ($SD = 1.40$) nach der Auseinandersetzung an. Die erste Hypothese, dass ProbandInnen nach der kognitiven Auseinandersetzung subjektiv mehr über Blockchain verstanden, wurde damit unterstützt.

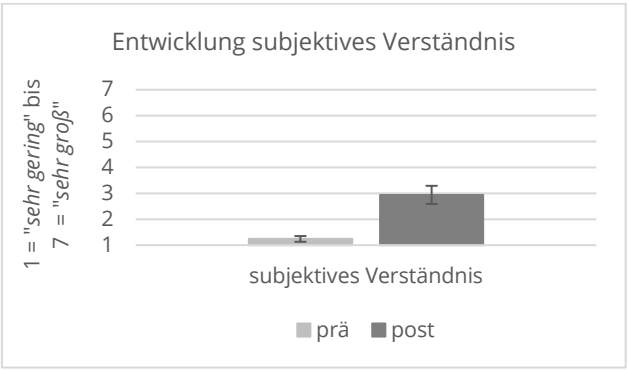

Bild 4: Anstieg des subjektiven Verständnisses; dargestellt sind Gruppenmittelwerte und 95%-Konfidenzintervalle

Untermauert wurden diese Ergebnisse auch mit dem insgesamt recht hohen objektiven Verständnis: Von den 9 Wissensfragen zum Lernmaterial beantworteten die Blockchain-Novizen durchschnittlich 5 Fragen richtig (*M* = 5.28, *SD* = 1.94, Range: 0-7, *N* = 68).

Zusätzlich zur Hypothesenprüfung wurde die User Experience des Lernmaterials untersucht, da aus der Literatur bekannt war, dass die Benutzerfreundlichkeit von Blockchain-Anwendungen eine wahrgenommene Nutzungsbarriere darstellt [1] und eine mangelnde User Experience des Lernmaterials ebenfalls eine Barriere für die Nutzungsintention darstellen könnte. Die Deskriptive Analyse zeigte, dass sowohl die Pragmatische (*M* = 5.03, *SD* = 1.00) als auch die Hedonische Qualität (*M* = 4.63, *SD* = 1.06) des Lernmaterials gut bewertet wurden.

3.2 Interesse (H2)

Das Interesse an Blockchain lag über alle ProbandInnen hinweg vor (*M* = 3.94, *SD* = 1.26, *Mdn* = 4.00) und nach (*M* = 3.71, *SD* = 1.49, *Mdn* = 3.67) der Präsentation des Lernmaterials im mittleren Bereich. Das Interesse sank im Mittel etwas, dieser Unterschied war statistisch jedoch nicht bedeutsam (Wilcoxon-Test: z = -1.06, p = .291, r = .13, n = 63). Der Manipulationscheck ergab, dass sich das Interesse nach der Präsentation des Lernmaterials nicht zwischen den beiden Experimentalgruppen unterschied (neutral: *M* = 3.74, *SD* = 1.44, *Mdn* = 3.67, *n* = 35; interessant: *M* = 3.77, *SD* = 1.60, *Mdn* = 3.83, *n* = 28). Es ist jedoch eine Tendenz erkennbar, dass das subjektive Interesse am Thema Blockchain in der interessant formulierten Bedingung stabil blieb, sich in der neutral formulierten Bedingung hingegen etwas verschlechterte (Bild 5). Dieser Unterschied war statistisch jedoch nicht bedeutsam (Vergleich neutral prä vs. post: Wilcoxon-Test: z = -1.34, p = .180, r = .23, n = 35). Die Manipulation des Interesses kann daher nicht als erfolgreich betrachtet werden.

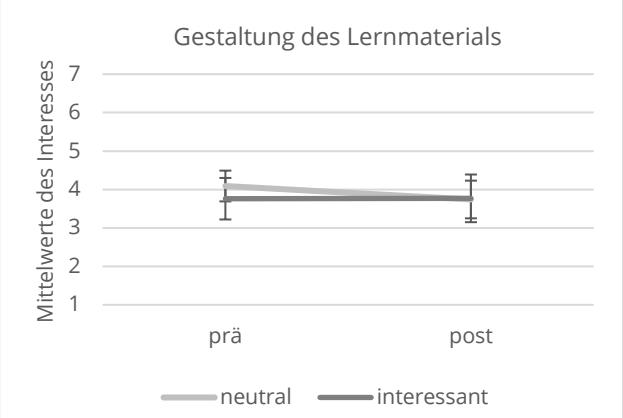

Bild 5: Manipulationscheck: Vergleich des Interesses prä vs. post nach Versuchsbedingung; dargestellt sind Gruppenmittelwerte und 95%-Konfidenzintervalle

