A Thief's End—Potentials of Blockchain as Anti-fraud Protection Using a Software Service Company as an Example

Christian Döberlein [a], Mirko Ahmad [a], Marina Bühler [a], Klaus Dehmel [a]

[a] *School of Business, Economics and Society, Friedrich-Alexander-Universität Erlangen-Nürnberg*

Abstract. With a constantly growing amount of data, not only the importance of data and its management for companies but also the urgency of secure data management increases. Traditional data management systems reach their limits here. Therefore, the potentials of blockchain to protect against fraud are discussed increasingly more frequently. While there are various theoretical explanations for blockchain's structure and functioning, there rarely are specific recommended actions. This paper examines blockchain's protection ability against fraud by focusing on three use cases. To identify the relevant uses cases for a software service company as an example used in this paper, the use cases were structured according to the specific business sectors of this company and according to the potential for fraud protection. The three identified and elaborated use cases are contract management, proof of existence combined with smart contracts, and collaborative monitoring. The integrated solution of the use cases and recommended action is a holistic blockchain platform, which consists of three levels. This model is not limited to the exemplary case of a software service company and can be built upon existing platforms, databases, and systems. Blockchain's potential for protecting against fraud in the examined uses cases was identified to be high.

Keywords. blockchain · platform · fraud protection · proof of existence · smart contracts

1. Introduction

In the information age, with megatrends such as digitization and globalization, the successful handling of huge amounts of data, also known as big data, is indispensable for companies to be able to compete in the market (Deloitte, 2017). This is not only about extracting the relevant information from immense amounts of data and thus generating knowledge but also about protecting against data theft. With increasing digital networking and the use of modern control systems, the threat of cyber attacks is also increasing for companies (Deloitte, 2017). According to a study by Deloitte (2017), the number of cyber attacks has not only almost doubled in the last five years, but large companies are usually attacked several times a month, often even daily. The targets of these e-crime attacks are usually financial and customer data and thus particularly sensitive and success-relevant information (KPMG, 2017).

Previous data management systems often have inadequate security mechanisms and are therefore not sufficiently protected against attacks (Verizon, 2017). In traditional data management systems, the data are stored on a central server so that data management is handled by a central instance (Schlatt et al., 2016). This often results in a lack of encryption during identity checks for access to the systems, but also in a lack of transparency of the data and data management, so that fraudulent activities sometimes do not fall within the conspicuousness range of the security systems and thus remain undetected (Verizon, 2017). One of the greatest dangers for companies is the negligent handling of data by employees so that, in addition to technical measures, adequate risk awareness must also be created among employees (Deloitte, 2017).

Due to the great importance of data for the success of a company, it is essential for companies to protect themselves against data fraud. In addition to new encryption methods, blockchain is often seen in this context as a disruptive technological innovation predicted to have waves of effects similar to those of the Internet (Bridgers, 2017).

The recommended course of action will be developed using the example of a software service company to analyze the chances of optimizing the security precautions of companies using blockchain.

First, a theoretical framework is established. Then specific use cases are considered, from which a recommended course of action for the software service company is derived. This summarizes the core elements of the use cases in an overall solution in the form of a suitable model and focuses on the creation of an innovative platform. Finally, the limitations for the applicability of blockchain and the general conditions of the designed recommendation for action are shown. The aim of the paper is to provide companies with a recommendation for action for efficient protection against fraud by using blockchain. The example of the company is used as a guideline.

2. Theoretical background

2.1. Definition, structure, and development of blockchain

Blockchaining is a technology which, due to its novelty, high complexity, and multitude of implementation options, has not yet been subject to a uniform definition (Condos et al., 2016). Regardless of the exact definition, blockchain is in principle understood as an electronic data register, which has some basic characteristics. These include decentralized data management, which makes mediators superfluous for any transactions via blockchain (Bridgers, 2017). These transactions include crypto currencies as well as intellectual property, product trade, and personal data (Bridgers, 2017). Blockchain was made possible above all by rapid developments in the Internet, digitalization, the computing power of computers, and innovative and decentralized data management systems (Brandon, 2016). Blockchain became known primarily as the basic technology for the crypto currency Bitcoin, but its range of applications goes far beyond this (Dai et al., 2017).

Mediators are no longer needed in this system since blockchain is based on a peer-to-peer principle in which the entire network verifies individual transactions and entire blocks. This means that there is no central coordination or mediators since the network nodes communicate directly with each other (Schlatt et al., 2016). All information is stored redundantly on each computer in the network, and each computer checks the transactions according to defined principles (Schlatt et al., 2016). This is called consensus mechanism and is one of the core elements of blockchain (Schlatt et al., 2016).

A decisive factor for the security of blockchain is cryptography, referring to modern methods for encrypting information. As soon as a transaction is confirmed by the network nodes, it is cryptographically encrypted and shared with the entire blockchain (Dai et al., 2017). In most cases, asymmetric encryption is used in the form of public key cryptography, which works as follows. A user receives a private key, a public key, and an address for each transaction. To send a transaction, the recipient's address and his own private key are required. The private key is used to authenticate the transaction and protects the transaction from fraud. The process can be simplified as follows: The sender encrypts the message with his own private key. The recipient then decrypts this message with the sender's public key. The recipient knows that the message could only be encrypted with the sender's private key, so he can trust the origin of the message (Brandon, 2016).

When the majority of nodes in a blockchain's network have validated the transaction, it is added to the blockchain with other previous valid transactions in a new block and shared with the entire blockchain (Underwood, 2016). This is where the consensus mechanism of the network nodes comes into play, known as mining, which ensures that transactions are encoded in blocks according to the specified cryptographic procedures (Brandon, 2016). There are various methods for mining, the best-known example being proof of work, which is also used for Bitcoin (Kewell et al., 2017). Here, calculation procedures are executed a million times to determine the appropriate input from the given output. The computers use highly complex hash functions for this purpose, which assign smaller target quantities to large input quantities to find the required character string and determine the so-called hash value (Kewell et al., 2017). The trial-and-error method is used, in which approaches are tested until the correct solution is found. The time required and the high costs of testing this method prevent potential hackers from manipulating blockchains with false data (Yermack, 2017).

When the desired input is found by a miner, that is, the computer that does the calculations, it receives payment—in the Bitcoin blockchain in the form of bitcoins released by the mining process. The transaction is then shared with the entire blockchain so that the remaining network nodes can control the solution. It is crucial that the verification process be simple since the algorithm is known to all participants, while the mining, that is, the process of providing evidence, is complex (Kewell et al., 2017).

Verified blocks are then added to the blockchain accordingly (Underwood, 2016). Each block contains a so-called hash of the previous block so that a chronologically correct sequence of blocks is guaranteed (Brandon, 2016). A hash pointer indicates that the previous block has not been falsified (Yermack, 2017). Once a transaction has been added to the blockchain, it can no longer be changed (Dai et al., 2017).

The individual transactions are therefore stored in blocks and thus shared with the entire blockchain. This process enables a high degree of transparency for all network participants, who can thus trace and control the entire transaction history (Dai et al., 2017). The decisive factor is that a blockchain goes far beyond a conventional database, among other things because of the way it functions, especially since it is not managed and controlled by a central authority (Underwood, 2016).

In principle, a distinction can be made between private and public blockchains (Underwood, 2016). Public blockchains are usually unattended and can therefore be used without restriction (Underwood, 2016). Anyone can participate in the consensus mechanism and enter into transactions (Coyne & McMickle, 2017). A well-known example is the crypto currency Bitcoin, which anyone can use freely. Public blockchains are increasingly being criticized because the competitive mining concept, in which the fastest miner receives a reward, requires large amounts of electricity (Yermack, 2017). Private blockchains are usually supervised, and their use is only accessible to certain participants (Underwood, 2016). This increases the security of the blockchain and the transactions and blocks included (Yermack, 2017). A disadvantage is that decentralization and thus a fundamental element of the blockchain is restricted (Yermack, 2017). Private blockchains therefore have more in common with traditional databases than public blockchains (Coyne & McMickle, 2017).

