International Journal of Applied and Physical Sciences
volume 7 pp. 1-9 doi: https://dx.doi.org/10.20469/ijaps.7.50001

Hype or Horror – Potentials and Hurdles of Blockchain Technology based on Legal Framework Conditions in Germany

Wanja Wellbrock*
Heilbronn University of Applied Sciences,
Schwäbisch Hall, 74523, Germany

Cathrin Hein
Frankfurt University of Applied Sciences,
Frankfurt, 60318, Germany

Christoph Hein
DB Systel GmbH, Frankfurt, 60329, Germany

Daniela Ludin
Heilbronn University of Applied Sciences,
Schwäbisch Hall, 74523, Germany

Abstract: This article summarizes the current status of the legal challenges facing the blockchain technology in Germany. Similar to the world wide web, blockchain represents a kind of basic technology on which new platforms and business models can be created. However, the question arises whether the German legal system is fundamentally capable of meeting the challenges posed by such decentralized technology. In particular concerning criminal offences or the new basic data protection regulation. It is questionable how the current negative headlines (e.g., silk road) will affect cryptocurrencies in the long term and, as a result, possibly also blockchain technology, not only concerning illegal content such as child pornography.

Keywords: *Blockchain, legal framework, data protection, reverse transactions*

Received: 28 October 2020; ***Accepted:*** 25 December 2020; ***Published:*** 25 March 2021

I. INTRODUCTION

The blockchain technology is often described as biggest opportunity set we can think of over the next decade [1]. Others see the potential: What the internet did for communications, blockchain will do for trusted transactions [2]. Still, others exaggerate when they celebrate blockchain as a technology that will revolutionize our whole way of thinking [3]. However, what is this supposedly revolutionary technology all about?

Blockchain is a basic technology on which new platforms and business models can be created [4]. The best-known use case of blockchain technology is probably the cryptocurrency Bitcoin. In 2008, an unknown person or group published the white paper "Bitcoin: A peer-to-peer electronic cash system" [5] as a blueprint for digital currency under the pseudonym Satoshi Nakamoto [4]. This is often seen as the digital community's reaction to the global financial crisis, in the wake of which banks had suffered a massive loss of confidence. Digital currencies based on blockchain technology do not require any intermediaries in the transactions [6].

By definition, blockchain is a decentralized database consisting of an ever-growing list of data records that are stored on different computers. The transactions are grouped in blocks and the checksum of the previous block is always included as a validation feature. This technique is also known as distributed ledger technology [7].

The question here is whether the German legal system is fundamentally capable of meeting the challenges posed by this distributed technology. So far, there are no concrete legal regulations in Germany regarding blockchain. Other countries are further along in this respect. In Thailand, a law for handling cryptocurrencies came into force on 13th of May 2018 [8]. The US state of Michigan has

*Correspondence concerning this article should be addressed to Wanja Wellbrock, Heilbronn University of Applied Sciences, Schwabisch Hall, 74523, Germany. E-mail: wanja.wellbrock@hs-heilbronn.de

presented a draft law after it became a criminal offence to change records stored using distributed ledger technology [9]. The US state of Tennessee legally defines blockchain technology as follows:

Blockchain technology means distributed ledger technology that uses a distributed, decentralized, shared, and replicated ledger, which may be public or private, permissioned or permission less, or driven by tokenized crypto economics or token less. The data on the ledger is protected with cryptography, is immutable and auditable, and provides an uncensored truth [10, 11].

A study by RWTH Aachen and Goethe University Frankfurt also raises the question of whether users of a blockchain network can be held responsible for illegal content. The study analyzed the non-financial content of the Bitcoin blockchain and discovered links to child pornography. By definition, every user of the Bitcoin blockchain has a copy of all data records on the computer used and could, therefore, be liable to prosecution.

It is undisputed that legal aspects will play a major role in the future in the environment of blockchain-based applications. To deal with the legal challenges for private individuals and companies, it is therefore inevitable that you acquire a basic understanding of the underlying technology and are aware of the legal risks and uncertainties of its use.