Eine Überprüfung der Hypothese 2 war dennoch möglich. Dazu wurde der Zusammenhang des Interesses (post) mit dem subjektiven (H2a) und objektiven Verständnis (H2b) sowie der Nutzungsintention untersucht. Zur deskriptiven Darstellung (Bild 6) erfolgte zunächst eine Einteilung der ProbandInnen anhand des Skalenmittelwertes in die Gruppen hohes Interesse (*M* > 3, *n* = 43) und niedriges Interesse (*n* = 24).

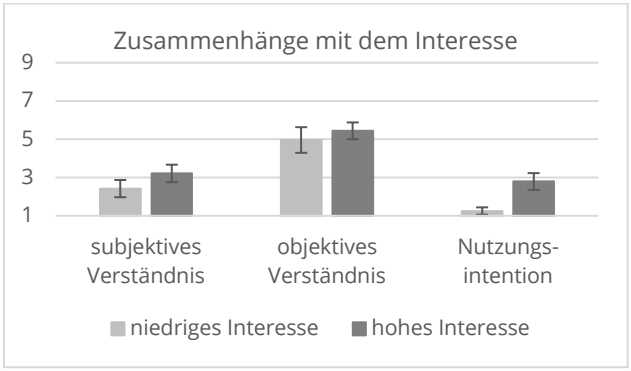

Bild 6: Zusammenhang des Interesses (post) mit den abhängigen Variablen; dargestellt sind Gruppenmittelwerte und 95%-Konfidenzintervalle

Im Anschluss wurde statistisch geprüft, ob ein Zusammenhang zwischen dem Interesse an der Blockchain-Technologie (post) und den abhängigen Variablen bestand. Wie Bild 6 bereits vermuten lässt, bestand ein großer und signifikanter Zusammenhang zwischen dem Interesse und der Nutzungsintention (H2c; Tabelle 1): Probanden mit einem hohen Interesse wiesen eine höhere Nutzungsintention auf als Probanden mit einem niedrigen Interesse.

Ein mittlerer positiver Zusammenhang konnte zudem zwischen dem Interesse und subjektivem Verständnis identifiziert werden (H2a). Es bestand hingegen kein signifikanter Zusammenhang zwischen dem Interesse an Blockchain und dem objektiven Verständnis (H2b).

Tabelle 1: Korrelationsmatrix Interesse (*n* = 67)

		Interesse post
Abhängige Variablen	Subjektiv. Verständnis	r_s = .27, p = .029
	Objektives Verständnis	r_s = .15, p = .233
	Nutzungsintention	r_s = .60, p < .001

3.3 Bildungsstand (H3)

Um die dritte Hypothese zu überprüfen, wurde analysiert, ob der Bildungsstand einen Einfluss auf das subjektive Verständnis (H3a), das objektive Verständnis (H3b) und die Nutzungsintention (H3c) hat. Da nur eine Person angab, einen Hauptschulabschluss zu haben, bezieht sich die folgende Analyse nur auf die Abschlüsse Mittlere Reife, (Fach-) Abitur und (Fach-) Hochschulabschluss (Bild 7).

Zunächst wurde mit allen drei abhängigen Variablen ein Kruskal-Wallis-Test durchgeführt, um zu überprüfen, ob es Unterschiede zwischen den Bildungsabschlüssen gab. Die Nutzungsintention unterschied sich nicht signifikant zwischen den drei Bildungsabschlüssen ($\chi^2(2)$ = 0.30, p = .860, n = 66). Da für das subjektive Verständnis

($\chi^2(2) = 17.79$, $p < .001$, $n = 65$) und das objektive Verständnis ($\chi^2(2) = 17.10$, $p < .001$, $n = 66$) signifikante Unterschiede bestanden, wurden Post-hoc-Tests durchgeführt, um zu untersuchen, welche Gruppen sich unterschieden.