Blockchain can be used in a wide range of applications—for example, in the financial sector it can not only be used in the form of crypto currencies but also make agreements simpler, more transparent, and cheaper (Underwood, 2016). It also has a high potential for disruption in other sectors and areas, such as in democratic elections, in healthcare, or with smart contracts (Yermack, 2017). Smart contracts are seen as particularly decisive. They are based on blockchain technology and simplify and automate the drafting and execution of contracts, as shown in use case 2, thus shaping numerous sectors, such as the legal sector (Dai et al., 2017).

Due to the high complexity of today's transactions and the increasing amount of data, blockchain technology offers numerous advantages that go beyond transparency and cost savings and can make its use worthwhile in countless areas. Errors and inefficiency caused by human actions in the company and its intermediaries can be reduced. Transaction data are accurately presented at all times without the use of paper documents or other controls that can slow down processes and increase costs (Underwood, 2016).

However, the biggest advantage is the protection against fraud, which is made possible by the use of blockchain.

2.2. *Characteristics of blockchain for the protection against fraud*

Due to its structure and functionality, blockchain offers clear advantages over conventional databases, such as systems for storing customer data in companies that are insufficiently protected against cyber attacks due to a lack of data transparency and protective mechanisms (Verizon, 2017). The following five core factors of blockchain result in a more efficient protection against fraud as the biggest advantage.

Firstly, decentralization in data storage and management results from the distributed computer network (Schlatt et al., 2016). This means that there are several independent network nodes that communicate and synchronize (Schlatt et al., 2016). A key aspect here is the redundant storage of data in each of these nodes so that the current system status is not lost in the event of a technical failure of a computer (Brandon, 2016). This redundancy and decentralized status storage enables the computers to monitor the system jointly and prevent information in the register from being falsified (Dai et al., 2017). The nodes thus work together on an equal footing according to the peer-to-peer principle (Schlatt et al., 2016).

Secondly, in the consensus mechanism, the system status is verified along the entire network instead of via a central authority, as is the case in classic databases (Schlatt et al., 2016). It is crucial that each computer monitors the validity of individual transactions as well as entire blocks and that the blockchain can only be supplemented if the majority of network nodes agree. This eliminates the need for intermediaries and third parties within the system (Schlatt et al., 2016) and thus reduces the risk of fraud through the influence of external parties. There are numerous principles for consensus mechanisms in the blockchain, for example, the proof-of-work principle is used for Bitcoin, while the crypto currency Ethereum uses proof of stake (li, 2018). Both principles aim to prevent disproportionate or erroneous use of the blockchain (Schlatt et al., 2016). The mining process makes it more profitable for potential scammers to secure bitcoins through successful mining than to risk an attack (Kewell et al., 2017). This in turn contributes to a higher resistance of the blockchain (Kewell et al., 2017). In this way, the proof-of-work principle prevents subsequent changes to the blockchain since the fraudster would have to achieve a higher computing power than the entire remaining network combined (Coyne & McMickle, 2017).

In addition, by manipulating one block, an attacker would automatically change the scatter values or hashes of all the other blocks—if the block to be manipulated lies far in the past, the fraudster would have to find the valid hashes for all other blocks in the blockchain up to the most recent block. At the same time, the blockchain is continuously expanded with new blocks. Therefore, this mechanism represents a further protection for the blockchain due to its noticeably insurmountable effort (Yermack, 2017).

Thirdly, verification by cryptography is important. Modern cryptography refers to methods for encrypting information that make data theft almost impossible (Schlatt et al., 2016). Examples are public key cryptography and hash cryptography, which are based on different principles

Fourthly, a transaction is cryptographically sealed and shared with the entire blockchain once it has been confirmed by the network nodes (Dai et al., 2017). This unrestricted transparency prevents the falsification or destruction of entries, for example, to cover up fraudulent activities.

Each network node can thus view all previous transactions and trace and control them (Schlatt et al., 2016). Fifthly, the transaction history is closely linked to the transparency of the blockchain. Invalid transactions are therefore immediately detected and not confirmed by the network nodes in the system (Dai et al., 2017).

2.3. *Application areas for a software service company in the area of protection against fraud*

Blockchain is a topic that has gained increasing attention in recent years. Thus, the blockchain can be used in a wide variety of areas. These main categories and their areas of application are shown in Table 1. The Fraunhofer Institute for Applied Information Technology (FIT) distinguishes the following 11 application areas: Internet of Things, smart grid, social media, supply chain management, the darknet, the public sector, the legal sector, medical technology, the financial sector, and proof of origin. It can be seen that both classic areas, such as the public and legal sectors, and newer ones, such as supply chain management (SCM), darknet,

or Internet of Things (IoT) are affected. Thus, one potential of the blockchain lies in the fact that there are hardly any restrictions regarding the areas of application (Schütte et al., 2017).

Blockchain can be classified into different main categories, shown in Table 1. By categorizing the blockchain, the above-mentioned areas of application can be classified (Witt & Richter, 2018). These areas of application and main categories are the result of a systematic literature search. In the process, the areas of application were assigned to the main categories, resulting in various application cases.

Table 1. Main categories, application areas, and examples of the blockchain (BC).

BC main category	BC application area	Example
Contract management	Legal and public sector, SCM	Data storage and data sharing
Proof of existence	Proof of origin, social media, SCM	Proof of content and origin
Smart contracts	IoT, legal sector, SCM	Automated contract execution
Collaboration monitoring	Public sector, SCM, IoT	Coordination of partners and processes

In combination with the business environment and the core competencies of a software service company, the relevant categories can be derived. These core competencies include the data center and the printing; the logistics and service center; and confidential cooperation with local authorities, government agencies, and companies.

As a result, areas of application such as the financial sector, the legal and public sectors, proof of origin, and IoT are more relevant to the software service company than, for example, darknet or medical technology as the company's activities are concerned with these areas. Based on this, three use cases were developed.

2.4. Use cases for protection against fraud

2.4.1. *Use case 1: Contract management*

The topic area of contract management in this section includes problems that can occur in current contracts. Contracts from and with institutions, end customers, and companies are considered. No differentiation is made here as many of the following problems can occur with all of them. Contract management can be considered in two parts.

Firstly, the identities of the contracting parties must be clarified before the contract is drawn up. Only if the identities of both contracting parties are proven, fraud can be excluded. Secondly, the contract itself must be protected against fraud. Without the blockchain, there are several possibilities of fraud when concluding a contract. The first source of fraud is the amount of information that a person must disclose when signing a contract in order to fully disclose their identity. A well-known procedure, especially in banks, is the "know your customer" (KYC) principle. Here, more information is requested when a contract is concluded than is actually necessary for the contract. The end customer does not know what this information is needed for. However, it is not only the lack of transparency of the information that is a problem but also the fact that all information is stored in a bundle and can be accessed in the event of an attack. Blockchain technology can eliminate this problem as the user himself has access to his data. If he updates his stored information, it is stored in a new block and added. This update takes place simultaneously at all network nodes in the network. This ensures that the amount of information is always up-to-date and can be monitored by the user (Guo & Liang, 2016).

Secondly, the "bring-your-own identity" (BYOI) principle poses a problem. Here, large providers such as Facebook or Google allow users to log in to new pages with their previous account from these websites. Although this is of course convenient for the end customer, he also passes on all his information to the existing providers. Again, there is a lack of transparency and the possibility of tracking the data. Just as with the amount of information, this problem can easily be solved by a blockchain. Since the end customer can log in via his public blockchain identifier (ID), third-party providers are no longer needed. It is assumed that it will be possible to register with this ID on the websites of authorities, institutions, or companies (Pratini, 2018).