II. BLOCKCHAIN-TECHNOLOGY

Bitcoin is considered to be the origin of blockchain technology. The technological cornerstones of the system are derived from this. It is a decentralized network within which an artificially limited amount of tokens is generated. While these tokens can be assigned to a user, the user remains anonymous. Like banks in the real world, a central instance was always needed before Bitcoin to control transactions and prevent double-spending. A unit of cryptocurrency may only be used once, just like a check in the old days [4].

Within a blockchain, all transaction data is stored, and new transactions are continuously compared with the existing transaction history to check whether a value has already been issued before [12].

The basis of blockchain-based applications is the decentralized structure of the network. While a centralized network has a corresponding instance that manages and controls the transactions made, a decentralized network dispenses with just that control instance and enables direct communication between the participants, with each participant having access to the uniform data stock at all times. Such networks cannot be controlled from the outside (see Fig. 1) [4].

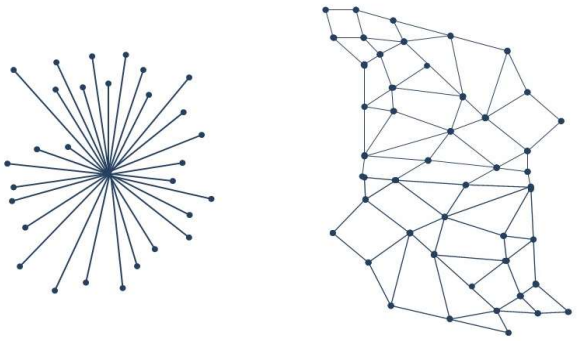

Fig. 1. Centralized vs. decentralized network structure

Blockchain networks are not only designed for the transmission of cryptocurrencies. For example, sales contracts can also be documented within the framework of smart contracts, since all transactions are publicly traceable. This is also known as the Internet of Value, in which every transfer of goods can be mapped [13].

For this purpose, the assets within the network are initially defined, listed and assigned to the owners. For these assets, the respective owners receive so-called tokens. These tokens represent the ownership of the respective asset and thus effectively prevent double-spending [4].

In the absence of a central authority, all participants of a blockchain have the same legitimation within the network. Each participant has theoretically stored the entire transaction history. As this already amounts to 147 GB (as of December 2017) at Bitcoin, for example, a distinction is now made between so-called lightweight nodes and full nodes. The former only store the relevant part of the blockchain, while the latter store the entire database.

The starting point for participation in the Bitcoin network is the so-called Wallet. However, the wallet is not

a wallet in the true sense of the word but only serves to manage the blockchain account. The address of the wallet is pseudonymized and serves the account management and the sending and receiving of transactions. The transactions are encrypted using public key procedures, which ensures that only authorized participants carry out transactions [5, 7, 12, 14].

Using the Bitcoin-blockchain as an example, the transactions primarily contain information about the origin and recipient of the Bitcoins. The special feature here is that no Bitcoins may remain in the source. If you have twenty Bitcoins and only want to transfer five of them to another user, you have to transfer the remaining fifteen Bitcoins yourself. Otherwise, the difference would be lost as a transaction fee for the user. The complete data set is sent to the other users of the network and is initially buffered until it is finally included in a block [13, 15].

All transactions within the blockchain are stored in blocks. In the Bitcoin blockchain, for example, they comprise approximately 900 to 2,500 transactions per block. Before being included in a block, the transactions are validated to prevent Bitcoins that have already been output from being output again. This creates the unchangeable transaction chain, the hallmark of the blockchain [13, 12, 16].

The so-called miners–computers that provide the network with computing power–close the blocks, calculate the mathematically generated identification number and link the block to the previous block in the chain (see Fig. 2). The determination of this unique fingerprint requires a high level of computing power due to the high number of leading zeros, so-called nonce. This process ensures data integrity in the blockchain and makes it impossible to change the transactions afterwards [7, 13, 12, 15, 16, 17, 18].

The network participants are often distributed worldwide, which results in differences in the transmission speed of the data. This can lead to imbalances in the data stock and it is not always guaranteed that all data is updated simultaneously at all participants. To counteract this, only the longest chain of blocks should always be accepted as valid [19].

