WHITE PAPER

BLOCKCHAIN IN SMEs

Publisher:
eco – Association of the Internet Industry

eco
ASSOCIATION OF THE
INTERNET INDUSTRY

Blockchain in SMEs

Contents

Figures 1-5 in the following paper are taken from the article "Blockchain-Technologie unter der Lupe" by Prof. Dr. Norbert Pohlmann. Appeared in IT-Sicherheit, 05/2018, p. 58 ff., at https://norbert-pohlmann.com/app/uploads/2018/10/388-Blockchain-Technologie-unter-der-Lupe-–-Sicherheit-und-Vertrauenswürdigkeit-kryptografisch-verkettete-Datenblöcke-Prof.-Norbert-Pohlmann.pdf

1. Introduction

Blockchain has made the leap into the public arena: Daily newspapers, business magazines, news portals and blogs are reporting almost daily about the new technology, which is the foundation for the crypto currency *Bitcoin*. And it's not only IT companies that are exploring blockchain. Insurance firms, logistics companies, banks, stock exchanges, and companies from numerous other sectors are working on scenarios for possible applications.[1] What initially looked like a hype is now becoming established as a trend with a highly promising future. As a quintessential cross-sectoral technology, blockchain has the potential to revolutionize entire value chains – because it enables the transaction of values in digital space without the need of an intermediary, and it represents a new, efficient method for the verification of data and data transfers in multi-stakeholder systems.

While – with the exception of the *Bitcoin* blockchain – past years have been characterized by theoretical concepts and Proofs of Concept, we are now seeing more engineers than visionaries, and they are subjecting blockchain technology to a reality check. The question of IT security has been an important element of this. After all, many of the possible applications are proceeding in very sensitive areas such as finance, insurance, and medicine. One advantage of blockchain: The technology offers "Security by Design" – as a result of its fundamental conception, blockchain is very difficult to compromise. Nonetheless, as is always the case for IT systems, several challenges remain.

An adaptation of the technology for small and medium-sized enterprises (SMEs) requires above all trust[2] in the security and reliability of the technology: Before the technology is likely to be used, it needs not only to be secure, but also resource-efficient and user-friendly. Interoperability with other systems is also of importance.

[1] For application scenarios see World Economic Forum, The future of financial infrastructure – An ambitious look at how blockchain can reshape financial services, 2016, at: http://www3.weforum.org/docs/WEF_The_future_of_financial_infrastructure.pdf; the German-language Blockchain Bundesverband, Statement on Token Regulation with a Focus on Token Sales, 10.02.2018, at https://bundesblock.de/wp-content/uploads/2019/01/180209_Statement-Token-Regulation_blockchain-bundesverband.pdf; the German-language BDEW, Blockchain in der Energiewirtschaft, 2017, at https://www.bdew.de/media/documents/BDEW_Blockchain_Energiewirtschaft_10_2017.pdf

[2] In detail, Werbach, The Blockchain and the New Architecture of Trust, 2018; Werbach, 33 Berkeley Tech. L.J. (2018), 487.

This paper by the Competence Groups Blockchain and Security in eco – Association of the Internet Industry provides an overview of the most important questions that SMEs should answer before initiating their own blockchain projects.

2. What is Blockchain?

Blockchain is a communication protocol in which transactions that have been carried out can be saved in a transparent manner in distributed databases. The protocol itself makes a range of functions available to ensure that the communication can be undertaken securely, transparently, and pseudonymously. To achieve this, all transactions and information are simultaneously saved in many different locations. The integrity of the data is guaranteed through the saving of the hash value of the respective previous data set.[3]

The essential characteristics of blockchain technology are the following:

- the decentralized data structure,
- the redundant distribution of the data in the network,
- the tamper-proof storage of the data in the network,
- and the transparency of the data stored.

In the meantime, there have been multiple enhancements made (for example, Lightning and Raiden)[4] and extensions of the original *Bitcoin* blockchain, such as what are known as "Smart Contracts",[5] which enable automated processing of application processes. Smart Contracts in particular open up

[3] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, S. 2, at https://bitcoin.org/bitcoin.pdf.
[4] Lightning unburdens a blockchain network and improves scalability. Using a separate payment channel, two nodes can carry out transactions between themselves free of charge, using a 2-2 multi-signature wallet. The channel is opened by an initial funding transaction. The nodes can then carry out any number of transactions with each other without having to store them in the blockchain. The claims are only netted and written back into the blockchain as soon as one of the two participants closes the channel by publishing a settlement transaction containing the final balance of both parties derived from the last commitment transaction. Raiden was developed for the Ethereum blockchain and is based on the same principle.
[5] The concept of Smart Contracts goes back to Szabo, The Idea of Smart Contracts, 1997, at: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html.

the potential for a multitude of applications over and above the original scope of crypto currencies.[6]

The core of a blockchain is a transaction register distributed over all nodes of the network (Distributed Ledger). All transaction data is shared between the participants in a Peer-to-Peer network.[7] As a rule, all participants in this network have the same rights and the same information, and as a result the same prerequisites to participate in the system and to add new information or transactions. To achieve this, every node saves the entire data set. If a node were to be hacked or a value changed, this deviation would be discerned by the entire system. The total redundancy of the database therefore protects the system against one-sided exercise of power, outage, and manipulation.[8]

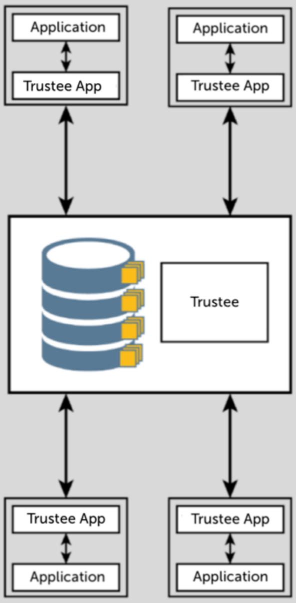

Fig. 1: Traditional centralized architecture

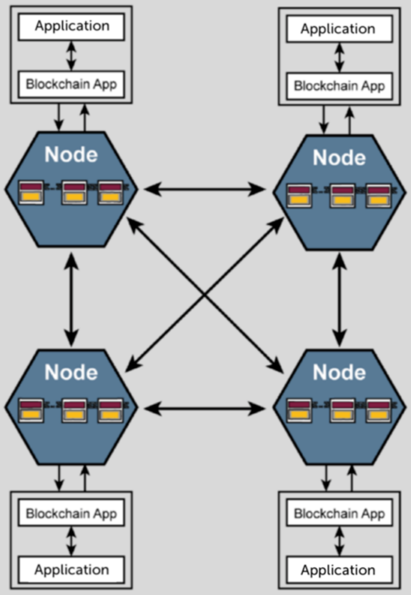

Fig. 2: Decentralized blockchain architecture

[6] Examples of this include structures for decision-making (http://boardroom.to/#About) and mechanisms for dispute resolution (https://www.bitrated.com/) on a blockchain basis; in-depth information on the latter application: Ortolani, Self-Enforcing Online Dispute Resolution: Lessons from Bitcoin, 36 Oxford J. Legal Studies (2016), 595–629; Kolain, Die Blockchain als „vollkommenes Gesetzbuch"?, Rechtshistorische Überlegungen zur Konfliktlösung in Smart Contracts, in: Hill/Martini/Kugelmann, Perspektiven der digitalen Lebenswelt, 2017, S. 147 – 162.

[7] De Filippi, Journal of Peer Production 2015, Issue 9, at: http://peerproduction.net/issues/issue-9-alternative-internets/peer-reviewed-papers/the-interplay-between-decentralization-and-privacy-the-case-of-blockchain-technologies.