Thirdly, national borders pose another problem. Within one country, legal steps are not always comprehensible, but the involvement of several countries can lead to longer processes and communication difficulties. Trans-regional communication and the involvement of several actors is a problem. Not only are processes more difficult to control, but they are also difficult to understand. Mergers of several countries, such as the EU, allow better supra-regional cooperation in the fight against crime but do not rule out fraud. Due to the independent networking of the blockchain nodes, national borders are no problem. Both the creation and the follow-up of the contract status can take place via the blockchain. All that is required is a common language, for example English, and a platform to which all contractual partners have access at all times (Guo & Liang, 2016).

Fourthly, intermediaries are affected. Intermediaries are particularly common in the financial sector. These intermediaries draw up contracts, monitor processes, or store contracts, for example. For these services to be provided, all the information of the contractual partners must be shared. In addition, new developments, for example in a contract, must be approved by the intermediary. Blockchain technology offers automatic monitoring of these contracts without intermediaries. Not the contracts themselves but the location of the contracts can be stored in a block and can be stored tamper-proof and decentralized. Every change

to the contract is immediately visible to all participants. This means that the blockchain can not only take over the tasks of the middleman but can also take over them faster and more directly (Pratini, 2018; Morabito 2017).

Fifthly, the administrative time or cost is a problem. Due to very slow processes, simple and repetitive procedures are very cost-intensive. There are several ways to reduce the administration time and costs. One measure would be the establishment of an e-government under the administration of a blockchain. The problem is administrative costs for the authorities. The processes are slow and repeat themselves constantly. The use of a blockchain in this area could make sense and make processes more efficient, help to avoid errors, and provide fraud protection. Denmark and Estonia have made first progress in this area. The targeted use of a blockchain in process optimization can save costs. Through the effectively driven reduction of bureaucracy many millions of euros could be saved annually (Vereinigung der Bayerischen Wirtschaft, 2017).

2.4.2. *Use case 2: Proof of existence and smart contracts*

Organized product and brand piracy is one of the greatest dangers for German industry; in 2016 alone, this resulted in total damage to the German economy of over €41.8 billion (Dierig, 2015). Product piracy is a form of patent infringement, the definition of which corresponds to the provisions of the German Patent Act. Trademark piracy is a colloquial term in which a third party unlawfully uses the legally protected trademark of an owner for commercial purposes (Grigori, 2014).

The main factors that make this fraud possible are in particular the internationally networked processes and supply chains of the global economy (Abele et al., 2011). The basis for this is the low risk of detection of a counterfeit, pirated, or manipulated product due to various inefficiencies of the system (Gausemeier et al., 2012). The main reason for this is the insufficient transparency of process flows (Drawert, 2003). Many companies have no or insufficient information about the procedures and processes of the suppliers of their respective component and system suppliers (Abeyratne and Monfared, 2016). As a consequence, this also allows for inadequate controls of processes and procedures (Abele et al., 2011). This limits the traceability and detectability of errors and deviations in processes (Grummt and Schill, 2009). In addition, there is often a lack of trust between the individual actors (Weber et al., 2016).

To avoid the error factors of product piracy, the creation of transparency and the complete, visible documentation of processes is of decisive importance. However, this turns out to be complex over the entire process flow—from raw materials to the finished end product—across internationally networked process chains. The aim is to be able to check and prove the correct process and transaction sequences at any time and not only to detect infringements by individual actors but also to avoid them in advance (Düring and Fisbeck, 2017). This requires appropriate information and control systems for monitoring. These must take on the task of controlling networked processes in order to detect deviations in deadlines, costs, or performance (Becker et al., 2008).

Today, the control of processes and procedures within the value chains is based on centralized instances that collect and verify data and information (Abeyratne and Monfared, 2016). Each actor, such as supplier, dealer, vendor, and logistics and financial service providers, usually uses its own centralized systems. As a result, documentation and control is only possible within the system of a single actor, which means that the important ability of the various systems to work together seamlessly and across actors is not given (Vatter, 2018). Moreover, in addition to an increased susceptibility to errors, these central storage locations are particularly at risk of fraud due to internal and external influences such as hacker attacks and corrupt employees. In summary, the central organization cannot be made transparent and tamper-proof (Düring and Fisbeck, 2017; Rosenberger, 2018b).

The use of blockchain technology offers a solution to the problems mentioned above. A distributed, consensus-based, and unchangeable ledger ensures that the origin of processes and materials and all subsequent transactions in the processes are monitored. The blockchain generates a formal register that allows identification and tracking (Pilkington, 2016). Specifically, the blockchain has two tasks—that of transaction monitoring and the active mediator role. An overview of the concrete technical functionality of blockchain is shown in Figure 1 and is explained in more detail below.

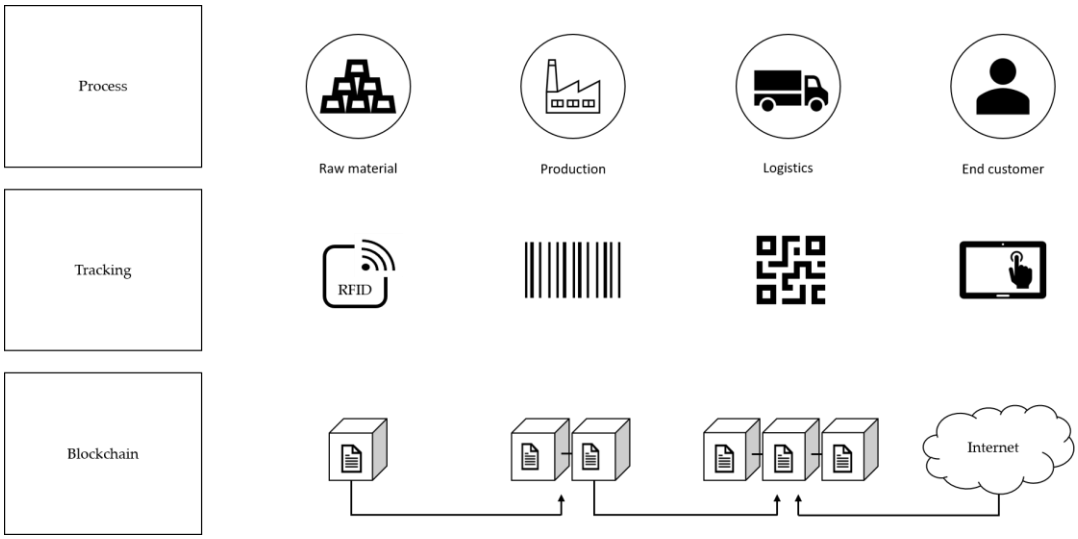

Figure 1. Blockchain for the transaction monitoring of process chains.

From a technical point of view, the blockchain enables the transmission and transfer of information from actor to actor in a fully automated and secure way without the need for intermediaries. Each actor in the chain of transactions (process) has direct access to the complete and non-manipulable transaction register back to the origin of the process. The first actor in the chain starts the process and creates a block, which is stored and verified decentrally on several computers in the distributed computer network. This happens, for example, as soon as the first raw material of a product enters the supply chain. As content in the supply chain (goods, merchandise, information, etc.) is passed on from actor to actor, this verified block is the starting point for the subsequent creation of a chain of blocks. This content is stored again in the distributed network, creating an unalterable transaction history. This chain cannot be changed or manipulated afterward since this would only be possible by changing each chain in the distributed computer network. In the event that a computer within the network should fail, additional copies available on the network ensure that the data are not lost (Aptea and Petrovskyb, 2016; Fraunhofer-Gesellschaft, 2017).

For technical implementation, each of the products in the supply chain is given an "information tag," which connects the actual product with its virtual identity in the blockchain using either a bar and QR code or an RFID and creates a digital product profile. The different actors also have their own digital profile within the blockchain network, which contains its processes, certifications, and requirements (Abeyratne and Monfared, 2016).