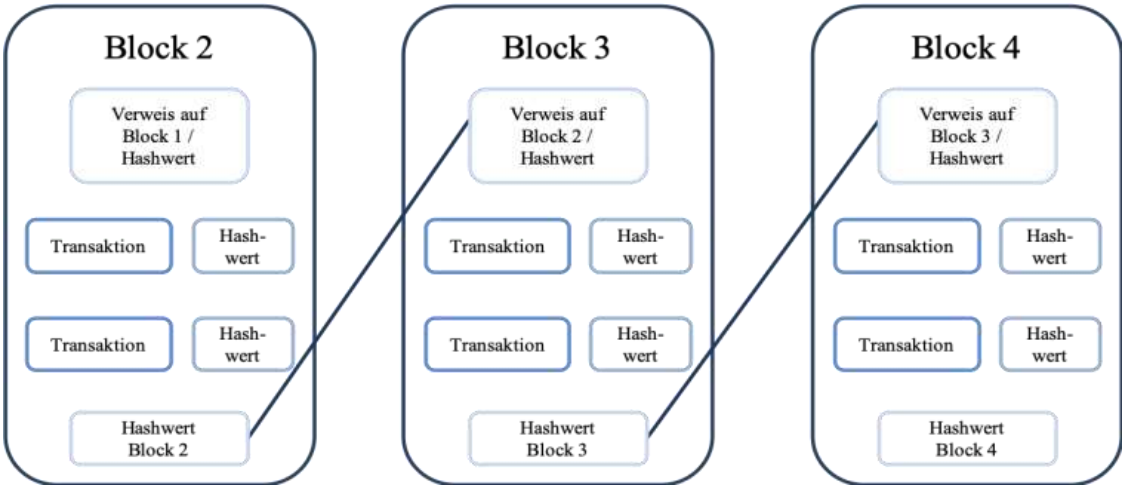

Fig. 2. Principle of the blockchain technology [7]

The provision of computing power by the miners costs time and money and is paid in two ways within the Bitcoin-blockchain. On the one hand, a transaction fee is charged by the miners for inclusion in a block, and on the other hand, new Bitcoins are generated in each new block, which the respective miner receives as compensation [13, 20, 21].

Not all blockchains are the same. There are different approaches based on this technology. One variant is private networks where it is not possible to join the closed circle of participants without further ado. An example is Hyperledger, an initiative that develops blockchain applications for companies [22].

In contrast, public blockchain applications are open to everyone and do not require any special permission, for example, the already mentioned Bitcoin or Etherum. Etherum is not only used for the exchange of cryptocurrency, but is also a smart contracts platform [7].

Blockchain applications require a fast internet connection and high computing power. The latter causes immense costs, especially due to power consumption, which is also one of the biggest criticisms of blockchain technology. At the same time, it is also the greatest protection against manipulation. Theoretically, only 51% of the computing capacity would have to be controlled within a blockchain and the application could then be

manipulated at will. However, because of the high cost of providing the computing capacity, it is usually more lucrative to simply use it as a miner and receive Bitcoins in return [5, 16].

Despite the low residual risk of hacking, blockchain technology ensures a high-security standard because the data is distributed decentrally, accessible to all users and encrypted. The absence of intermediaries, such as banks, allows faster processing and, especially in regions with a less developed legal system, enables contracts or transfers to be executed correctly and securely [16].

The underlying technology enables secure transaction processing and mutual trust between the contracting parties is not necessary. The entire transaction history is displayed in a comprehensible manner and users can view it at any time. In addition, blockchain networks work autonomously, which means that external influences have no effect on the network [7, 16].

A. *Child pornography as an example of the need for legal action*

At the beginning of this article, we have already referred to the links found to child pornographic material within the Bitcoin network [23]. This is mainly done via special transaction types or note fields of standard transactions [4]. Since all transaction data is continuously and unalterably stored within a blockchain and is accessible to every user, the question arises as to whether the mere storage of the transaction history, which is a prerequisite for access to the network, is equivalent to the criminal possession of child pornography according to 184b para. 3 StGB. However, the provision of the data for retrieval on a server is usually not sufficient as a criminal offence [24]. However, amendments to the StGB are currently being discussed in the German Parliament, after the fact that even retrieval via radio or Telemedia would be punishable [25]. Therefore, changes are to be expected in the future.