[8] For the functionalities see also Bechtolf/Vogt, ZD 2018, 66, 67; Martini/Weinzierl, NVwZ 2017, 1251; Heckelmann, NJW 2018, 504, 505; Hofert, ZD 2017, 161, 162 f.

If a given number of transactions has been exceeded, a new block will be calculated. A consensus mechanism is used to achieve this. The consensus mechanism is the fundamental component to protect the blockchain against manipulation. It solves the "Double-Spending Problem"[9] in that it prevents a participant from transferring a value several times – for example, sending a *Bitcoin* to participant A, and then sending the same one again to participant B. Only when the majority of the nodes connected to the Peer-to-Peer network agree about the creation of a new block will this be validated and added to the previously generated blocks.

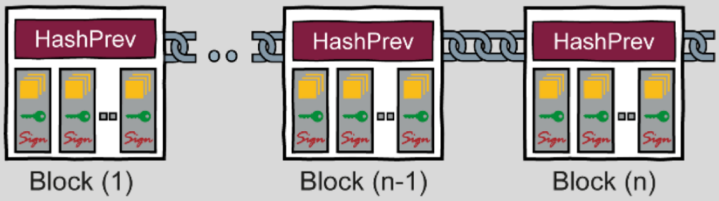

Fig. 3: Data structure of a blockchain

In order to reach an agreement, proposals for new blocks are first drawn up. This is done by validators (called "miners" in the *Bitcoin* blockchain). The participants must then agree on which proposed block will actually be inserted into the chain. The validation of the transactions and information takes place, for example, in a computationally intensive procedure using "Proof of Work", before they are written into the blockchain database. Proof of Work is a procedure in which the miners are required to solve a calculation task, the solution of which can be easily verified by all participants in the network.[10]

Further information on the functioning of blockchain and the commonly used terms can be found at: https://international.eco.de/topics/blockchain/

[9] Already seen in Chaum, 8 Sci. Am. (1992), 96–101.

[10] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008 (Fn. 9), S. 2 with regard to the Proof of Work mechanism; in-depth information on other verification mechanisms EZB, Virtual currency schemes – a further analysis, 2015, p. 10, at https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf.

2.1. Different Types of Blockchain

As a rule, blockchains are categorized into one of three different types: public, private, und federated blockchains.[11] However, this classification is not completely clear-cut: there are also hybrid forms such as public-permissioned and private-permissioned blockchains.

A. Public Blockchain

In public blockchains, anyone can be involved in the network. Participation is not subject to any form of control and anyone can participate in reading, writing, and verifying the data. This makes public blockchains open and transparent, because any participant within the network can check any record at any given time.[12] The decision-making and the verification of transactions takes place via a range of consensus mechanisms, such as the Proof of Work and the Proof of Stake.[13] *Bitcoin* and *Ethereum* are examples of public blockchains.

B. Private Blockchain

A private blockchain – often also called a permissioned blockchain – is only available to a specific group of users, e.g. within a company. In contrast to a public blockchain, here there are one or several persons responsible, who take care of the operation of the blockchain and access to it.[14] As a rule, there is also a graded system of rights. This defines which user is allowed to execute what actions and is granted access to which data. All imaginable consensus mechanisms are possible; instead of the energy and computationally intensive Proof of Work, less costly procedures (Proof of Stake, Delegated

[11] More information in Schwintowski/Klausmann/Kadgien, NJOZ 2018, 1401, 1403; Schrey/Thalhofer, NJW 2017, 1431, 1433.
[12] Schrey/Thalhofer, NJW 2017, 1431, 1433; Hofert, ZD 2017, 162, 162 et seq.
[13] ECB, Virtual currency schemes – a further analysis, 2015 (Fn. 9), p. 10.
[14] Evans, Economic Aspects of Bitcoin and Other Decentralized Public-Ledger Currency Platforms, The University of Chicago Law School, Coase-Sandor Institute for Law and Economics Working Paper No. 685, p. 16, at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2424516.

Proof of Stake, Hashgraph, Proof of Authority etc.)[15] can be used, but at the same time these entail a reduction in security. The private blockchain is strictly speaking no longer a blockchain in the narrow sense of the term, because it lacks the central characteristic of decentralized data storage. The data is nonetheless secured cryptographically. Examples of private blockchains are *Ripple*[16] and *Hyperledger*.[17] Since *Ethereum* is open source software, the code can also be used without modification to build a private blockchain. Private blockchains lend themselves to implementation in companies, as here it is generally important that the data is not freely accessible for everyone.

C. Federated Blockchain

The federated blockchain is an extension of the private blockchain. In this case, there is more than one body responsible for the network. Generally, a group of companies or organizations work together and make joint decisions for the benefit of the whole network. Consensus is often achieved through a majority decision; with regard to the governance, there is considerable flexibility in the design. Given that the security of the system often does not play as great a role as in public blockchains, many consensus mechanisms can be used that enable the fast and scalable processing of transactions. Examples of federated blockchains include *R3*,[18] the *Energy Web Foundation*,[19] *B3i*,[20] *Enerchain*,[21] and the collaborative project of German energy suppliers, *ETH@Energy*.[22] [23]

[15] An overview of the standard consensus mechanisms and their fields of application can be found (in the German language) at https://www.bitfantastic.com/uebersicht-ueber-blockchain-konsensus-algorithmen/#Der-grosse-Nachteil.
[16] See https://ripple.com
[17] See https://www.hyperledger.org
[18] See https://www.r3.com
[19] See https://energyweb.org
[20] See https://b3i.tech
[21] See https://enerchain.ponton.de
[22] See https://www.eth-energy.de
[23] Further information in Werbach, 33 Berkeley Tech. L.J. (2018), 487, 490, 498 et seq., 536.

D. Alternative Systems – Example of IOTA

IOTA (named after the smallest letter in the Greek alphabet) is also a system for performing digital transactions. Although *IOTA* is often mentioned in the context of blockchain, the system does not use blockchain based on chained blocks. At *IOTA*, transactions are recorded in a "Directed Acyclic Graph" (a "Tangle"). The intention is to keep transaction costs as low as possible and to ensure better scalability. The sender pays for its transaction in the *IOTA* network with corresponding computational power (Proof of Work). As such, *IOTA* is a distributed ledger without being a blockchain. The system is geared towards secure communication and payment between machines for IoT applications and is managed by the *IOTA* Foundation. The reference software is open source. The security of the system is based partly on a central body, the "coordinator".

2.2. Smart Contracts

Smart Contracts offer especially high potential for disruptive business models.[24]

Smart Contracts are programs that are executed on a blockchain. A Smart Contract is basically a set of rules for triggering transactions – a defined transaction (an "if" condition) can in turn trigger a transaction (a "then" sequence). A transaction can be both a transmission of data (e.g. external IoT sensor) or a transmission of crypto currency.

The encryption and distributed storage in the blockchain make the process tamper-proof and safe from manipulation. Smart Contracts are not intelligent. A Smart Contract does not further develop itself independently and cannot adapt its code to emerging conditions in the sense of an artificial intelligence.

What is new about the Smart Contract is that it can process transactions in digital space in an automated manner, without the need for an intermediary.

[24] Further information on the technical functionalities in Heckelmann, NJW 2018, 504; Kaulartz/Heckmann, CR 2016, 618; Jacobs/Lange-Hausstein, ITRB 2017.

Every transaction is publicly readable. And it is not possible to modify the history of such transactions. As soon as a Smart Contract has been executed, the execution cannot be reversed. This means that a Smart Contract is a program that is executed completely autonomously. This is ensured through the decentrality of the network. There is no controlling body that can intervene in the program execution – at least, not if the Smart Contract runs on a public blockchain such as *Ethereum*.