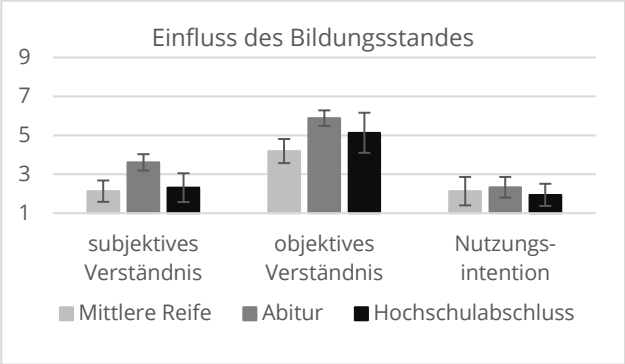

Bild 7: Einfluss Bildungsstand auf die abhängigen Variablen; dargestellt sind Gruppenmittelwerte und 95%-Konfidenzintervalle; bei Abitur bzw. Hochschulabschluss sind ProbandInnen mit Fachabitur bzw. Fachhochschulabschluss inbegriffen.

Das subjektive Verständnis war beim (Fach-) Abitur signifikant höher als bei der mittleren Reife ($U = 95.50$, $p < .001$, $r = .53$, $n = 49$) und dem (Fach-) Hochschulabschluss ($U = 119.00$, $p = .002$, $r = .45$, $n = 49$). Es gab keinen Unterschied zwischen dem subjektiven Verständnis bei der Mittleren Reife und dem (Fach-) Hochschulabschluss ($U = 124.50$, $p = .890$, $r = 0.02$, $n = 32$).

Beim objektiven Verständnis erreichten Personen mit einer Mittleren Reife einen signifikant geringeren Punktwert als Personen mit (Fach-)Abitur ($U = 71.50$, $p < .001$, $r = .60$, $n = 49$) oder (Fach-) Hochschulabschluss ($U = 75.50$, $p = .041$, $r = 0.36$, $n = 32$). Das objektive Verständnis zwischen (Fach-) Abitur und (Fach-) Hochschulabschluss unterschied sich nicht ($U = 206.00$, $p = .198$, $r = 0.18$, $n = 49$).

3.4 Alter (H4)

Bei der vierten Hypothese wurden mögliche Effekte des Alters auf das subjektive (H4a) und objektive (H4b) Verständnis und die Nutzungsintention (H4c) überprüft. Da das Alter nicht normalverteilt war, wurden zunächst Spearman-Korrelationen durchgeführt (Tabelle 2). Demnach zeigte sich für den subjektiven als auch den objektiven Lernerfolg ein mittlerer negativer Zusammenhang, der anzeigt, dass jüngere ProbandInnen größere Lernerfolge aufwiesen. Für die Nutzungsintention konnte kein statistisch bedeutsamer Zusammenhang mit dem Alter nachgewiesen werden.

Tabelle 2: Korrelationsmatrix Alter ($n = 65$)

		Alter
Abhängige Variablen	Subjektiv. Verständnis	$r_s = -.44$, $p < .001$
	Objektives Verständnis	$r_s = -.41$, $p = .001$
	Nutzungsintention	$r_s = -.12$, $p = .349$

Auch die Einteilung der Variable Alter nach der Theorie der Digital Natives (ab 1980 geboren) und der Digital Immigrants (vor 1980 geboren) [10, 11] untermauerte diese Ergebnisse (Bild 8).

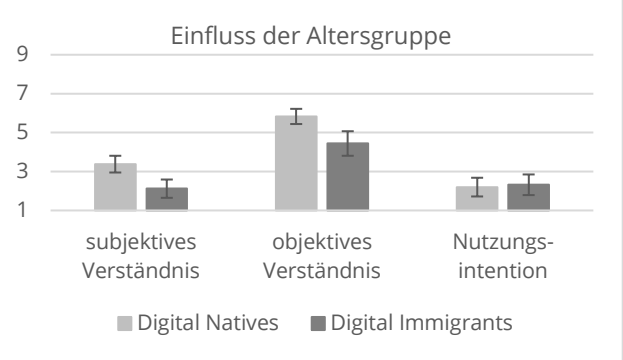

Bild 8: Einfluss der Altersgruppe auf die abhängigen Variablen; dargestellt sind Gruppenmittelwerte und 95%-Konfidenzintervalle.