The facts of the case are different for the element of the crime of intent according to 15 StGB. In this case, knowledge and will of the realization of the offence are assumed [26]. It seems questionable to assume intentional action if the original purpose of the trade with the cryptocurrency Bitcoin is the purpose of the trade. Precisely because it would declare the mere, use of the network a criminal offence since illegal content could be located somewhere within the network. However, if such a reading were to prevail, there would hardly be any practical use cases for the technology.

The question remains whether the miners will play a different role in this process from a criminal law perspective. They would be accomplices within the meaning of 25 (2) StGB if they were complicit in the dissemination and made the data accessible to a larger circle of people who could no longer be controlled [26]. Although they make their computing power available to the network and contribute significantly to the dissemination of the data by closing the blocks, they do not check the transactions in terms of content and thus have no responsibility for the transactions of the users and cannot influence them. Centralized control of the content would undermine the actual purpose of the network, for example, the decentralized exchange of cryptocurrency. The intention according to 15 StGB cannot be assumed either. The purpose of the network is the trade with crypto-currency and the motivation to participate for the miners is financial.

Illegal contents within blockchain transactions represent a new set of circumstances, which has not yet been sufficiently analyzed from a legal point of view. The legislator should create a framework to provide legal security for the average user.

B. *Data protection aspects of blockchain technology*

The basic data protection regulation in force for the EU member states since May 2018 must also be applied in Germany for the processing of personal data. According to Art. 4 No. 1 DS-GVO, personal data is any information relating to an identified or identifiable natural person« and allows identification without the use of other sources of information. However, it must be clarified in advance whether a public blockchain contains such data at all or whether it is rather anonymous information where data subjects can no longer be identified.

Within a blockchain network, pseudonyms are used instead of clear names, which makes it impossible to identify the respective natural persons directly [12]. However, the person is still identifiable under Art. 4 No. 1 DS-GVO if it is possible to draw conclusions about the natural person by linking the pseudonym with other data. It is therefore questionable whether the address of a user in a blockchain is considered a pseudonym and the DS-GVO would be applicable or whether, due to the encryption mechanisms, the data is already anonymous and therefore data protection law does not apply. The address of a user in the Bitcoin network is generated by means of a hash function and is in principle to be regarded as pseudonymization since the establishment of a personal reference for the future cannot be ruled out.

According to relative theory, the identification of natural persons by third parties is very broad and anonymization is almost impossible. However, it is not possible to clearly identify a responsible person within a blockchain

network within the meaning of the DS-GVO. From this point of view, the absolute theory would have to be applied and, consequently, the possibilities that a third party could use for identification would have to be considered. It is therefore questionable what means another person is likely to use, according to the general judgement, to identify the person behind the pseudonym. Technological progress and the proportionality between necessary effort and the interest in identification must be taken into account [27]. If, for example, health data were to be stored in encrypted form in the blockchain, a greater interest in identification could be assumed than, for example, with less sensitive data.

By linking Bitcoin transactions to the user's IP address, conclusions can be drawn about the user's financial circumstances and behavior, thus leading to a deanonymization of the person behind the transaction [13, 28]. In addition, the identity can be determined by linking to additional information, such as the purchase in an online shop and the resulting delivery address [28]. A blockchain always has a complete profile of all users and their transactions. Using the Bitcoin blockchain as an example, all financial transactions are archived without any gaps. If a person publishes their Bitcoin address, it is possible to track all payment transactions of this person. For example, Wikileaks has published its own Bitcoin address to generate donations. By publishing the address, it is possible to analyze all transactions of this address and to draw conclusions about the financial situation of Wikileaks. This traceability can be an advantage when generating donations. For natural persons, however, this is rather a risk that can only be counteracted by the already mentioned use of constantly new keys for transactions. Otherwise, such profiling cannot be prevented, and conclusions can be drawn about financial circumstances within the Bitcoin system or other blockchain networks. Whether personal data are processed therefore depends in particular on the interests and technical possibilities of the person responsible or another person [29].