Thus, for example, contractual partners can define in advance that in the case of rain on a particular day in a specific location, a certain sum of money will be paid out – this would be an example application in the form of weather insurance for film production. The Smart Contract can receive the required weather data without human intervention – for example, from an Internet-capable weather station. The payment of the insured sum can occur using a blockchain-based crypto currency, such as *Bitcoin*. In this way, the processing of the contract can occur completely separately to any central body such as an insurance company – and without the need for a specialist to manually check whether the damages actually occurred. Once they are running, Smart Contracts can usually no longer be stopped by individuals – they are "obstinately" executed in line with pre-determined programming. This can lead to conflicts with mandatory legal requirements, which can potentially be offset by appropriate embedding into contractual structures.

The best-known blockchain for Smart Contracts is the *Ethereum* blockchain. This blockchain, with its integrated programming language, makes tools available in an open platform for developers to develop Smart Contracts independently and use them in a blockchain. The preparation of Smart Contracts has been a fixed component of the technology from the very beginning. Here, *Ethereum* differentiates itself most strongly from the *Bitcoin* blockchain. By now, however, there are also Smart Contract solutions for the *Bitcoin* blockchain,[25] as well as chain-neutral approaches.[26]

[25] See Ortolani, Self-Enforcing Online Dispute Resolution: Lessons from Bitcoin, 36 Oxford J. Legal Studies (2016), 595–629.

[26] Further information Kolain/Wirth, MultiChain-Governance, in: Taeger, Jürgen (Ed.), Recht 4.0, Innovationen aus den rechtswissenschaftlichen Laboren, 2017, S. 833 – 845.

2.3. Interfaces & Wallets

Every blockchain application requires a connection to the "real" world – somehow the transaction must be initiated, credit stored, and data transferred for the triggering of actions in the blockchain. The handling and management of units of value on blockchains takes place as a rule using what are known as "wallets" – software programs that manage the balance of crypto currencies and enable transferal of currency units to other participants. A wallet is not only necessary for users who want to transfer the sum X from A to B. The wallet is also used to pay the operating costs for a public blockchain that is being used for a project. This is necessary because, as a rule, every transaction that is processed on a public blockchain costs a certain fee – similar to a transaction fee – in the respective crypto currency. There are now a wide range of providers and trading platforms,[27] so that it is no longer necessary for a project to develop its own.

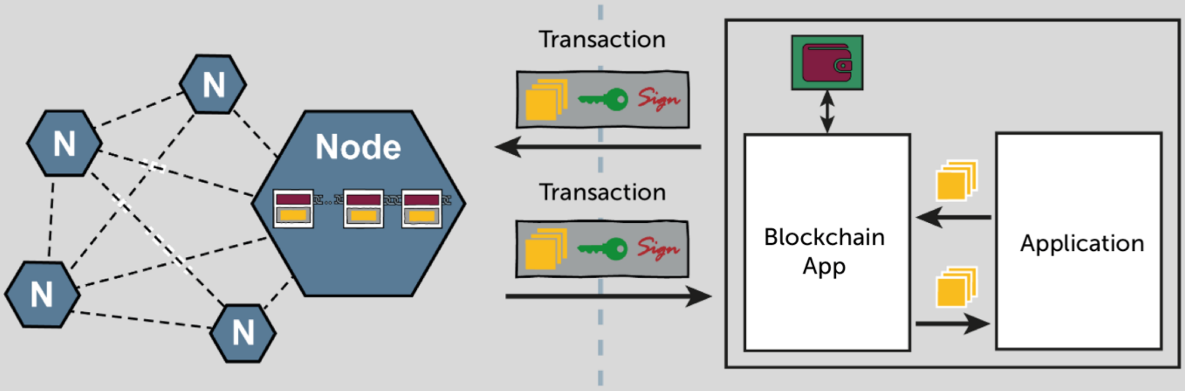

Fig. 4: Interfaces between blockchain infrastructure and blockchain application

A further interface to the outside is necessary if external data sources are to be connected that can trigger the actions of a Smart Contract. A range of initiatives for regularizing standards are currently underway, such as the German DIN SPEC 3103 "Smart Contracts und Sensoren in Blockchains für

[27] See https://www.btc-echo.de/tutorial/wallet-bitcoins-sicher-aufbewahren/

Industrie 4-0-Anwendungen"[28]. Standardization is also being driven forward internationally by the *ISO*; in 2016 a technical committee on "*Blockchain and Distributed Ledger Technologies*" was established, which is currently working on the development of eleven standards.[29]

It makes sense to orient oneself along the lines of one of the existing curricula for blockchain developers which are available online.[30]

Companies that do not themselves have sufficient in-house know-how for the application of the blockchain technology can make use of an external service provider; ideally, one who has already successfully implemented multiple blockchain projects.

2.4. The Limits of Blockchain Technology

Blockchain is no panacea. It can accelerate certain processes and make them more efficient, and it enables the implementation of processes and use-cases that have hitherto not been possible. But there are limits: The transparency of public blockchains can represent a problem in some scenarios. If sensitive or business-relevant data are to be distributed, doing this within a protected environment with a clearly defined and limited user group should be considered. In this case, a private or a federated blockchain may be suitable. There are also technical hurdles: The processing power of mini computers is often insufficient for the operation of a node, which is why miniaturization in particular in the area of IoT is currently setting limits. There are also constraints, especially in public blockchains, when it comes to the scalability, or the processing of a large number of transactions in a short period of time.[31] In addition to this, there are legal challenges, such as if the blockchain processes personal data.[32]

[28] See https://www.din.de/de/forschung-und-innovation/din-spec/alle-geschaeftsplaene/wdc-beuth:din21:287248829

[29] See https://www.iso.org/committee/6266604/x/catalogue/p/0/u/1/w/0/d/0

[30] Röder, Curriculum für Blockchain-Entwickler, 2018, Curriculum für Blockchain-Entwickler, Computerwoche 2018, available in the German language at https://www.computerwoche.de/a/curriculum-fuer-blockchain-entwickler,3545842.

[31] Hofert, Regulierung der Blockchains, 2018, S. 46 et seq.; Fairfield, 88 S. Cal. L. Rev. (2015), 805, 828 et seq.; Croman et al., On Scaling Decentralized Blockchains, A Position Paper, 2016, at http://fc16.ifca.ai/bitcoin/papers/CDE+16.pdf.

[32] For implications for data protection law, see Schrey/Thalhofer, NJW 2017, 1431; Hofert, ZD 2017, 161; Bechtolf/Vogt, ZD 2018, 66; Pesch/Böhme, DuD 2017, 93.

Whether a project really needs a blockchain should always be carefully examined. In many cases, the functions can also be implemented using conventional technical solutions.

3. Blockchain in SMEs – Prerequisites and Challenges

Automated transactions and value chains are of interest in particular to small and medium-sized enterprises. They open up the possibility for companies to join forces and interconnect, in order to ensure that not only production, but also the processing of transactions, is reliable, flexible, and automated. Moreover, blockchain technology offers the potential for automated information exchange and invoicing processes, and the tracking of delivery chains and production data. A further area of usage is the issuing of company-own crypto currencies as a financing tool for defined projects, or as a crowdfunding approach, with what are known as Initial Coin Offerings (ICOs).[33]

Despite all the potential of the technology, there are so far only a few SMEs that are making use of blockchain technology for their products and processes. One reason for this is the complexity of the technology: In order to develop an understanding of the possibilities, the use scenarios, and the hurdles, an intensive examination of the topic is necessary. So far, there are not many standards or norms that offer orientation, and many developments are only being driven forward by a small circle of enthusiasts. Nonetheless, there are a range of companies that are already implementing projects, such as the certificate management system of *CERTIVATION GmbH*[34], *Deutsche Bahn AG's* blockchain-based revenue distribution[35], or *AXA Insurance's* automated reimbursement of flight costs, called *FIZZY*[36].