By means of "proof of existence" or "proof of work," it can finally be proven that a transaction or an electronic document took place or existed in a certain form at a certain point in time (Crosby et al., 2016).

The solution of transaction monitoring is based on smart contracts. The basis for this is that clear conditions for the cooperation and transaction of goods within a smart contract are defined between the actors within the process chain of the supply chain. The smart contract checks the compliance with the contents of the smart contract by means of an automated computer program and automatically permits the transactions if the specified contractual conditions are met. In this way, it is possible to independently place orders within the supply and process chains and automatically execute disposition decisions (Fraunhofer-Gesellschaft, 2017). For example, a potentially fraud-prone transaction, such as an automatic order triggering, can be prevented if the necessary prerequisites and the type of transaction processing do not meet the specified conditions.

Due to the blockchain architecture, the described functionalities of the blockchain ensure tamper-proof, end-to-end transparency, that is, complete transparency and traceability of events and goods' movements along the entire value and process chain (Düring and Fisbeck 2017). In summary, this use case can be used to prevent fraudulent and manipulative transactions in the supply chain, such as the diversion, counterfeiting, and theft of products or information, and thus the emergence of plagiarism and counterfeiting (Aptea and Petrovskyb, 2016; Pilkington, 2016). In addition, the need for transparency also deters potential fraudsters from entering a supply chain network monitored by blockchain. By setting up a platform service based on blockchain, potential customers are offered the opportunity to register on the platform for a license fee. After registration, these companies can now deposit supply chain information on the platform. This information can be chosen at will, from the identification of the origin and condition of raw materials to the finished product, as each material, part product, or end product is provided with a unique digital profile that contains all relevant information. This can also be understood as an automatic accreditation process since the system is classified as forgery-proof due to its structure. Figure 2 illustrates the above-mentioned functioning of the platform as a digital intermediary and accreditation body.

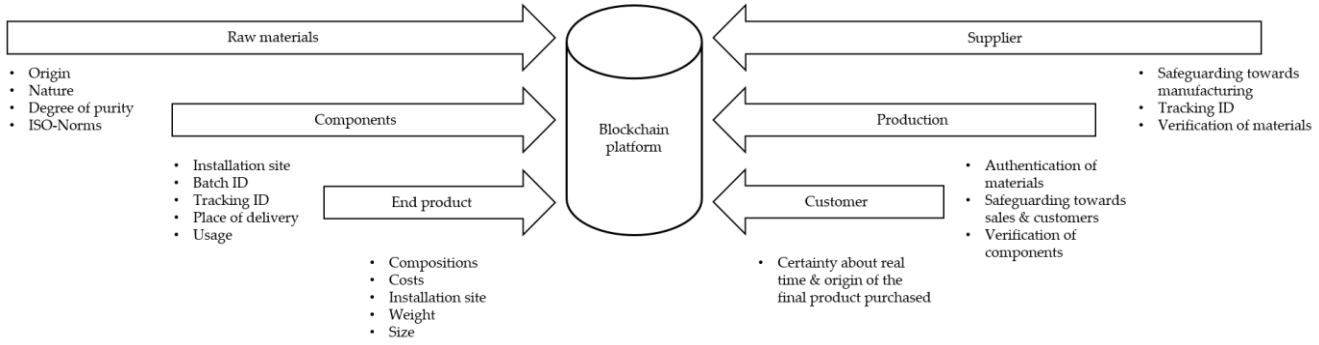

Figure 2. The blockchain platform as protection against fraud along the supply chain.

A manufacturer of luxury watches is used as an example to illustrate how a blockchain platform works. Already during the selection and procurement of the materials necessary to create the watch, both socio-ethical and economic damage can occur. On one hand, it must be ensured that the materials are sourced and mined from certified areas and suppliers qualified for the extraction of mineral resources, and on the other hand, the manufacturer must be certain that the materials are genuine and that they are supplied in full. This information is deposited and stored on the platform by the first link of the supply chain, the supplier. Once the materials have arrived at the production site, the platform can be used to verify that they are available in the contractually agreed quality. If this is the case, the assembly of the watch begins. Since each individual part is stored on the platform with a unique hash value, there is a complete and forgery-proof history of the finished product at the end of production. This history includes all information relevant for the supplier, the manufacturer, and the customer. If the customer now purchases a watch, he can not only validate the authenticity of the product via the assigned ID and registration on the platform but also track the entire previous manufacturing process. This creates a confirmation of the authenticity of the purchased product as well as a guarantee that the recycled materials are obtained from certified and authorized sources.

By depositing the information and the so-called proof of existence on the blockchain-based platform, not only an increased mutual trust between the actors in the supply chain is created but also a comprehensive fraud protection along the entire process, especially in the areas of product piracy and patent infringement. In addition, by setting up smart contracts via the platform, the watch manufacturer is offered the possibility of automatically procuring and reordering spare parts or raw materials. Conversely, depending on the fixed contract period, it gives suppliers an additional security to maintain long-term business relationships with the manufacturer as the automatism of the smart contracts prevents human errors such as forgetting to reorder or ordering too few materials. Conversely, however, the watch manufacturer can also stop or refuse payments to suppliers if there is a breach of contract within the smart contract, such as insufficient material quality or incorrect delivery. Therefore, the platform makes it possible to manage all financial transactions concerning the supply chain—apart from the end customer—in a fraud-proof way.

A further advantage is the automated design of payroll accounting. If payroll payments are linked, for example, to the hours worked, the fulfilment of target goals, or other performance factors, it is possible to adjust the payroll automatically. These are then retrieved in a second step by the companies registered on the platform and can be processed directly in the booking system. This leads to additional security on both the employer and employee sides as individual posting errors or illegally paid wages are prevented.

2.4.3. *Use case 3: Collaboration monitoring*

While on one hand the blockchain can be used to store information about objects (products, raw materials, operating resources) and their references (e.g., existence, ownership, and time of transactions), and on the other hand to control the collaboration of different actors across networked process chains, the potential of the blockchain can also be used specifically to protect the cooperation and coordination of equal actors and the cooperation rules underlying the collaboration (Witt and Richter, 2018).

Within an organization, efficient and cross-departmental cooperation is based on IT systems implemented throughout the organization, such as ERP, CRM, and PPS systems (Rensing and Després, 2017; Erdmann, 2000). However, these systems are increasingly at risk from external IT attacks. According to the Microsoft Security Report for 2017, attacks on corporate systems have increased by 300% worldwide in 2016 alone (Microsoft, 2017).

In addition to the theft of data, these attacks are also aimed in particular at manipulating and disrupting the workflows and processes in companies—and thus error-free collaboration. As an evaluation of the IT attacks that have been taking place since 2013 shows, not only large industrial and digital service companies but also federal authorities are targets for such IT attacks (Wirtschaftswoche, 2016). The trend of transforming centrally managed corporate systems to cloud-based system solutions is increasing, which further increases the security risk for the proper functioning of systems (Ebert and Weber, 2015; Langmann and Stiller, 2017).

The factors that make such IT attacks successful are manifold. In addition to individual, often unintentional, human errors, there are company-specific technical inefficiencies in the respective IT infrastructures (Biener et al., 2015). In general, however, the

following four basic causes can be defined: On one hand, the traditional, centralized database administration and its lack of logical and IT-side separation of different system areas represents a security risk (Rahm, 1994; Mertens et al., 2017). On the other hand, data exchange between systems, such as machine-to-machine communication in manufacturing environments, is a major target for IT attacks (Kafitz, 2009). In addition, a lack of transparency as well as the possibility of controlling and coordinating processes provide a target for manipulation and data theft by fraudulent actors. For a large proportion of users, it is often unclear which data are stored in the systems, who entered the data into the system, at what time, and who has the rights to use and read these data (Tsolkas and Schmidt, 2017; Bauernhansl et al., 2014). To counter these aforementioned inefficiencies, the potential of the blockchain is used in this use case to make the exchange of data between systems, the control of data protection rules, and the access and usage control of systems more secure. Figure 3 shows the structure of a fraud-proof access and usage control of systems by means of blockchain.