According to Art. 4 No. 7 DS-GVO, the controller is "the natural or legal person [...] who alone or jointly with others determines the purposes and means of the processing of personal data". This is intended to assign responsibility to a body, inter alia for compliance with data protection provisions. However, a blockchain network is characterized in particular by its decentralized structure and the absence of centralized responsibility.

In practice, control by the miners would considerably impair trust in the network and its security. Miners within the Bitcoin system therefore always ensure on their own initiative that they do not exceed the 51% limit. Joint responsibility of the miners must be rejected [30]. The miners can only summarize the transactions and calculate hash values, but cannot change the corresponding data, which means that they cannot be held responsible for any personal data that may be contained. In principle, there is no possibility for all members of the blockchain network to delete individual transactions. The individual user cannot create or influence transactions for others, nor is he able to edit his own transactions retroactively [28].

In Art. 16 p. 1 and 17 para. 1, the DS-GVO stipulates various rights that data subjects can assert against the persons responsible for their personal data. In view of the unchangeability of the blockchain, the greatest potential for conflict can be assumed here. First, Article 16 sentence 1 of the DS-GVO establishes the right of data subjects to demand that the data controller immediately corrects any incorrect data relating to them. This right of correction is essential for the data subject since incorrectly stored data can influence decisions, such as the granting of credit. Even apparently, meaningless inaccuracies are covered by this right, as it is not possible to predict whether they will be relevant in the future. Entries in the blockchain cannot be changed afterwards. Art. 16 sentence 1 DS-GVO is thus in complete contrast to transaction data, which is actually unalterable, and special technical implications are required to implement such a right in practice.

Art. 17 (1) DS-GVO regulates the right to deletion in certain cases. Accordingly, data may only be stored for as long as it is actually needed. As soon as the respective purpose for which the data have been processed has been fulfilled, the data subjects are entitled to demand that the data be deleted. The data controller must, therefore, ensure that access to the data is no longer possible or only possible at a disproportionately high cost. However, it is technically difficult to comply with such a request, as this would also invalidate all hash values and thus make the entire chain inconsistent. In order to circumvent the right to deletion, it could also be argued that the purpose of the network is precisely the continuous updating of the transaction history and that a right to deletion would therefore not apply at all [12, 28].

It turns out that data protection law can indeed be applied in a public blockchain network, but the implementation of the rights of data subjects does not seem to be easy to handle in practice. This requires separate regulations on how data protection is to be applied in blockchain networks or how technical implications, which guarantee the implementation and maintenance of data protection, are to be used in principle.

III. CIVIL LAW ASPECTS OF BLOCKCHAIN TECHNOLOGY USING THE EXAMPLE OF SMART CONTRACTS

According to 143 para. 1 BGB (German Civil Code), rescission of contracts is effected by declaration to the party opposing the rescission and has the effect according to 142 para. 1 BGB that a legal transaction is to be considered null and void from the beginning. For contracts within the blockchain network, this would mean that transactions already validated and stored in the blocks would have to be considered void retroactively in the event of an effective challenge. However, the technology is characterized precisely by the immutability of the transaction history [2].

The effect of the rescission is standardized in 346 para. 1 BGB. According to this, the services received are to be returned and the benefits obtained are to be surrendered if one of the contracting parties has reserved the right to withdraw from the contract or if it has a statutory right of withdrawal. The question arises as to how a rescission can be represented in the blockchain, especially if the seller does not cooperate. For example, in a blockchain, no one can create transactions for other users since the respective key pair belonging to the address is always required.

Furthermore, the question arises as to how it can be guaranteed within a blockchain network that only authorized persons to conclude contracts. Although in traditional transactions it is also not excluded that an unauthorized person may enter into such a contract, the immutability of the blockchain usually creates higher hurdles in the reversal or termination of transactions. For example, a legal transaction is pending invalid if one of the contracting parties is a minor. For the legal transaction to be effective, the consent of his legal representative is then required in this case in accordance with 107 BGB (German Civil Code), unless the Minor merely gains a legal advantage. It is questionable how such pending invalidity can be depicted in a blockchain, just as it is to be examined whether a Minor executes transactions.