However, not all projects are suitable for the use of blockchains. And even in places where blockchain makes good sense, every company should firstly ask

[33] Further information in Kaulartz/Matzke, NJW 2018, 3278; Borkert, ITRB 2018, 39; Weitnauer, BKR 2018, 231.
[34] See https://www.certivation.com
[35] See https://www.deutschebahn.com/de/Digitalisierung/technologie/Neue-Technologien/blockchain-3241170
[36] See https://www.fizzy.axa

themselves and answer several important questions – which this paper briefly outlines in the following.

3.1. Which preconditions need to be met before the use of blockchain?

Before beginning a blockchain project, it should first be clarified whether the use of the technology really represents an advantage over other possibilities of implementation. Purely internal applications can perhaps be better implemented with conventional database technology. Application cases for blockchain can often be found in multi-stakeholder scenarios, in which the transparency and verifiability of the data exchange or transaction is important.

For the successful implementation of a blockchain project, as an important second step, the most appropriate blockchain for the project should be identified. All solutions currently available in the market have their advantages and disadvantages, and the selection depends on the planned application, the number of participants, the desired scalability and speed, and the connections required to other already existing systems. If the project is company internal, the choice will probably be for a private blockchain. In contrast, for the collaboration of companies along a supply chain, for example, a federated blockchain is likely to be the first choice. If there is insufficient expertise within the company for this assessment, specialized consulting companies can offer support in the decision-making and the implementation of the project.

3.2. How expensive is a blockchain project?

Even though many blockchain infrastructures are open-source projects, usage is not completely free of charge: As already noted, in the case of public blockchains like *Bitcoin* or *Ethereum*, every transaction costs a certain sum in crypto currency.[37] Those who use a private blockchain need to pay for the infrastructure themselves and cover the costs of hardware and power requirements, or fall back on such services as the now available “Blockchain-as-a-Service” offers – more about this can be found in Section 3.5.

In particular, the fluctuating costs of transactions in public blockchains represent a risk. Companies that are dependent on stable costs for the entry of their data into the blockchain should weigh up very carefully the use of a public blockchain and instead consider a private blockchain or blockchain alternatives such as *IOTA*. In a public blockchain, transaction costs can increase dramatically as a result of an increasing number of transactions in the blockchain, and the entry no longer costs EUR 0.01, but EUR 5.00. In a public blockchain, it is also generally the case that transactions are prioritized by miners when the fee offered for the transaction is high – those who offer intermediate prices do not land at the top of the list, and the transaction takes longer. With Lightning and Raiden, however, there is already active work being done for the large and established blockchain technologies to master a considerably larger volume of transactions (see Section 2). If we get to the point where more than a million transactions are possible per second, then the transaction costs will sink further.

3.3. How efficient is blockchain?

The potential of blockchain technology for more efficient consumption of resources and lower operating costs is essentially dependent on the blockchain type being used (see Section 2.1). The best known blockchains – the crypto currencies *Bitcoin* and *Ether* – make use of the Proof of Work procedure for the validation of transactions. This procedure is very secure, but is very computationally (and therefore energy) intensive and only permits a limited number of transactions for each unit of time. As alternatives to the Proof of Work procedure, other processes of validation (for example, Proof of Authority and Proof of Stake) have been developed. These are more efficient (both computationally and from an energy perspective), but require more

[37] For a historical overview of the transaction costs in the Bitcoin system, see https://bitcoinfees.info.

trust in the administrators or the actors involved. Here, a conflict of objectives arises, given that security has so far been purchased through high energy consumption using the Proof of Work process.[38] It is of course contrary to the core idea of blockchain technology to yet again endow some network participants with extended permissions (e.g. Proof of Authority) or to deny other stakeholders access to the blockchain (e.g. private and permissioned blockchains). As described in Section 4 on data protection in blockchain systems, such adaptations can increase legal certainty, as responsibilities are defined with corresponding liability.

Particularly high gains in efficiency can be achieved in places where blockchain replaces manual processes with automated processes or takes on the function of an independent third party, such as a trustee or a certification authority. In these cases, even high transaction costs are often not of consequence, given that a complete stage in the value chain – and as a result also the cost center – is omitted.[39]

3.4. Middleware and Platforms – Status Quo

Many open-source projects and a multitude of large manufacturers and service providers offer professional support for Distributed Ledger Technology platforms. For example, *Amazon* has recently developed its own templates for the simple creation and deployment of diverse blockchain networks, and has integrated the necessary developer tools into its own *Amazon Web Services (AWS)* platform.[40] With its *Azure* Blockchain-as-a-Service,[41] *Microsoft* is following a similar path (see section 3.5).

Suitable frameworks are available now for all popular programming languages. Web developers can quickly find their way around the *Ethereum* network with web3js. The *Hyperledger Consortium* operated by *IBM* and

[38] For an overview of the verification mechanisms, see ECB, Virtual currency schemes – a further analysis, 2015 (Fn. 9), p. 10.
[39] World Economic Forum, The future of financial infrastructure – An ambitious look at how blockchain can reshape financial services, 2016 (Fn.1).
[40] See https://aws.amazon.com/de/partners/blockchain
[41] See https://azure.microsoft.com/en-us/solutions/blockchain

other large companies bases its *Chaincode* on *Go*, *node.js*, and *Java*, the latter being well established in the enterprise environment.

But it is not only the public distributed ledger systems that are in demand. The Berlin start-up "*BigchainDB*", with its eponymous product, provides a component which acts like a drop-in replacement for a database.[42] This means that *BigchainDB* behaves like a database, but has the features of a blockchain. Legacy systems benefit from this, because the adaptations required are, as a rule, considerably fewer.

This results in a number of advantages in adopting the technology, in particular for SMEs:

- SMEs should be careful in value creation networks not to invest too specifically in a special proprietary blockchain architecture from a single major supplier, in order to prevent a hold-up problem from developing.
- One possible approach can be to establish consortia at an early stage out of existing value chain networks, such as supply-chain management, that address the implementation of blockchain solutions. In this way, SMEs in the consortium work together on the development of the blockchain solution, share the costs within the consortium, and avoid dependent relationships.
- Train up your own technical staff in appropriate training formats[43] or join relevant interest groups[44] and working groups[45] in order to develop competencies. A nice side effect: You increase your attractiveness as an innovative employer for IT specialists.

3.5. Usability and Blockchain-as-a-Service (BaaS)

Blockchain-as-a-Service (abbreviated to BaaS) enables a relatively inexpensive and quick entry to distributed ledger technologies. The infrastructure can grow according to needs, and these services generally

[42] See https://www.bigchaindb.com/whitepaper/bigchaindb-whitepaper.pdf.
[43] Training course for qualified blockchain developers, certified by TüV Rheinland Akademie https://www.maibornwolff.de/blockchain-development-school
[44] See https://international.eco.de/topics/blockchain/
[45] EAM body and working group on DLT https://www.cba-lab.de

provide a dedicated contact person. Pilot projects, in particular, benefit from this, given that they can concentrate on the added value of distributed ledger technology for the business model – the technology is made available in operable and tested form.

This results in a range of advantages, especially for SMEs, which simplify the on-boarding of the technology:

- Less IT competency is necessary in-house. This means that BaaS offers are important and useful above all for small and medium-sized enterprises who lack in-house specialists.
- The blockchain solution can be implemented more simply.
- It is to be expected that the usability of BaaS offers will increase rapidly, given that there is competition between providers.

BaaS can, however, also have disadvantages for SMEs:

- Less flexibility in the design of the blockchain solution.
- Dependence on the large platform providers (this is exactly the kind of dependence that blockchain is actually designed to overcome).