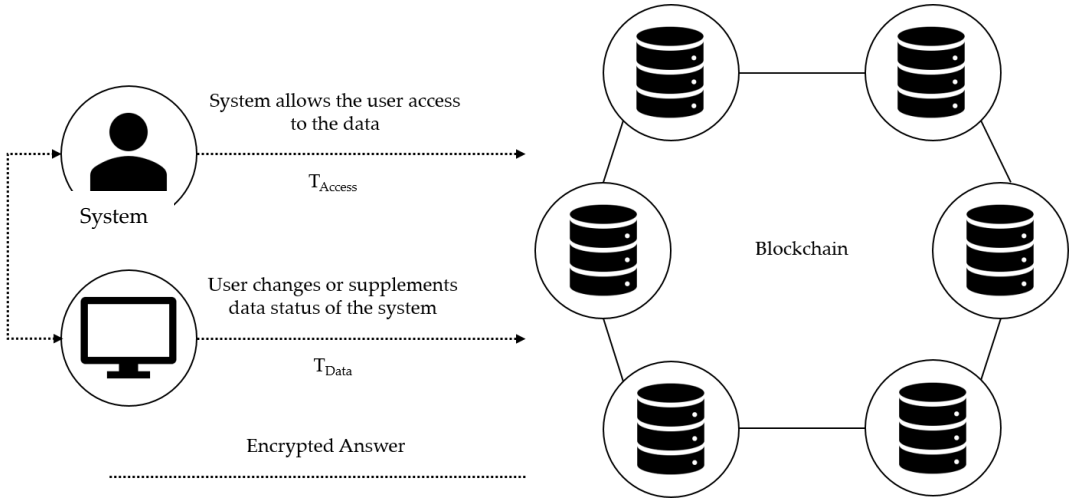

Figure 3. Secure access and usage management with the blockchain.

The basis within the scope of securing access and usage management is to better protect the rights and data of users and thus to increase the security of the systems as a whole. A fundamental distinction must be made between system users and the systems themselves. Users represent potential users of systems, while systems are those applications that secure, manage, and distribute data (e.g., ERP systems). The blockchain itself does not serve as the actual data storage but only stores the access and usage authorizations. The entirety of the data is stored in a memory outside the blockchain, which is implemented via a key-value database that assigns only one data value to a data index (key). Two different transactions are used to store the access authorization in the blockchain. The first transaction is the so-called access transaction, T_{Access}. This transaction is executed when a user (e.g., a system administrator) allows another user to access, use, or change the data or prohibits this user from using the data. The second transaction, called T_{Data}, is executed as soon as the system accesses the data entered or modified by a user. A public key is assigned to each account of a system, which can be traced back to the pseudonym of the account creator. A user installs a new application and confirms the system's policy that the user may use the user's data. Then the transaction T_{Access}, which contains the user's public key, is sent to the system's blockchain. The system can now automatically check with each action whether the user has the rights to change data in the system or to enter new data. If permission is granted, the access or modification of data by the user is logged by the transaction T_{Data} (Zyskind et al., 2015; Wiefling et al., 2017).

Both within and outside the company, the ever-increasing networking of players is creating a wide range of fraud opportunities. The potential of the blockchain in collaboration monitoring can, in comparison to the other use cases, be used primarily for the protection of internal, collaborative processes. When implementing the access management described above, the user organization has the possibility to assign and manage usage, modification and access rights to employees in a fraud-proof way. Thus, the proposed platform solution also creates internal security mechanisms against fraud as employees are deprived of the theoretical possibility of manipulating data internally.

3. Discussion

3.1. Attributes for the protection against fraud of the blockchain platform

In principle, the platform system can be set up in various ways since there are several blockchain protocols that differ in their functionality. Despite this divergence, however, most of these protocols have five similar key attributes, which will serve as the basis for the platform solution in the following. These five similar attributes of otherwise divergent blockchain protocols are access

restriction, transparency, immutability, scalability, and security (Bartoletti et al., 2017) and ensure that the platform is scalable, compliant with corporate policy, flexible in design, and adaptable to new requirements as needed.

The access restriction allows exclusive access exclusively for members registered on the platform, whereby external third parties can be granted access if required. This makes it possible to guarantee an overview of the participating parties and to prevent the manipulation of the data managed on the platform.

Furthermore, every node or access point of the network has the same information because as soon as a block is verified, the information stored in the respective block is stored as a copy in every node. This allows a transparent, access-authorized system.

The data and information once stored in a block or node is cryptographically secured and can only be decrypted with a cryptographic key that is individual for each data record. This encryption ensures that all data stored via the platform has a clear history and thus prevents a lack of data integrity or guarantees that the data is immutable.

Since the platform's network consists of an arbitrarily expandable number of nodes, each providing computing power, the platform system is scalable. The more computers available to the system, the more transactions can be verified and processed via the platform. Based on the above-mentioned aspects of transparency through information equality and access verification of each node, there is no need for a separate synchronization of data.

The security aspect is based on the aforementioned attributes of the platform. The presented attributes transparency, scalability, access restriction and immutability of the data guarantee a secure system compared to conventional data management platforms.

3.2. Structural design of the blockchain platform

Based on the five core attributes of the blockchain platform, a three-level model is suitable for representation. Each level of this model serves a specific purpose, which will be explained in the following.

On the lowest level, the blockchain level, the so-called pointers, or hashes, are managed. These serve to verify the data transactions and thus validate the data integrity. The blockchain level refers to the attributes' transparency through decentralization, the immutability of the stored data, and data integrity. On the middle level, the storage level, the actual data stored on the platform are stored.

This is a relational data management system. This form of data management system consists of tabular blocks, the relation of the individual cells enabling a link to the two connected levels (Meier and Kaufmann, 2016). An important aspect here is that the storage level interacts with the blockchain level through automated hash synchronization. As a result, access by external, non-authorized units is impossible unless these units know the hash value for decrypting the individual data records. The last level to be named—the platform—processes, visualizes, and interacts with the aforementioned storage level by transferring data stored there to a meaningful application from which the data can be retrieved. Figure 4 illustrates this structure.

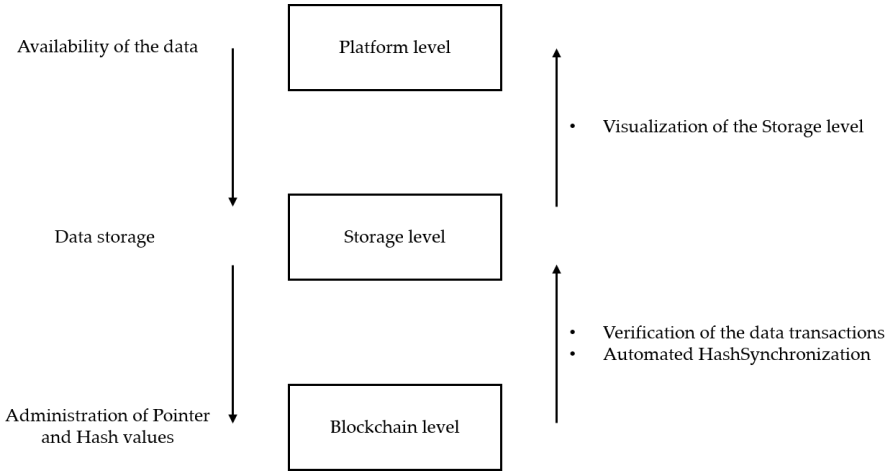

Figure 4. Structural design of the blockchain platform.