Das subjektive Verständnis (Digital Natives: $Mdn = 4.00$, $n = 40$; Digital Immigrants; $Mdn = 2.00$, $n = 25$; $U = 242.50$, $p < .001$) und das objektive Verständnis (Digital Natives: $Mdn = 6.00$; Digital Immigrants $Mdn = 5.00$; $U = 226.50$, $p < .001$) waren bei Digital Natives signifikant höher als bei Digital Immigrants. Die Nutzungsintension unterschied sich nicht zwischen den Gruppen (Digital Natives: $Mdn = 2.00$; Digital Immigrants; $Mdn = 2.00$; $U = 439.50$, $p < .393$).

3.5 Geschlecht (H5)

Im Rahmen von Hypothese 5 wurde überprüft, ob das Geschlecht (männlich: $n = 17$, weiblich $n = 50$) einen Einfluss auf das subjektive Verständnis (H5a), das objektive Verständnis (H5b) oder die Nutzungsintention (H5c) hatte (Bild 9).

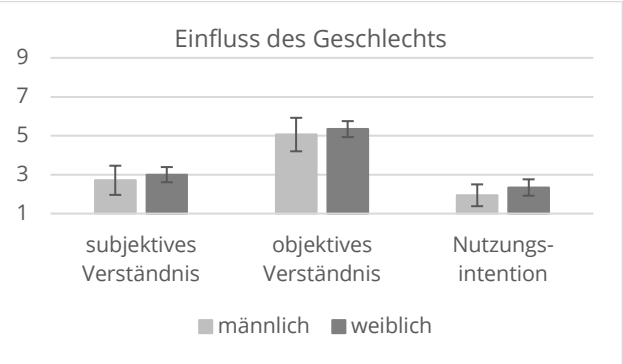

Bild 9: Einfluss des Geschlechts auf die abhängigen Variablen; dargestellt sind Gruppenmittelwerte und 95%-Konfidenzintervalle.

Weder für das subjektive Verständnis (männlich: $Mdn = 3.00$; weiblich: $Mdn = 3.00$; Mann-Whitney-U-Test: $U = 366.50$, $p = .389$, $r = .11$) noch für das objektive Verständnis (männlich: $Mdn = 5.00$; weiblich: $Mdn = 6.00$; $U = 387.00$, $p = .574$, $r = .07$) oder die Nutzungsintention (männlich: $Mdn = 2.00$; weiblich: $Mdn = 2.00$; $U = 370.00$, $p = .407$, $r = .01$) konnte ein statistisch bedeutsamer Unterschied gefunden werden. Zusammenfassend hatte

das Geschlecht in der vorliegenden Studie keinen Einfluss auf das Verständnis oder die Nutzungsintention der Blockchain.

3.6 Zusammenhang Verständnis und Nutzungsintention (H6)

In Hypothese 6 wurde angenommen, dass das Verständnis und die Nutzungsintention von Blockchain einen großen Zusammenhang zeigen. Um dies zu überprüfen, wurden die abhängigen Variablen korreliert. Wie Tabelle 3 zeigt, ist ein höheres subjektives Verständnis mit einer höheren Nutzungsintention verbunden (mittlerer, positiver Korrelationseffekt). Für das objektive Verständnis und die Nutzungsintention konnte hingegen kein Zusammenhang festgestellt werden. Dies bedeutet, dass die Nutzungsintention mit dem subjektiven Verständnis in Verbindung steht, nicht aber mit dem objektiven Verständnis.

Bei der Korrelation des subjektiven und objektiven Verständnisses konnte zudem ein positiver und großer Zusammenhang festgestellt werden. Das heißt, dass Personen (unbeachtet anderer Einflussfaktoren) ihr Verständnis subjektiv höher einschätzten, wenn ihr Wissen objektiv höher war.

Tabelle 3: Korrelation abhängige Variablen (n = 67)

	Objektives Verständnis	Nutzungsintention
Subjektives Verständnis	r_s = .48, p < .001	r_s = .28, p = .023
Objektives Verständnis		r_s = .04, p = .762

4. Diskussion

Insgesamt waren die Blockchain-Novizen der Studie gut dazu in der Lage, etwas über Blockchain zu lernen, da ihr subjektives Verständnis am Thema Blockchain signifikant stieg und sich dies auch in der hohen Quote der richtig beantworteten Wissensfragen widerspiegelte. Das erstellte Lernmaterial kann damit als gut geeignet betrachtet werden, um Blockchain-Novizen etwas über Blockchain beizubringen, was die positive Einschätzung der User Experience untermauert. Bezogen auf die Cognitive Load Theory bedeutet dies, dass die mentale Belastung der ProbandInnen durch das Lernmaterial angemessen war.