When a BaaS solution is worth considering:

- BaaS offers enable a fast and easy entry to blockchain technology.
- BaaS offers can be good as a testing environment for blockchain solutions in the company, given that BaaS is associated with less investment risk.
- If, in the BaaS phase, the use of blockchain proves to be a worthwhile option, the company can then work towards the building of company-own competencies in the medium to long term for original, company-own blockchain solutions, given that these are more flexible and less expensive in the long run, and the dependence on a provider is reduced.

3.6. Interoperability

As is so often the case in the introduction of new software and IT systems, the use of blockchain in many cases demands adaptations of existing applications and systems. Many varying technologies and communications protocols are involved in this, and new tools are regularly being introduced.

However, standards are still only gradually becoming established. It is a challenge to keep up with the fast pace of development.

Blockchain has the potential to substantially revolutionize a range of sectors. The automotive industry, banking, retail (for example, foodstuffs and textiles), and also the energy sectors are therefore intensively investigating the impact of blockchain technologies on existing business models, and on the existing technical infrastructure. Appendix I provides an overview of a range of further blockchain applications.

Recommendations for SMEs

One obstacle to adaptation which is often mentioned, especially by SMEs, can be summarized under the term "interoperability." Interoperability is the capability to work together with differing systems, technologies, or organizations.[46]

The more that distributed ledger technologies move into software architectures, the more important the standardization of interfaces and protocols will become, in order to ensure a high level of interoperability between existing systems and a blockchain network. The interoperability challenge is, however, not blockchain-specific, but is a general issue for the introduction of new software and database systems.

3.7. Standardization

An obstacle for small and medium-sized enterprises is that the technology is still in the development phase. It is not clear what the blockchain systems of the future will look like. So far, no national or international standard for its implementation has crystalized.

However, there are certainly ambitions for introducing official standards. For example, *ISO* has been working since 2016 with German participation (*DIN Standards Committee for Information Technology and Applications, NIA*) on

[46] Zur Interoperabilität von Blockchains, Kolain/Wirth, MultiChain-Governance, in: Taeger, Jürgen (Ed.), Recht 4.0, Innovationen aus den rechtswissenschaftlichen Laboren, 2017, S. 833 – 845.

the development and establishment of ISO/TC 307 as a standard for blockchain.[47] *The German Federal Office for Information Security (BSI)* has now published two papers, in which concepts and requirements for the technology are assessed.[48]

However, there is still no guarantee that the various blockchain architectures will be sufficiently compatible with each other.

Conclusions for SMEs

For SMEs in particular, this results in a certain risk of costly investment mistakes and the danger of a hold-up problem. At the same time, in looking at the question of standards, the effect of innovation should not be neglected: If the definition of standards occurs too early, there is the risk of inhibiting innovation. As a consequence, there is always a certain trade-off between innovation and standardization.

4. Security and Data Protection

One key question for the introduction of new software or systems into the company – which will arise at the very latest when production operations are involved – is security. Therefore, in the following section, several security aspects are handled which should be taken into account if the use of distributed ledger technology is being planned or considered in the company.

[47] International Organization for Standardization, ISO/TC 307 – Blockchain and distributed ledger technologies, at https://www.iso.org/committee/6266604.html;

[48] German Federal Office for Information Security (BSI), Blockchain sicher gestalten – Eckpunkte des BSI, Version 2.0, at https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Blockchain_Eckpunktepapier.pdf?__blob=publicationFile&v=3.

4.1. IT Security

Blockchain technology cannot solve existing IT security problems in small and medium-sized enterprises. The architecture of blockchain may ensure system-inherent security for data exchange, but security risks continue to exist on the end points – meaning systems and devices that are connected to the blockchain. If these systems or devices store the transferred data in unencrypted form outside of the blockchain, the risk of data theft is not reduced. As a result, the use of blockchain technology in no way replaces the need for basic protection in the systems, such as virus and malware protection, professional rights management, and authentication.[49]

The classic IT security questions for conventional systems remain relevant for blockchain technology: hardware and software security, bugs, secure authentication, password security, keys and their administration, protocols, etc. The interfaces with the real world in particular are critical to security.

Cryptography is one of the core elements of blockchain technology. The technology to break cryptography is developing just as fast as encryption technology. It is highly probable that encryption algorithms that are still secure today will in the future be cracked. As with other technologies, there is therefore also the need for blockchain applications to be able to replace encryption algorithms. This is easier to implement for private blockchains than for public blockchains, where coordination with the respective community is always necessary.

In large networks with many nodes, it must on principle also be assumed that old data – which is protected by cryptography that is no longer secure – exists as a copy and remains available on one or more nodes. In this context, blockchain technology does not differ greatly from other systems when it comes to questions of IT security.

[49] On this and on the following, German Federal Office for Information Security (BSI), Blockchain sicher gestalten – Eckpunkte des BSI, Version 2.0 (Fn. 31) and German Federal Office for Information Security (BSI), Blockchain sicher gestalten – Konzepte, Anforderungen, Bewertungen; Pohlmann, 2019, Cyber-Sicherheit – Das Lehrbuch für Konzepte, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung, Springer Vieweg Verlag, Wiesbaden.

4.2. The "Garbage In – Garbage Out" Problem

Who checks the data that is stored in the blockchain? To reduce the risk of fraud or human error in the transmission of data to the blockchain, the quality of data collection and the sensor technology play an important role. In general, how the data from the real world arrive in the blockchain is very important. Here, the correctness, consistency, authenticity, and completeness must always be ensured. In production processes, sensors should ideally collect the data and automatically send it to the blockchain.

With regard to the digitalization of SMEs, blockchain technology should not be considered or viewed in isolation. Only once it is used in connection with automation or sensors can blockchains unfold their full potential and ensure data integrity. The use of distributed ledger technology is most appropriate for companies that have already achieved a certain degree of digitalization.

One challenge for SMEs for the use of blockchains in supply-chain management stems from the fact that the transmission of data to the blockchain needs to occur at the first stage of value creation, and therefore upstream. But it is precisely these stages of value creation that are often the least digitalized. A good example to look at here is the food industry. If – for example, in the case of a ready-made meal – the intention is for it to be possible to trace which exact farm the ingredients come from, then the data of every single farmer needs to be written into the blockchain. In order to exclude the possibility of fraud and human error, the transmission of data to the blockchain should occur automatically through sensors during the harvest. For this, a certain level of digitalization is necessary at the upstream levels. Only when the digital infrastructure in the form of automatic and quality assured data collection and sensor technology exists along the entire value chain can the "Garbage In – Garbage Out" problem be solved. In long and complex value chains, only the large market actors will be able to generate enough pressure to motivate all participants to implement the necessary digital infrastructure.

The recording of objects, for example to document their origin, also poses the same challenge for the initial Root Certificate: At what point is a material product digitalized for the first time? And who will become established as the certification body for blockchain entries, and thus create a trustworthy basis for the technology? For digital goods, this is quite simple; in contrast, goods in the real world must be individually identifiable and describable.

Conclusion for SMEs:

Not all scenarios are suited for blockchain implementation. Therefore, it is advisable to experiment, build prototypes, test, and improve or discard a less promising approach and build something new.

4.3. Data Protection Law

As with other systems, the handling of sensitive or personal data in blockchains is security-relevant. After all, blockchains are often public.

4.3.1. Scope of Application

Data stored in a blockchain can represent personal data, and thus fall within the scope of the General Data Protection Regulation (GDPR).[50] In the context of the GDPR, personal data is any information that refers to a specific natural person, or where inference to the person can be made. So-called pseudonymous data – data that itself does not allow identification, but for which an assignment rule exists – is also considered personal data. Completely anonymous data does not fall within the scope of the GDPR.