The blockchain is an independent, decentralized network. It is therefore questionable how it is to be ensured within this framework that transactions are not subject to a legal prohibition in the sense of 134 BGB. Since there is usually no central control authority, there is initially no verification of the transaction contents. In this case, an automatism could be built into the blockchain network, which routinely compares transactions with certain laws [12]. However, it is usually necessary to interpret the corresponding prohibition law. The blockchain, however, only stores fixed parameters and leaves no room for questions of interpretation. This also leads to collisions with the immorality according to 138 BGB. Whether or not there is a violation of moral standards is usually judged differently and can therefore only be checked with difficulty by automatic mechanisms [12]. Finally, this raises the question of whether legal terminology such as good faith, discretion, unreasonableness or force majeure will be considered in a blockchain network in the future [4].

IV. POSSIBLE SOLUTIONS

This chapter presents three exemplary approaches to solving the problems mentioned above, at least to some extent. The so-called reverse transactions execute faulty transactions once again in reverse, thus restoring the economic state that existed before the wrong transaction. However, all transactions remain transparent [12].

Pruning involves the partial deletion of past transactions by a central instance. It should be noted that the data to be deleted must already be contained in a new transaction. This process makes it possible to remove data without losing proof of the respective legitimacy and to continue the blockchain. This preserves the functionality of the entire blockchain since the hash value of the block is not changed. However, this will in all probability lead to a loss of traceability and protection against forgery.

The use of the Chameleon hash makes it possible to bypass the actual unchangeability underlying the blockchain technology by allowing changes to already verified transactions. However, this implementation requires the use of a central instance that carries out deletions according to certain parameters and is responsible for them [28].

V. CONCLUSION

There are destructive revolutions that attack the existing. In addition, there are productive revolutions that take the path of the new and try to make the old superfluous [3]. As early as 2015, the World Economic Forum published a study that predicted that by 2025, 10% of the world's GDP would already be generated using blockchain technology.

In addition, the blockchain technology should make it possible, among other things, to circumvent corruption by making transactions directly with each other, without a third party. However, potential users in countries with a high level of corruption or weak infrastructure may not yet be able to take advantage of the conditions for participating in a blockchain network, such as a PC with appropriate Internet speed.

Today, almost 1.7 billion people worldwide still do not have access to a bank account, yet the majority of

these people own a mobile phone. The Libra Association, whose members include Facebook, Uber and PayPal, is trying to take advantage of this imbalance by establishing its own digital currency called Libra based on a blockchain network. In this way, access to a simple global monetary and financial infrastructure is to be created for billions of people, regardless of their place of residence, occupation or income. At present, however, this is not a publicly accessible blockchain network, but one that requires approval and is to become public within five years. Initially, the mining will be operated only by members of the Libra Association. The threatening competition does not seem to harm the price of the crypto-currency Bitcoin, however, since April this year the price has been rising again. Currently, one Bitcoin is worth about 9,389 Euro.

For the current legal challenges with regard to the blockchain technology, it can be said that there are at least approaches to solving the problems, although not all hurdles can be overcome without further ado. The extent to which these affect the integrity or are detrimental to the actual application depends on the intentions of the users in the respective area of application and the goals to be pursued. There is no need for new legal regulations, but an appropriate interpretation with regard to blockchain technology and the development of exceptions, such as the acceptance of reverse transactions to fulfil the reverse transaction of a contestable legal transaction.

On the part of the legislator, too, it remains to be seen whether the appropriate legal framework for blockchain technology will not be created, as other countries have already implemented it. The CDU/CSU and the SPD have determined in their coalition agreement how they want to position themselves with regard to the blockchain technology. Among other things, it states that they want to develop a comprehensive blockchain strategy and advocate an appropriate legal framework for the trade-in cryptocurrencies and tokens at European and international level. Furthermore, innovative technologies such as distributed ledgers are to be tested and a legal framework created based on this experience.

However, it is not only at the national government level that the technology is being further researched. In addition, on the European level with the European Blockchain-Partnership, an institution has been created, which wants to invest in different projects, which support and promote the use of the blockchain. Members are not the only EU Member States, but also some members of the European Economic Area. The aim is to build a European Blockchain infrastructure that supports the provision of cross-border digital public services with the highest security and privacy standards by 2020. In addition, the European Commission has set itself the task of achieving international standardization of the blockchain.