Die experimentelle Manipulation des Interesses in eine neutrale und eine interessante Bedingung war nicht erfolgreich. Möglicherweise war die Variation über die Formulierung der Lerntexte zu gering, um ein unterschiedliches Interesse am Thema Blockchain zu erzeugen. Dennoch konnten die Teilhypothesen zur Rolle des Interesses über das subjektiv eingeschätzte Interesse (post) korrelativ untersucht werden. Zunächst zeigte die deskriptive Analyse, dass das Interesse durchschnittlich im mittleren Bereich lag, was für ein neues und komplexes Thema als gut zu bewerten ist. Die Korrelationsberechnungen offenbarten, dass ein höheres Interesse (post) mit einer subjektiv höheren Lernleistung und mit einer höheren Nutzungsintention, nicht jedoch mit einem höheren objektiven Verständnis verbunden war. Für die Korrelation zwischen Interesse und Nutzungsintention (r_s = .60) kann jedoch keine Kausalaussage getroffen werden. Das heißt, es ist unklar, ob ein höheres Interesse zu einer höheren Nutzungsintention führt oder umgekehrt. Darüber hinaus wäre auch der Einfluss weiterer Variablen denkbar, die sowohl das Interesse als auch die Nutzungsintention beeinflussen.

Zudem sollte der fehlende Zusammenhang zwischen dem Interesse und dem objektiven Verständnis hervorgehoben werden. Das Interesse allein reicht demnach nicht aus, um einen hohen objektiven Lernerfolg zu erzielen. In Bezug auf die Cognitive Load Theory bedeutet dies, dass das Interesse am Thema keinen Einfluss auf die mentale Belastung hatte, die beim Lernprozess entstand. Wie die Analysen zeigten, geht ein hoher Lernerfolg vielmehr mit einem höheren Bildungsstand und einem niedrigeren Alter einher. Das objektive Verständnis scheint daher stark von den bestehenden Wissensstrukturen einer Person und der Möglichkeit, an diese anzuknüpfen, abzuhängen. Ein hohes Interesse am Thema reicht demnach nicht aus, um fehlende nützliche Wissensstrukturen (Schemata) zu kompensieren.

Der Bildungsstand einer Person spielte eine wichtige Rolle dabei, wie einfach eine Person etwas über Blockchain lernen konnte. Dabei muss jedoch kritisch betrachtet werden, dass an der Studie vor allem Personen mit höheren Bildungsabschlüssen teilnahmen und über Personen mit einem niedrigeren Bildungsstand keine Aussagen getroffen werden können. Für die zukünftige Betrachtung des Bildungsstandes wäre demnach die Untersuchung einer breiteren Stichprobe interessant. Zukünftig könnte zudem evaluiert werden, welches Wissensstrukturen bzw. welches Vorwissen besonders hilfreich ist, um Informationen über Blockchain leicht zu lernen. Dabei wäre es möglich, das allgemeine (technische) Vorwissen, aber auch verschiedene Abstufungen des Vorwissens über Blockchain, näher zu betrachten.

Auch das Alter erwies sich als zentrale Einflussgröße für das subjektive und objektive Verständnis. Gemäß der Theorie der Digital Natives und der Digital Immigrants [10, 11] fiel es älteren ProbandInnen objektiv schwerer, Inhalte über Blockchain zu erlernen, was mit ihrer subjektiven Einschätzung übereinstimmte. Auch dieses Ergebnis könnte durch eine geringere Möglichkeit erklärt werden, an bestehende Wissensstrukturen (Schemata) anzuknüpfen. Damit stellte das Lernmaterial für weniger gebildete oder ältere Personen im Mittel eine größere mentale Belastung im Sinne des Intrinsic Loads dar. Dies führte laut der Cognitive Load Theory [7, 8] dazu, dass die Ressourcen für den Germane Load, den Verstehensprozess, geringer waren, um Inhalte über Blockchain zu verarbeiten.