As already described, this system is a universally applicable construct that is relatively easy to integrate into the existing structures of a software service company. Thus, the distinctive software competences as well as the comprehensive know-how in the field of IT services are to be regarded as key in the creation of the platform as it is precisely these areas of knowledge that are necessary to create the platform. A further core competence, the computer center, already offers the possibility to store and manage large amounts of data. This means that the storage level of the model only has to be implemented in the data center and that having

to acquire new resources for storing the data stored on the platform is avoided. Furthermore, the interaction of the blockchain level with the other two levels creates a fraud-proof alternative that expands the software service company's competencies in a meaningful way.

3.3. The blockchain platform within the framework of a software service company

The proposed solution of integrating a blockchain platform within the core competencies of a software service company offers many advantages. For example, the networking of the platform with the data center ensures a resource-saving innovation and makes use of the already high security standards of the data center. By integrating the blockchain level, the important core attributes of transparency, decentralization, immutability, and, as a result, increased security in the area of fraud protection are provided for existing and new customers. The following Table 2 concludes by outlining the core aspects of the respective application possibilities. The possibilities of a blockchain-based platform as an additional service offer of the software service provider are manifold.

The current creation, administration, and implementation of contracts offers various fraud possibilities, but the provision of a platform that operates on the blockchain system offers a way to eliminate many of the fraud possibilities presented. Before a contract is concluded, the identities of the contracting parties must be verified. This is done by registering on the offered platform. Here, the user can decide for himself which information is stored and to what extent. After the registration and verification of these user data, the data are stored in the computer center and simultaneously converted into hashes, which are managed on the blockchain level. Since the blockchain operates decentrally, and every node registered in the network receives the same information for filing and storage, the data, once stored, can no longer be falsified or changed.

As already mentioned, these data are cryptographically encrypted and can only be retrieved and used with a matching counter key. This creates an increased sense of security for the contracting parties in two ways. Firstly, each party knows that the other party has also stored its personal information on the platform and thus verified it, thus preventing identity fraud. Secondly, the contracts themselves, which are managed via the blockchain platform, are secured both by cryptographic encryption using hashes and by the information storage on all network nodes. Thus, both the contractual partners, their identities, and the actual contracts are protected against the presented fraud possibilities, which can result in an extraordinarily unique selling point for the existing clientele of the software service provider.

A further advantage of the platform is the verification of data and the conclusion of contracts between institutions and private individuals. For example, if a private person wishes to take out a loan or present a certificate of good conduct, he can, provided the relevant information is contained on the platform, simply transmit it to the institutions by passing it on the hash. The participating institutions can now decrypt the deposited information and no longer have to verify it themselves, as before.

In addition to the existing customers and employees of the software service company, new customers can also benefit from the design of a platform solution. The benefits extend over the entire supply chain, right through to the end customer. Due to the horizontally very far-reaching diversification possibilities, there is still the possibility to comprehensively prevent fraudulent activities. By issuing licenses for the use of the platform and linking these to license fees, further revenue channels are created that build on the already existing core competencies of the software service provider as an IT service provider and software developer. For this reason, the blockchain can be designed as private and permissioned. A public blockchain is not practicable due to the necessity of an identity check and the creation of revenue channels.

Table 2. The attributes of the blockchain platform for a software service company.

	Contract management	**Proof of existence**	**Smart contracts**	**Collaborative processes**
Customer group	Mainly existing customers, such as lawyers Potential to integrate private customers and authorities	Companies Suppliers Producers End customers	Companies Suppliers Producers	Companies (external/internal)
Conditions	Registration on the platform Payment of license fees by users Attitude of authorities toward the blockchain security concept	Registration of the entire supply chain via the platform Payment of license fees by users Willingness to cooperate	Registration of the entire supply chain via the platform Payment of license fees by users Integration of financial transactions via the platform	Registration on the platform Company size and the associated benefits of different platforms (ERP, CRM, etc.) within the company
Blockchain attributes	Transparency Encryption Decentralized management	Transparency Transaction history Verification	Transparency Automation of the transactions Security of the financial data	Transparency Immutability
Protection against fraud opportunities	Contracts Contracting party Identities	Origin Production process Authenticity of the goods	Avoidance of false financial transactions Automatic control of wage and salary statements	Abuse of rights of use Data theft by internal or external parties

4. Summary, further research, and limitations

From the current perspective, numerous questions still need to be clarified for the value-adding use of blockchain technology in organizations, such as legal framework conditions, technical implementation, and sustainability. Basically, a technical and functional connection of blockchain with existing platforms, systems, and databases (e.g., ERP, CRM, PPS systems) is important for the effective use of the technology (Banerjee, 2017). This is also relevant from the point of view of the acceptance of the blockchain technology by the employees of an organization—the linking of new technologies with existing systems and databases is a decisive factor of technology acceptance (Ortmann and Guhlke, 2014).

Smart contracts enable protection against fraud in many areas of application, and they also form the basis for DAOs and crypto currencies (Voshmgir, 2016). Transaction monitoring is also the basis for fraud protection with crypto currencies. Therefore, it makes sense not to consider the application areas and potentials of the blockchain separately, but to take an integrated approach from the beginning. Otherwise, synergy effects in particular will remain unused in the development of blockchain solutions. However, the high additional investment costs are problematic in this context as they have to be incurred in addition to the already very high basic investment costs for system programming, building up computer capacities, and embedding and linking to other systems (Thiele, 2016).

Furthermore, the value-adding use of blockchain technology in organizations is currently not yet possible due to the lack of a legal and regulatory framework (Rosenberger, 2018a). KPMG's legal department concluded in 2017 that almost all legal questions regarding the regulatory classification of blockchain are still unresolved. For example, it is not clear who is liable for technical

problems within a given blockchain or for hacker attacks on the blockchain in general. For example, it must be clarified which processes will be used in the case of reversals due to uncovered unauthorized transactions and to what extent guarantee regulations will be designed (KPMG Law, 2017).

Finally, blockchain itself is not fully protected against manipulation and hacker attacks despite the potential shown in the use cases. As the momentous attack on one of the most frequently used crypto currencies, Ethereum, in 2017 shows, hacker attacks on e-wallets are possible, especially with crypto currencies (Holtermann, 2017). Furthermore, blockchain prevents the subsequent manipulation of information and data records, but the information fed into blockchain can also be manipulated or incorrect. To ensure that the information fed into blockchain is correct, intermediaries could again be important to verify the correctness of the data (Karabasz, 2018).

These mentioned problems hinder the implementation and realization of a blockchain-based platform solution. Especially without a legal framework, smart contracts do not offer any added value since the written code is not binding. Thus, although mediation on the platform would be an innovation, it would not be legally binding. Although the technical conditions and know-how for such a platform can be built up internally, an actual application is therefore not yet in sight.

However, many companies, experts, and even studies describe the blockchain technology as one of the most significant innovations of the present era after the invention of the internet (Samit, 2017). There are many reasons for this, such as the way it works and the technology behind blockchain—the decentralization, the consensus mechanism, the verification by cryptography, and the automatic update of each block. The combination of these technologies makes it possible to use blockchain in a huge range of applications. Whether in classical areas, such as the public sector, or in newer ones, such as IoT, there are already numerous applications in use today. When talking about blockchain, it is important to mention that Bitcoin or crypto currencies are not the blockchain; rather, crypto currencies are an application of the blockchain.

In contract management, blockchain enables the resolution of many previous fraud possibilities and cost factors. Both the identity of the contract partners can be recorded and stored decentrally, and the location of the contract can be stored in blocks.

Especially with regard to product and brand piracy, end-to-end transparency, from raw material to end product, is important. Due to its decentralized nature and tamper-proof storage of data and complete traceability, blockchain also offers enormous potential here. In combination with smart contracts and contract management, it is thus possible to store not only the contracts but also the products stored in the contracts in a fraud-proof manner. If these application scenarios are extended by IT systems, CRM, ERP, etc. can also be protected against IT attacks by the blockchain. It is apparent that the individual categories must not be considered in isolation as there are many interfaces and overlaps. Thus, when implementing the blockchain technology, it is possible to consider several areas at once. Only in this way can a comprehensive overall solution be achieved.