In addition, it has founded the European Blockchain Observatory together with the European Parliament, which among other things is to bundle blockchain initiatives in Europe and create a transparent forum for the exchange of information and opinions. Furthermore, the exchange and debates on the topic of Blockchain are to be promoted.

Furthermore, a new interest group, the International Association for Trusted Blockchain Applications, INATBA for short, was founded. The aim of INATBA is to exploit the potential and advantages of blockchain and distributed ledger technology and to promote legal certainty, transparency and integrity. It is questionable, however, to what extent seriousness can still be guaranteed with this multitude of facilities. In particular, neither Ethereum nor Bitcoin representatives are currently represented in the INATBA initiative.

However, not only countless institutions are being founded, which advertise with blockchain as a slogan. New innovative applications for the technology are also being sought in a wide variety of industries. For example, the Austrian postal service has now offered a so-called Crypto Stamp. This involves stamps that consist of a real paper stamp on the one hand and a virtual counterpart on the other. The virtual part is linked to the Ethereum blockchain and thus provides access to the cryptocurrency ether. Whether these offers will help to establish the blockchain in society remains questionable.

The blockchain is supposed to guarantee trust, security and integrity. Nevertheless, there is also a security risk, especially for external interfaces, which are needed for reading and writing data. It also remains to be seen whether the algorithms used will become outdated over time and to what extent they will still be able to communicate with each other. The lack of standards in the area of blockchain applications means that the various networks are not compatible with each other. The multitude of possible solutions makes it difficult, especially for inexperienced users, to decide on a particular application.

Furthermore, it remains questionable how, in contrast to the institutions and research ideas, the negative headlines will affect cryptocurrency in the end and, as a result, possibly blockchain technology. Bitcoins, for example, has already been used to pay for purchases via the Silk Road Internet platform. This was a sales platform in the Dark Web on which, among other things, drugs or hacker software was offered which could be paid for with Bitcoins when making a purchase. The Dark Web is not accessible via common web browsers and search

engines. It is an anonymous network. However, on the one hand, these problems can never be avoided in a publicly accessible network without a control authority or access requirements. Silk Road was just one example of a multitude of illegal platforms on the Internet. If there is no control at all, it can be assumed that illegal transactions are also being conducted via public blockchain applications or that their payment is largely anonymous via systems such as Bitcoin.

In any case, it remains to be investigated in the future to what extent the data of a blockchain are valid in the real world. The immutability of the data in the blockchain does not guarantee the validity of the data outside the blockchain.

It is not yet clear in which direction the blockchain technology will go. The technology still needs some further development and it will only become clear in the future whether the announced revolution through the blockchain technology will actually occur and last in the long term. In any case, however, caution is advised in view of a large number of offers. Many providers and institutions may want to profit from the hype about blockchain, but in the end, they have little contact with it. Not everywhere where blockchain is written on, it is also blockchain in it.

REFERENCES

[1] S. Jaiswal. (2018) Is blockchain a game-changer for healthcare? [Online]. Available: https://bit.ly/3Ea3cS7

[2] K. Schiller. (2018) Was sind smart contracts. [Online]. Available: https://bit.ly/3k1mcKo

[3] M. Matuschek. (2017) Blockchain-A technology is revolutionizing the way we think. [Online]. Available: https://bit.ly/3E8le7a

[4] B. Bundesverband. (2018) Blockchain, data protection, and the GDPR. [Online]. Available: https://bit.ly/3A5Akb0

[5] G. Rapier. (2017) From yelp reviews to mango shipments: IBM's CEO on how blockchain will change the world. [Online]. Available: https://bit.ly/38WdRkH

[6] D. Streichert. (2018) Blockchain–Game changer in der logistik. [Online]. Available: https://bit.ly/3hpFx6h

[7] D. Burgwinkel, *Blockchain technology: Einführung für business-und IT manager*. Walter de Gruyter GmbH & Co KG, 2016.