Die Ergebnisse zum Alter und zum Bildungsstand sind mit anderen Studienergebnissen zur Digitalisierung vergleichbar. So fast eine Überblicksarbeit zusammen, dass ältere Menschen insgesamt weniger von neuen Technologien profitieren und ein altersbezogener Digital Divide besteht [16]. Eine digitale Spaltung kann auch aufgrund von Bildungsunterschieden entstehen. Diese Spaltungen können jedoch reduziert werden, wenn Personen bestimmte Technologien selbst anwenden, wie beispielsweise eine Studie zur Nutzung von Smartphones zeigte [17]. Zusammengefasst weisen Personen mit einem geringeren Bildungsstand oder einem höheren Alter einen höheren oder möglicherweise anderen Informationsbedarf auf. Es sollten daher leicht zugängliche und verständliche Möglichkeiten geschaffen werden, damit diese Personen neue Technologien wie Blockchain besser verstehen und selbst anwenden, um dem Digital Divide entgegenzuwirken. Die zukünftige Forschung und Entwicklung zum Thema Blockchain sollte diese beiden Personengruppen besonders beachten, damit diese von den Potentialen der Blockchain oder der Digitalisierung im Allgemeinen profitieren können und sich nicht davon „abgehängt" fühlen.

Für das Geschlecht zeigten sich hingegen keine Unterschiede in den abhängigen Variablen, was so jedoch nur für das objektive Verständnis erwartet worden war. Für das subjektiv eingeschätzte Verständnis und die Nutzungsintention war ein Unterschied angenommen worden. Offensichtlich waren die Probandinnen gut dazu in der Lage, ihr eigenes Wissen einzuschätzen und wurden nicht durch Geschlechtsstereotype in ihren Einschätzungen beeinflusst. Die Studie zeigt damit, dass Frauen in einem ähnlichen Maße von Blockchain und der Digitalisierung profitieren könnten wie Männer. Dass dies jedoch noch nicht der Fall ist, zeigt der dritte Digitalisierungsbericht des BMFSFJ [18]. Demnach sind derzeit nur 16% der Beschäftigten im Digitalisierungsbereich weiblich und es sollten zukünftig mehr Maßnahmen ergriffen werden, damit Frauen stärker von der Digitalisierung profitieren und diese mitgestalten können.

Im Rahmen der Studie wurde zudem die Frage aufgeworfen, ob ein geringeres Verständnis der Blockchain-Technologie mit einer geringeren Nutzungsintention verbunden ist. Die korrelativen Analysen offenbarten einen kleinen Zusammenhang zwischen dem subjektiven Verständnis und der Nutzungsintention, jedoch keinen Zusammenhang zwischen dem objektiven Verständnis und der Nutzungsintention. Dasselbe Muster spiegelte sich auch in den Ergebnissen zum Interesse wider. Offenbar sind die Nutzungsintention und das subjektive Verständnis miteinander verknüpft, nicht jedoch das objektiv richtige Verständnis und die Nutzungsintention. Dies bedeutet möglicherweise, dass ein subjektives Modell von der Funktionsweise und den Vorteilen der Blockchain ausreicht, um die Nutzungsintention zu erhöhen und vom Potential der Blockchain zu profitieren. Die eigentliche Nutzungsbarriere [1] besteht demnach nicht beim Fehlen eines objektiv richtigen Verständnisses der Technologie, sondern im subjektiven Eindruck, Blockchain nicht zu verstehen.

5. Zusammenfassung

Ausgangspunkt der Studie war, dass eine der größten Nutzungsbarrieren von Blockchain das mangelnde Verständnis und damit die mangelnde Wahrnehmung des Potentials in der Allgemeinbevölkerung ist. Aufgrund der vorliegenden Studienlage wurden drei Forschungsfragen aufgeworfen: Erstens, ob es möglich ist, Blockchain-Novizen die Technologie einfach zu erklären. Dies kann aufgrund der insgesamt recht hohen Quote an richtig beantworteten Wissensfragen angenommen werden. Zweitens, wurde untersucht, ob es Personengruppen gibt, die einen anderen oder höheren Informationsbedarf haben, um Blockchain zu verstehen. Auch dies kann angenommen werden. Älteren Personen und Personen mit einem niedrigeren Bildungsstand fiel es schwerer etwas über Blockchain zu lernen. Drittens wurde die Frage aufgeworfen, ob die Nutzungsintention mit dem Verständnis für Blockchain verbunden ist. Dies war in der Studie nur teilweise der Fall. Die Ergebnisse deuten darauf hin, dass ein objektiv richtiges Verständnis der Technologie für deren Anwendung nicht notwendig ist, aber ein subjektives mentales Modell der Blockchain und ihres Potentials von Vorteil ist, um eine höhere Nutzungsintention zu erzielen. Die zukünftige Forschung in diesem Bereich sollte sich daher darauf fokussieren, wie die Nutzungsintention und das Interesse genau erhöht werden könnten, damit möglichst viele Personen vom Potential der Technologie profitieren.