The platform solution developed within the scope of this paper combines the potentials of blockchain with the previously described use cases. Using the example of the software service company, new target groups, such as the end customer himself, can be enabled to interact with this platform in addition to existing customer groups. This can be integrated into existing structures and is based on a three-level model (blockchain, storage, and platform level). The existing, comprehensive know-how of a software service company in the field of IT services can be used as a key factor in platform development. The data center forms the storage level of the model. By implementing a blockchain level that interacts with the other two levels, a fraud-proof software solution is created for a broad customer base.

Based on the results of this elaboration, the next step is to program a prototype of the platform in practice and to integrate it into the structures of the using company (e.g., into the computer center of the software service company) according to the tripartite structure. In particular, the usability of the platform with a specific customer focus group (e.g., lawyers or tax advisors) should also be considered to verify both the actual benefit of the platform with regard to fraud protection and the monetary benefit of the platform on the basis of the individual application possibilities.

Despite the large number of potentials, many questions are still open that do not yet allow for the unrestricted use of the blockchain technology. Legal and regulatory frameworks still need to be created, both at the national and international levels. Although blockchain has been tamper-proof up to now, there is no guarantee that it will remain so in the future. In the past, there have been successful attacks on the weak points of blockchain, such as users' e-wallets. As long as blockchain acts in the interface of systems, these interfaces (apps, devices, IT systems, websites) must also be secured and further developed. This is also where the need for further research lies—because not only must the blockchain be secure but also the interfaces, platforms, and systems used in this context. Likewise, it cannot be guaranteed that the blockchain technology can be manipulated in the future by more powerful servers and computers.

References

Abele, E., Kuske, P. & Lang, H. (2011). Produktpiraterie im Maschinenbau – Herausforderung im 21. Jahrhundert. In: *Schutz vor Produktpiraterie* (pp. 2-21). Berlin, Heidelberg: Springer Berlin Heidelberg.

Abeyratne, S. & Monfared, R. (2016). Blockchain ready manufacturing supply chain using distributed ledger. *International Journal of Research in Engineering and Technology*, 5(9), pp. 1-10.

Aptea, S. & Petrovskyb, N. (2016). Will blockchain technology revolutionize excipient supply chain management?. *Journal of Excipients and Food Chemicals*, 7(3), pp. 76-78.

Banerjee, A. (2017). Integrating Blockchain with ERP for a Transparent Supply Chain. URL: https://www.infosys.com/oracle/white-papers/documents/integrating-blockchain-erp.pdf (last accessed 24 June 2018).

Bartoletti, M., Lande, S., Pompianu, L. & Bracciali, A. (2017). A general framework for blockchain analytics. In: *Proceedings of the 1st Workshop on Scalable and Resilient Infrastructures for Distributed Ledgers*, pp. 1-6.

Bauernhansl, T., Hompel, M. & Vogel-Heuser, B. (2014). *Industrie 4.0 in Produktion, Automatisierung und Logistik. Anwendung, Technologien, Migration,* Wiesbaden: Springer Vieweg.

Becker, J., Knackstedt, R. & Pfeiffer, D. (2008). *Wertschöpfungsnetzwerke. Konzepte für das Netzwerkmanagement und Potenziale aktueller Informationstechnologien.* Heidelberg: Physica-Verlag Heidelberg.

Biener, C., Eling, M., Matt, A. & Wirfs, J. H. (2015). *Cyber risk. Risikomanagement und Versicherbarkeit.* St. Gallen: Institut für Versicherungswirtschaft der Universität St. Gallen.

Blockgeeks (2018). Basic Primer: Blockchain Consensus Protocol. URL: https://blockgeeks.com/guides/blockchain-consensus/ (last accessed 19 June 2018).

Brandon, D. (2016). The blockchain: The future of business information systems?. *International Journal Of The Academic Business World*, 10(2), pp. 33-40.

Bridgers, A. (2017). Will workplaces be going off the rails on the blockchain?. *Journal Of Internet Law*, 20(11), pp. 3-6.

Condos, J., Sorrell, W. H. & Donegan, S. L. (2016). Blockchain Technology: Opportunities and Risks. URL: https://legislature.vermont.gov/assets/Legislative-Reports/blockchain-technology-report-final.pdf (last accessed 28 June 2018).

Coyne, J. G. & McMickle, P. L. (2017). Can Blockchains Serve an Accounting Purpose?. *Journal of Emerging Technologies in Accounting*, 14(2), pp. 101-111.

Crosby, M., Pattanayak, P., Verma, S. & Kalyanaraman, V. (2016). BlockChain Technology: Beyond Bitcoin. *Applied Innovation Review,* (2).

Dai, J., Yunsen, W. & Vasarhelyi, M. A. (2017). Blockchain: An Emerging Solution for Fraud Prevention. *CPA Journal*, 87(6), pp. 12-14.

Deloitte (2017). Cyber-Security Report 2017 – Teil 2: Cyber-Risiken in Unternehmen. URL: https://www2.deloitte.com/content/dam/Deloitte/de/Documents/risk/RA-Risk-Advisory-Cybersecurity-Report-2017-2-14122017-s.pdf (last accessed 29 June 2018).

Diering, C. (2015). Gefälschte Produkte können lebensgefährlich sein. URL: https://www.welt.de/wirtschaft/article148270435/Gefaelschte-Produkte-koennen-lebensgefaehrlich-sein.html (last accessed 29 June 2018).

Drawert, S. (2003). Supply Chain Controlling: Strategy, Conception and integrated Tools for the Supply Chain Performance Analysis and Optimization. URL: https://redaktion.brainguide.de/upload/publication/d4/10tp5/03e192e300c40b568416eec63b3d8130_1311535203.pdf (last accessed 29 June 2018).

Düring, T. & Fisbeck, H. (2017). Einsatz der Blockchain-Technologie für eine transparente Wertschöpfungskette. In: Hildebrandt A. & Landhäußer W. (Eds.). *CSR und Digitalisierung. Der digitale Wandel als Chance und Herausforderung für Wirtschaft und Gesellschaft* (pp. 449-464). Berlin, Heidelberg: Springer Gabler.

Ebert, N. & Weber, K. (2015). Sicherheit von Cloud-basierten Plattformen zur Anwendungsintegration: eine Bewertung aktueller Angebote. *FHWS Science Journal*, 3(2), pp. 10-23.

Erdmann, J. (2000). Integriertes Prozeßmanagement: ein multidimensionaler Ansatz für das Management von Prozessen in Unternehmen: Entwicklung eines integrierten Prozeßmanagementansatzes und Entwurf einer für den Ansatz adäquaten Informationsarchitektur. Hannover: Norderstedt: Libri Books on Demand.

Fraunhofer-Gesellschaft (2017). Blockchain und Smart Contracts. Technologien, Forschungsfragen und Anwendungen. URL: https://www.fraunhofer.de/content/dam/zv/de/forschung/artikel/2017/Fraunhofer-Positionspapier_Blockchain-und-Smart-Contracts_v151.pdf (last accessed 29 June 2018).

Gausemeier, J., Glatz, R. & Lindemann, U. (Eds.) (2012). *Präventiver Produktschutz. Leitfaden und Anwendungsbeispiele.* München: Hanser.

Guo, Y. & Liang, C. (2016). Blockchain application and outlook in the banking industry. *Financial Innovation*, 2(24).

Grigori, K. M. (2014). *Prävention und Bekämpfung von Marken- und Produktpiraterie. Leitfaden für Analysen, Ermittlungen und Schutzstrategien.* Wiesbaden: Springer Gabler.

Grummt, E. & Schill, A. (2009). Datensicherheit trotz transparenter Güterströme. Kooperative Zugriffskontrolle für den Lieferketten-übergreifenden Einsatz automatisch erfasster Produktdaten. *Wissenschaftliche Zeitschrift der Technischen Universität Dresden,* 58(1-2), pp. 103-107.