[8] R. Maas. (2018) Thailands new crypto law comes into force. [Online]. Available: https://bit.ly/3noFlIc

[9] T. Giese. (2018) Michigan - immutability of the blockchain should become law. [Online]. Available: https://bit.ly/3noKvE0

[10] H. Wieduwilt. (2018) Problem for future technology-child pornography found in the blockchain. [Online]. Available: https://bit.ly/3hH45Ij

[11] C.-H. Chen, Y.-S. Ye, W.-T. Hsu *et al.*, "Automatic venipuncture insertion point recognition based on machine vision," *Journal of Advances in Technology and Engineering Research*, vol. 4, no. 5, pp. 186–190, 2018. doi: https://doi.org/10.20474/jater-4.5.1

[12] E. Sixt, *Bitcoins and other decentralized transaction systems*. Wiesbaden, Germany: Springer Gabler, 2017.

[13] T. Gayvoronskaya, C. Meinel, and M. Schnjakin. (2018) Blockchain–hype oder innovation, technischer bericht nr. 113. [Online]. Available: https://bit.ly/2X7kEpH

[14] H. Khadija and K. Elif, "Contact less signs monitoring using doppler radar sensor," *Journal of Advances in Technology and Engineering Research*, vol. 5, no. 2, pp. 72–78, 2019. doi: https://doi.org/10.20474/jater-5.2.2

[15] S. Gros and A. M. Wagner. (2018) Blockchain and smart contracts - modern it concepts from a (data protection) legal point of view. [Online]. Available: https://bit.ly/3tvB5YC

[16] S. Breidenbach, F. Glatz, and T. Braegelmann, *Rechtshandbuch Legal Tech*. Vienna, Austria: MANZ Verlag Wien, 2020.

[17] D. Drescher, *Blockchain Basics: An Introduction to the Elementary Concepts in 25 Steps*. Nordrhein-Westfalen, Germany: MITP-Verlags GmbH & Co. KG, 2017.

[18] D. Streichert. (2018) Vorteile und nachteile der blockchain-technologie. [Online]. Available: https://bit.ly/3E8WQ59

[19] H. Bechtolf and N. Vogt, "Data protection in the blockchain-a question of technology," *Magazine for Ür Data Protection*, vol. 2, pp. 66–71, 2018.

[20] F. Glatz, J. Holthusen, and S. Kufeld. (2016) Vorstellung der blockchain-technologie "hallo, welt". [Online]. Available: https://bit.ly/3hom0TQ

[21] M. Heinrich, "M. heinrich, "spreading" as an offense in media criminal law, contributions to media criminal law - part," *ZJS*, vol. 5, pp. 569–588, 2016.

[22] A. Schlund and H. Pongratz, "Distributed ledger technology and crypto "a clauses - a legal consideration," *German Tax Law*, vol. 12, pp. 598–604, 2018.

[23] M. Henze. (2018) A quantitative analysis of the impact of arbitrary blockchain content on bitcoin. [Online]. Available: https://bit.ly/2Xg7Vkr

[24] E. Hilgendorf and B. Valerius, *Computer and Internet Criminal Law: A Floor Plan*. London, UK: Springer-Verlag, 2012.

[25] D. Bundestag. (2014) Draft law of the parliamentary groups of the CDU/CSU and SPD to amend the criminal code of. [Online]. Available: https://bit.ly/3k2l1KP

[26] U. Kindhauser, *Criminal Code Text and Practice Commentary*. Baden-Baden, Germany: Nomos, 2017.

[27] J. M. Hofmann and P. Johannes, "DS-GVO: Instructions for the autonomous interpretation of the personal reference: Definition of terms of the decisive question of the material scope of application," *Magazine for Ür Data Protection. S*, vol. 5, pp. 221–226, 2017.

[28] M. Martini and Q. Weinzierl, "The blockchain technology and the right to be forgotten-the dilemma between not-to-forget-can and to-be-forgotten," *New Magazine for Ür Administrative Law*, vol. 36, no. 17, pp. 1251–1259, 2017.

[29] E. Hofert, "Blockchain-profiling - processing of blockchain data inside and outside ss outside the networks," *magazine for ür Data Protection (ZD)*, vol. 4, pp. 161–166, 2017.

[30] J. Erbguth and J. G. Fasching, "Who is responsible for a bitcoin transaction," *Applicability of the GDPR to the Bitcoin blockchain. Z data protection*, vol. 12, pp. 560–565, 2017.