Auch wenn die demographischen Eigenschaften keinen Einfluss auf die Nutzungsintention gezeigt haben, sollte den vulnerablen Altersgruppen (Ältere und Personen mit geringerem Bildungstand) eine erhöhte Aufmerksamkeit bei der Forschung und Entwicklung von Blockchain und der Digitalisierung im Allgemeinen geschenkt werden. Eine Vernachlässigung würde möglicherweise dazu führen, dass sich diese Personengruppen durch die fortschreitende Digitalisierung „abgehängt" fühlen und der „Digital Divide" verstärkt wird.

Danksagung

Wir bedanken uns bei Julia Claus, Lilli Geisler, und Bianca Trobisch für ihre Unterstützung im Rahmen der Studie.

Literaturverzeichnis

[1] V. Sadhya, H. Sadhya, Barriers to Adoption of Blockchain Technology, AMCIS 2018 Proceedings, (2018).

[2] F. Casino, T. K. Dasaklis, C. Patsakis, A systemeatic review of Blockchain-based applications: Current status, classification and open issues, Telematics and Informatics, 36 (2019), 55-81.

[3] Y. Yuan, F. E. Wang, Blockchain and Cryptocurrencies: Model, Techniques, and Applications, IEEE Transactions on Systems, Man, and Cybernetics: Systems (2018) Vol. 48, 1421-1428.

[4] R. C. Atkinson, R. M. Shiffrin, Human Memory: A

Proposed System and its Control Process, Psychology of Learning and Motivation (1968), Vol. 2, 89-195.
[5] R. C. Anderson, P. D. Pearson, A schema-theoretic view of basic processes in reading comprehension, In P. D. Person, Handbook of reading research (1984), 255-291.
[6] J. Sweller, Cognitive load during problem solving: effects on learning. Cognitive Science (1988), Vol. 12, 257–285.
[7] J. Sweller, J. J. G. van Merriënboer, F. G. W. C. Paas, Cognitive architecture and instructional design. Educational Psychology Review, (1998), Vol. 10, 251-296.
[8] L. L. Shirey, R. E. Reynolds, Effect of interest on attention and learning. Journal of Educational Psychology, (1988), Vol. 80, 159-166.
[9] U. Schiefele, K. P. Wild, Aufmerksamkeit als Mediator des Einflusses von Interesse auf die Lernleistung, Sprache und Kognition, (1994), Vol. 13, 138-145.
[10] M. Prensky, Digital Natives, Digital Immigrants, On the Horizon, (2001), Vol, 9, 1-6.
[11] John Palfrey, Urs Gasser: Born Digital: Understanding the First Generation of Digital Natives, Basic Books, (2008).
[12] I. J. Deary, Intelligence, Annual Review of Psychology, (2012) Vol. 63, 453-482.
[13] E. Hargittai, S. Shafer, Differences in Actual and Perceived Online Skills: The Role of Gender. Social Science Quarterly (2006), 432-448.
[14] R. E. Anderson, Females Surpass Males in Computer Problem Solving: Findings from the Minnesota Computer Literacy Assessment, Journal of Educational Computing Research (1987), Vol. 3, 39–51.
[15] M. Schrepp, A. Hinderks, J. Thomaschewski, Design and Evaluation of a Short Version of the User Experience Questionnaire (UEQ-S), International Journal of Interactive Multimedia and Artificial Intelligence, (2017) Vol. 4, 103-108.
[16] A. Wanka, V. Gallistl, Ältere Menschen und Digitalisierung aus der Sicht der kritischen Gerontologie, Expertise zum Achten Altersbericht der Bundesregierung, (2020).
[17] W. Sung, A study of the digital divide in the current phase of the information age: The moderating effect of smartphones, Information Polity, (2016) Vol. 21, 291-306.
[18] BMFSFJ, Digitalisierung geschlechtergerecht gestalten, https://www.bmfsfj.de/bmfsfj/ministerium/berichte-der-bundesregierung/dritter-gleichstellungsbericht, (2021).

ISSN 1437-7624