In this context, not only public keys, but also other data stored as payload in a blockchain, and hash values (potentially of a pseudonymous nature) can represent personal data. Encryption of data does not automatically remove the data from the scope of the GDPR.[51]

What is important is reference to the person, because a range of legal obligations must be complied with in the processing of personal data. In many ways, blockchain technology does not seem to be compatible with the

[50] Further information in Hofert, ZD 2017, 161, 163 et seq.; Bechtolf/Vogt, ZD 2018, 66, 68 et seq.; Martini/Weinzierl, NVwZ 2017, 1251, 1252 et seq.; Schrey/Thalhofer, NJW 2017, 1431, 1433.
[51] Bechtolf/Vogt, ZD 2018, 66, 68 et seq.; Hofert, ZD 2017, 161, 163; Spindler/Bille, WM 2014, 1357, 1366 et seq.

current data protection regulatory model. The possibility of developing blockchain projects on the basis of anonymization is therefore of considerable importance.

4.3.2. Classification of Participants According to Data Protection Law

The GDPR recognizes three categories of actors:

- Data Controllers, who define the scope, type, and manner of data processing,
- Data Processors, who are bound to the instructions for carrying out certain data processing activities on behalf of the controller, and
- Data Subjects, that is, individuals whose personal data is processed.

It is only with difficulty that a distributed system like a public blockchain can be integrated within this strict categorization. In the case of a public blockchain, a range of questions arise with regard to dealing with regulatory stipulations – beginning with the question of who is actually the Data Controller in the sense of data protection law.[52]

The *German Blockchain Association*[53] therefore suggests, for example, classifying nodes as infrastructure – similar to an ISP or a hosting provider – and therefore not as relevant actors from the perspective of data protection law, ensuring them instead neutrality when it comes to data protection law. The Data Controller for the purposes of data protection law would then simply be the provider of the application that interacts with the blockchain.[54] Such handling is desirable, but it would require an amendment to data protection law or – although only possible within limits – further judicial development of the corresponding law.

Nevertheless, the GDPR, even in its existing version, offers options to resolve apparent conflicts: For example, the concept of "Joint Controllers" (Art. 26

[52] Erbguth/Fasching, ZD 2017, 560; Martini/Weinzierl, NVwZ 2017, 1251, 1253 et seq.; Saive, CR 2018, 186.
[53] See https://bundesblock.de
[54] Blockchain Bundesverband e.V., Blockchain – Chancen und Herausforderungen einer neuen digitalen Infrastruktur für Deutschland, Version 1.1, 16.10.2017, p. 26, at https://bundesblock.de/wp-content/uploads/2017/10/bundesblock_positionspapier_v1.1.pdf.

GDPR) can certainly be made use of for the governance of a permissioned blockchain. The contractual conditions of the data processing also offer some design options, such as in the relationship between the provider of a blockchain-based application and the individual nodes.

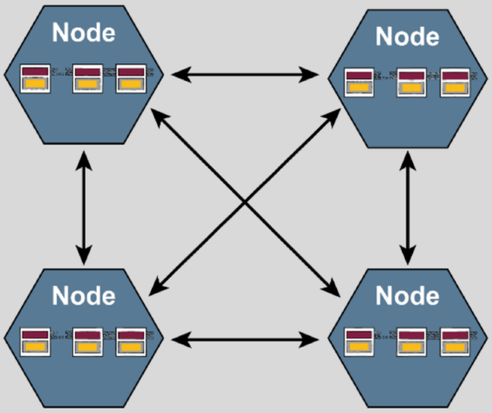

Fig. 5: Blockchain peer-to-peer network

In legal terms, coping with compliance requirements can result in complex governance models and technical challenges for the development of the project: For example, the Joint Controllership of several participants requires not only a contract in which the decision-making process and areas of responsibility are precisely described, but also the actual possibility of implementing decisions within the blockchain and complying with the rights of data subjects. This can only succeed if the legal requirements are also supported on the technical level.[55]

A further challenge exists in the handling of the rights of data subjects – a solution needs to be found to delete personal data or to remove the personal reference, in order to satisfy the stipulations of data protection law. If the possibility cannot be excluded that personal data is involved, topics related to data protection law must be taken into account from the very beginning in the development of projects. If in doubt, it is possible to work together with the responsible data protection authority to clarify how implementation can be undertaken in a legally compliant manner.

[55] Further information; Pesch/Böhme, DuD 2017, 473; Bechtolf/Vogt, ZD 2018, 66, 70 f.; Martini/Weinzierl, NVwZ 2017, 1251, 1256 ff.

5. Summary

Blockchain technology is without question not only a very interesting technology, but one which – as far as can be foreseen today – is likely to be used in numerous new application areas. A number of examples can be found in the following section of this paper.

In spite of all the enthusiasm ("technology hype") which accompanies new technologies in popular public debate, a down-to-earth exploration of whether the use of a blockchain actually offers a concrete advantage is necessary in approaching each application scenario. In instances where it can be concluded that a decentralized data structure, additional resources for the redundant distribution of the data in a network, and tamper-proof storage of the data are no more advantageous than existing security mechanisms, then database systems which are already established on the market are usually the more cost-effective and reasonable choice. Blockchain technology also does not solve any fundamental IT security issues. Despite "Security by Design," a blockchain is still only as secure as the environment in which it is operated: Keys, passwords, and credentials must also still be secured, as must the network components and computers on which the blockchain is operated.

Even if questions of efficiency, usability, standardization, or interoperability are not yet optimal for every application scenario, one thing is nevertheless certain: The development of blockchain technology is progressing fast and the first solutions are already becoming established in the marketplace.

This is particularly true for increasingly interconnected value chains embedded in multi-stakeholder systems. For these, blockchain has revolutionary potential as a cross-sectoral technology. Values of all kinds can be transferred digitally and securely without intermediaries, and are traceable for all parties involved.

The Competence Group Blockchain in eco – Association of the Internet Industry is accompanying this ongoing development and, together with its network of members, offers all interested parties a platform for the exchange of know-how and best practices: international.eco.de/topics/blockchain.

I. Sample Applications

The *Bitcoin* blockchain is the most well-known application for blockchain technology, but only one of numerous possibilities. There are no blueprints for blockchains. They have to be developed and tested individually. The following examples illustrate worthwhile applications for blockchain technology.

A. Finance, Payment, and Banking

The best-known application of blockchain technology is the crypto currency *Bitcoin*[56], a digital surrogate currency. In the financial crisis 2007/2008, the still anonymous founders wanted to create a currency – a financial instrument with payment and depository functions – that could not be controlled or manipulated by people. The exchange rate of *Bitcoin* with real currencies is very volatile, meaning that investing in *Bitcoins* is highly speculative.

Bitcoin means that blockchain is often strongly associated with fintech applications.[57] Over the years, a number of other crypto currencies have established themselves. A few well-known examples are *Bitcoin Cash*[58], *Litecoin*[59], *Ether*[60], and *XRP*[61].

In Germany, established banks, as well as the *Deutsche Börse (German Stock Exchange)*[62] and the German federal financial supervisory authority *BaFin*[63], have also been exploring ways of using blockchain and other distributed ledger technologies. Blockchains are being tested to document the trade with securities in a traceable and tamper-proof manner, and to optimize and accelerate the procedures for transaction processing. Many banks have their

[56] See https://bitcoin.org/de/

[57] On this, Hofert, Regulierung der Blockchains, 2018, p. 1 et seq.; Fairfield, 88 S. Cal. L. Rev. (2015), 805, 829 et seq.