Holtermann, F. (2017). Hackerangriff auf Ethereum. Sieben Millionen Dollar in drei Minuten. URL: https://www.handelsblatt.com/finanzen/maerkte/devisen-rohstoffe/hackerangriff-auf-ethereum-sieben-millionen-dollar-in-drei-minuten/20080278.html (last accessed 24 June 2018).

Kafitz, W. (2009). Sicherheit und Plagiatsschutz beim automatisierten Datenaustausch. *ZWF,* 104(6), pp. 513-517.

Karabasz, I. (2018). Auch die Blockchain bietet keine absolute Sicherheit. URL: https://www.handelsblatt.com/meinung/kommentare/kommentar-auch-die-blockchain-bietet-keine-absolute-sicherheit/22672752.html?ticket=ST-1757069-9jYxeRdUNUu6RkWprz2b-ap6 (last accessed 26 June 2018).

Kewell, B., Adams, R. & Parry, G. (2017). Blockchain for good?. *Strategic Change*, 26, pp. 429-437.

KPMG (2017). E-Crime in der deutschen Wirtschaft 2017. pp. 17-22.

KPMG Law (2017). Blockchain: Bisher noch fast alle juristischen Fragen offen. URL: www.kpmg-law.de/mandanten-information/blockchain-bisher-noch-fast-alle-juristischen-Fragen-offen/ (last accessed 25 June 2018).

Langmann, R. & Stiller, M. (2017). Industrial Cloud – Status und Ausblick. In: S. Reinheimer (Ed.). *Industrie 4.0. Herausforderungen, Konzepte und Praxisbeispiele* (pp. 29-47). Wiesbaden: Springer Vieweg.

Meier, A. & Kaufmann, M. (2016). *SQL- & NoSQL-Datenbanken*. Berlin, Heidelberg: Springer Berlin Heidelberg.

Mertens, P., Bodendorf, F., König, W., Schumann, M., Hess, T. & Buxmann, P. (2017). *Grundzüge der Wirtschaftsinformatik*. 12th edition. Berlin: Springer Gabler.

Microsoft (2017). *Microsoft Security Intelligence Report*. 22nd edition. Microsoft Security.

Morabito, V. (2017). *Business Innovation Through Blockchain - The B³ Perspective*. Cham: Springer.

Ortmann, U. & Guhlke, B. (2014). Leitfaden Technologieakzeptanz. Konzepte zur sozial- und humanverträglichen Gestaltung von Industrie 4.0. URL: https://www.uni-bielefeld.de/soz/las/TA/itsowl/dokumente/itsowl-TA_Meilenstein_3.pdf (accessed 28 June 2018).

Pilkington, M. (2016). Blockchain technology: principles and applications. In: F.-J. Olleros and M. Zhegu (Eds.). *Research handbook on digital transformations* (pp. 225-253). Cheltenham, UK, Northampton, MA, USA: Edward Elgar Publishing.

Pratini, N. (2018). Identity, privacy, and the blockchain. URL: https://fin.plaid.com/articles/identity-privacy-and-the-blockchain (last accessed 7 June 2018).

Rahm, E. (1994). *Mehrrechner-Datenbanksysteme*. *Grundlagen der verteilten und parallelen Datenbankverarbeitung*. 1st edition. Bonn: Addison-Wesley-Verlag.

Rensing, C. & Després, L. (2017). Leitfaden Groupware Systeme. Zusammenarbeit über zeitliche und räumliche Distanz unterstützen. URL: http://www.httc.de/fileadmin/httc/images/AgenturKommunikation/Leitfaden-Groupware-Systeme.pdf (last accessed 28 June 2018).

Rosenberger, P. (2018a). Ausblick. In: *Bitcoin und Blockchain* (pp. 129-148). Berlin, Heidelberg: Springer Berlin Heidelberg.

Rosenberger, P. (2018b). Innovationstreiber Blockchain. In: *Bitcoin und Blockchain* (pp. 63-75), Berlin, Heidelberg: Springer Berlin Heidelberg.

Samit, J. (2017). 4 Technology Trends That Will Transform Our World in 2018. URL: http://fortune.com/2017/12/26/4-technology-trends-2018/ (last accessed 30 June 2018).

Schlatt, V., Schweizer, A., Urbach, N. & Fridgen, G. (2016). Blockchain: Grundlage, Anwendungen und Potenziale. Projektgruppe Wirtschaftsinformatik des Frauenhofer-instituts für Angewandete Informationstechnik FIT. URL: https://www.fit.fraunhofer.de/content/dam/fit/de/documents/Blockchain_WhitePaper_Grundlagen-Anwendungen-Potentiale.pdf (last accessed 30 June 2018).

Schütte, J. et al. (2017). BLOCKCHAIN UND SMART CONTRACTS – Technologien, Forschungsfragen und Anwendungen. URL: https://www.iuk.fraunhofer.de/content/dam/iuk/de/documents/Fraunhofer-Positionspapier_Blockchain-und-Smart-Contracts.pdf (last accessed 30 June 2018).

Thiele, C.-L. (2016). Blockchain-Technologie positiv gegenüberstehen. URL: https://www.bundesbank.de/Redaktion/DE/Themen/2016/2016_11_11_blockchain_technologie.html (last accessed at 23 June 2018).

Tsolkas, A., & Schmidt, K. (2017). *Rollen und Berechtigungskonzepte. Identity- und Access Management im Unternehmen*. 2nd edition. Wiesbaden: Springer Vieweg.

Underwood, S. (2016). Blockchain beyond Bitcoin. *Communications of the ACM*, 59, pp. 15-17.

Vatter, P. (2018). Anwendungsmöglichkeiten der Blockchain-Technologien (Vorlesung). *FOM Hochschule für Ökonomie & Management, Nürnberg.*

Vereinigung der Bayerischen Wirtschaft (2017). Bürokratiekosten und neue Wege zur Vermeidung von Bürokratie. URL: https://www.vbw-bayern.de/Redaktion/Frei-zugaengliche-Medien/Abteilungen-GS/Recht/2017/Downloads/Studie-B%C3%BCrokratiekosten-vbw-April-2017.pdf (last accessed 24 June 2018).

Verizon (2017). 2017 Data Breaches Investigation Report. pp. 24-25.

Voshmgir, S. (2016). Blockchain, Smart Contracts und das Dezentrale Web. URL: https://www.technologiestiftung-berlin.de/fileadmin/daten/media/publikationen/170130_BlockchainStudie.pdf (last accessed 24 June 2018).

Weber, I., Xu, X., Riveret, R., Governatori, G., Ponomarev, A. & Mendling, J. (2016). Untrusted Business Process Monitoring and Execution Using Blockchain. In: *International Conference on Business Process Management*, pp. 329-347. Springer, Cham.

Wiefling, S., Lo Iacono, L. & Sandbrink, F. (2017). Anwendung der Blockchain außerhalb von Geldwährungen. *Datenschutz Datensicherheit – DuD,* 41(8), pp. 482-486.

Wirtschaftswoche (2016). Cyber-Krieg. Die größten Hacker-Angriffe aller Zeiten. URL: https://www.wiwo.de/technologie/cyber-krieg-die-groessten-hacker-angriffe-aller-zeiten/7814454.html (last accessed 21 June 2018).

Witt, J. & Richter, S. (2018). Ein problemzentrierter Blick auf Blockchain- Anwendungsfälle. *Tagungsband Multikonferenz Wirtschaftsinformatik*, pp. 1247-1258.

Yermack, D. (2017). Corporate Governance and Blockchains. *Review of Finance,* 21(1), pp. 7-31.

Zyskind, G., Nathan, O. & Pentland, A. (2015). Decentralizing Privacy: Using Blockchain to Protect Personal Data. *2015 IEEE Security and Privacy Workshops (SPW)*, San Jose, CA, pp. 180-184.