[58] See https://www.bitcoincash.org

[59] See https://litecoin.org/

[60] See https://www.ethereum.org

[61] See https://www.ripple.com

[62] See https://deutsche-boerse.com/dbg-de/unternehmen/gruppe-deutsche-boerse/geschaeftsfelder/blockchain-business-areas

[63] See https://www.bafin.de/DE/Aufsicht/FinTech/Blockchain/blockchain_node.html

own blockchain projects, but also form consortia in order to research blockchain technology together, such as *we.trade*.[64]

Finally, Initial Coin Offerings (ICOs) are increasingly being issued and discussed. For business models based on crypto currencies, ICOs represent a still largely unregulated form of crowdfunding. When raising capital, tokens or a new crypto currency are issued and sold to investors. Initial Coin Offerings are not yet on an equal footing with conventional forms of financing. However, *BaFin* has already published guidelines for ICOs.[65]

Private companies, such as *Quantoz N.V.*[66] from the Netherlands, offer accounting systems on a blockchain basis, with which, among other things, internal accounting processes within the organization can be managed.

B. e-Government, and Identity & Document Management

Blockchain technology not only helps to optimize the processes between different administrative bodies, but it also serves internal cooperation within administrations – for example, in checking whether certain data or documents are available in an administration. It is also possible to use blockchain technology to ensure the integrity of data and documents or to verify the identities of persons and goods.

[64] See https://we-trade.com/

[65] See https://www.bafin.de/SharedDocs/Downloads/DE/Merkblatt/WA/dl_hinweisschreiben_einordnung_ICOs.pdf?__blob=publicationFile&v=2

[66] See https://quantoz.com/

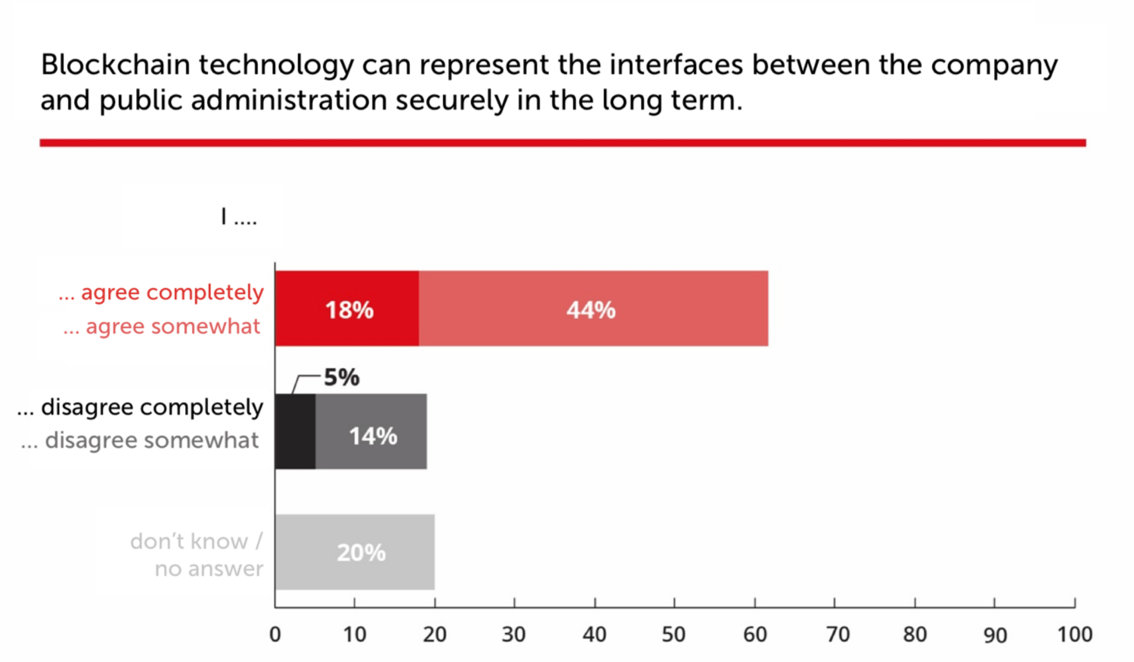

Fig. 6: Survey by the eco Association from April 2018

The security and cryptography inherent in blockchain allow the development of innovative identity standards, in which, for example, users themselves have complete control over their personal data. With a blockchain application for identity management, users can decide themselves which data is passed on and thus have a transparent overview of data collection and data processing.

While it may in fact be difficult to forge identification papers, given that they are now equipped with very complex security features, doing so is not impossible. In addition to this, the handling and checking of the security features is not always quick and easy. As a result, services have been developed that represent an identity in the blockchain via a Smart Contract. These Smart Contracts can be assigned attributes and can be certified by third parties. Identities and their associated (and at times certified) attributes can then be forwarded via a secure communication channel.

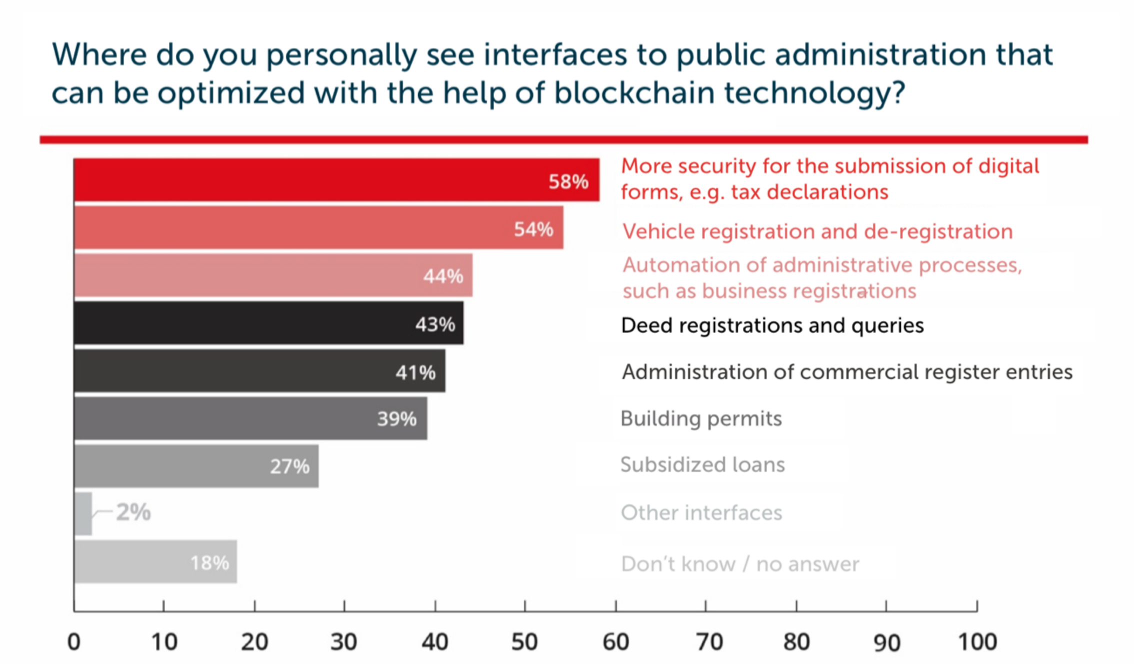

Fig. 7: Survey by the eco Association from April 2018

A number of individual initiatives have joined the *Sovrin Network*[67], in order to collaborate on a joint system. In Germany, the *bbw University of Applied Sciences* with the project *ISÆN*[68], *esatus AG*[69], and *regio iT*[70] are all active in the network.

In the future, the following scenario could conceivably apply to land register entries for real estate: Instead of handing over money and transferring ownership step by step and only through a notary, a blockchain could handle the process. Georgia[71] has already migrated its land registry to a blockchain solution; a similar pilot project was successfully completed in Sweden[72]. While the motivation in Georgia was mainly due to the fight against corruption, in Sweden the focus is on the need to maintain citizens' confidence in government services, even in the age of cyber crime.

[67] See https://www.quantoz.com
[68] See https://www.bbw-hochschule.de/forschung/forschungsprojekte/isaen.html
[69] See https://www.esatus.com/Solutions/Blockchain
[70] See https://www.regioit.de/aktuelles/regio-it-nachrichten/2017/fuehrerschein-pruefen-per-blockchain/
[71] See http://agenda.ge/en/news/2018/396
[72] See https://www.lantmateriet.se/contentassets/8d2b5d7647634c02a329b01e46e61071/the-land-registry-in-the-block-chain---testbed-2017.pdf?qry=blockchain

C. The Energy Sector

The energy sector is very active in testing the use of blockchains and Smart Contracts to advance the trade in energy sources. The drivers of this development are the automation potential and the traceability of transactions. Smart Contracts also offer the possibility of using the invoice handling function to make transactions of small units economically viable. Buying electricity at charging stations or feeding privately generated electricity into the grid are possible scenarios. Currently, it is not uncommon for administrative costs to be more expensive than the actual electricity costs.

Blockchain could be used for communication between the generator and the electricity provider, or between the vehicle and the charging station, for every charging session and for each and any provider. Intermediaries – who conclude collective agreements with the electric charging station, charge for each charging session with the e-tanker, and receive a commission each time – would become superfluous.

A prominent and active platform for energy trading on the basis of blockchain technology is the *Enerchain*[73], but also the pipeline operator for natural gas *Open Grid Europe*[74] is exploring the use of blockchain technology. There are also projects which deal with mechanisms for the automated stabilization of power grids using blockchain technology.[75]

Several projects are dealing with the use of Distributed Ledger Technologies for conveying market communication in the energy sector. The *energy web foundation*[76] is focused on the definition of a new uniform communication standard in data exchange. The *edna German Energy Market & Communications Association*[77] is a consortium of different service providers from the energy sector, and it also wants to provide market communication services using blockchain technology. In the project consortium *ETH@Energy*[78], a number of German energy providers and grid operators have joined forces and have been actively piloting the transfer of relevant process steps to a federated blockchain since 2016.

[73] See https://enerchain.ponton.de/
[74] See https://www.open-grid-europe.com
[75] See https://innovation.elia.be
[76] See https://www.energyweb.org
[77] See https://edna-bundesverband.de/
[78] See https://www.eth-energy.de

D. Insurance

The blockchain initiative of the insurance sector, *B3i*[79], is examining whether sector-wide standards and procedures can be developed with blockchain technology – for example, as the basis for new business models.

The insurance company *AXA*[80] has already implemented an insurance policy for delayed flights as a pilot project. In this, flight delays are registered and the payment of the insured sum is triggered automatically.

E. E-Commerce, Logistics, and Traceability

Alongside "classic" applications in payment transactions, blockchain also offers itself as a retail infrastructure for e-commerce providers, one which will complement or even replace conventional market places. A particularly ambitious project in this sector is the "*Global Alliance of Merchants on the Blockchain*".[81] A number of well-known companies are involved and it aims to incorporate every product in a Smart Contract in order to allow the retailers to market their products independently of the conditions of the established platforms.

In the supply-chain area, there are numerous blockchain projects and ideas, ranging from proof of manufacture through to the digitalization of freight logistics. The payment provider *Wirecard*,[82] for example, offers a prototype of a universally usable supply-chain platform. The prototype focuses on connecting retailers and producers, and integrating all business processes in Smart Contracts.

Traceability – ensuring gapless tracking of goods – still poses great challenges for IT. A key reason for this is that a continuous flow of data across different IT systems must be guaranteed: from production through to the end customer. The complexity of today's supply chains also means that the tracked goods can be manipulated – for example, by infiltrating the supply chain with counterfeit products. But also improper handling of goods, above

[79] See https://www.b3i.tech
[80] See https://www.fizzy.axa
[81] See https://www.gamb.io
[82] See https://www.wirecard.com

all the breaking of a required continuous cold chain, are well-known problem areas. The Danish *A. P. Moller-Maersk Group*, together with *IBM*,[83] is one of the pioneers in the digitalization of logistics processes using blockchain technology.

Meanwhile Track & Trace solutions based on blockchain solutions are also available as ready-made systems. In addition, service providers such as the company *SEEBURGER*[84] also offer the processing and archiving of electronic invoices on a blockchain.

Directly after diamonds have been mined, the company *Everledger*[85] registers them and their individual characteristics on a blockchain as proof of identity and provenance. Currently, it is necessary to trust the certificate of authenticity in the trading of diamonds. These can get lost or be forged. Through using blockchain technology, *Everledger* makes the path of the diamond completely traceable from the mine to the customer. The certificates of authenticity are entered into the blockchain, and can thus always be attributed to the correct diamond. No-one can falsify the entries or delete them from the blockchain. Through this, trading is expected to become more transparent and more secure. The same procedure can also be applied to other luxury goods, e.g. textiles, art, or jewelry.

It is also particularly important for the food and pharmaceutical industries to be able to prove the origin or authenticity of products as well as their unbroken supply chains. *Merck* and *SAP*,[86] for example, are already working on a concept and have developed the *SAP Pharma Blockchain POC App*.

Lufthansa[87] and *Deutsche Bahn (German Rail)*[88] are also testing a large number of application fields for blockchain solutions, both in the fields of logistics as well as for process optimization and the billing of internal services via Smart Contracts. *Deutsche Bahn* is also testing federated scenarios in cooperation with other transport associations, with the intention of using blockchain to transparently manage the very complex revenue distribution from ticket sales in regional public transport. This is motivated by the fact that

[83] See https://www.tradelens.com/
[84] See https://blog.seeburger.de
[85] See https://diamonds.everledger.io
[86] See https://blogs.sap.com
[87] See http://blockchainforaviation.com/
[88] See https://www.deutschebahn.com/de/Digitalisierung/technologie/Neue-Technologien/blockchain-3241170

increasingly seamless travel chains that integrate more and more providers have been hampering unambiguous distribution of revenues.

The project *SAMPL*, or *Secure Additive Manufacturing Platform*,[89] is using another form of proof of origin and authorization management. Here, a blockchain is used to manage both the permissible number of print operations and the authorization and release of the printer used for the production of so-called 3D-prints in additive manufacturing.

[89] See http://www.sampl-3d.de/

II. Authors

The eco Competence Groups Blockchain and Security would like to thank everyone who worked on this paper:

Sebastian Beyer
Product Manager Blockchain Ensured Certificates Service
CERTIVATION GmbH, Lingen (Ems)
sbeyer@certivation.com

Prof. Dr. Georg Rainer Hofmann
Director, Information Management Institute IMI
Aschaffenburg University of Applied Sciences
hofmann@th-ab.de

Martin Lundborg
Head of the Communication and Innovation Department
WIK Wissenschaftliches Institut fur̈ Infrastruktur und
Kommunikationsdienste GmbH, Bad Honnef
m.lundborg@wik.org

Christian Märkel
Senior Economist
WIK Wissenschaftliches Institut für Infrastruktur und
Kommunikationsdienste GmbH, Bad Honnef
c.maerkel@wik.org

André Mundo
Area Head for Distributed Ledger Technologies
MaibornWolff GmbH, Munich
andre.mundo@maibornwolff.de

Prof. Norbert Pohlmann
Department of Informatics and Journalism
if(is) - Institute for Internet Security, Westphalian University of Applied Sciences, Gelsenkirchen
pohlmann@internet-sicherheit.de

Lars Steffen
Director eco International
eco – Association of the Internet Industry
lars.steffen@eco.de

Stephan Zimprich
Leader of the eco Competence Group Blockchain
Partner, Fieldfisher (Germany) LLP, Hamburg
stephan.zimprich@fieldfisher.com

The English edition was translated from the original German by Judith Ellis, Eilín Geraghty, and Cáit Kinsella.