PLATTFORM INDUSTRIE 4.0

WORKING PAPER

Blockchain and the Law in the Context of Industrie 4.0

Imprint

Published by
Federal Ministry for Economic Affairs and Energy (BMWi)
Public Relations
10119 Berlin
www.bmwi.de

Text and editing
Plattform Industrie 4.0
Bertolt-Brecht-Platz 3
10117 Berlin

Design and production
PRpetuum GmbH, 80801 Munich

Status
February 2019

Illustrations
Iaremenko – iStockphoto (Title),
Alengo – Getty Images (p. 3),
simpson33 – iStockphoto (p. 6),
mattjeacock – iStockphoto (p. 10),
ilkercelik – iStockphoto (p. 11),
Yuichiro Chino – Getty Images (p. 15),
NicoElNino – iStockphoto (p. 18),
Juhari Muhade – Getty Images (p. 19),
maxkabakov – iStockphoto (p. 21),
Erik Isakson – Getty Images (p. 24),
Cecilie_Arcurs – iStockphoto (p. 26)

This publication as well as further publications can be obtained from:
Federal Ministry for Economic Affairs and Energy (BMWi)
Public Relations
E-mail: publikationen@bundesregierung.de
www.bmwi.de

Central procurement service:
Tel.: +49 30 182722721
Fax: +49 30 18102722721

Content

Introduction

Blockchain

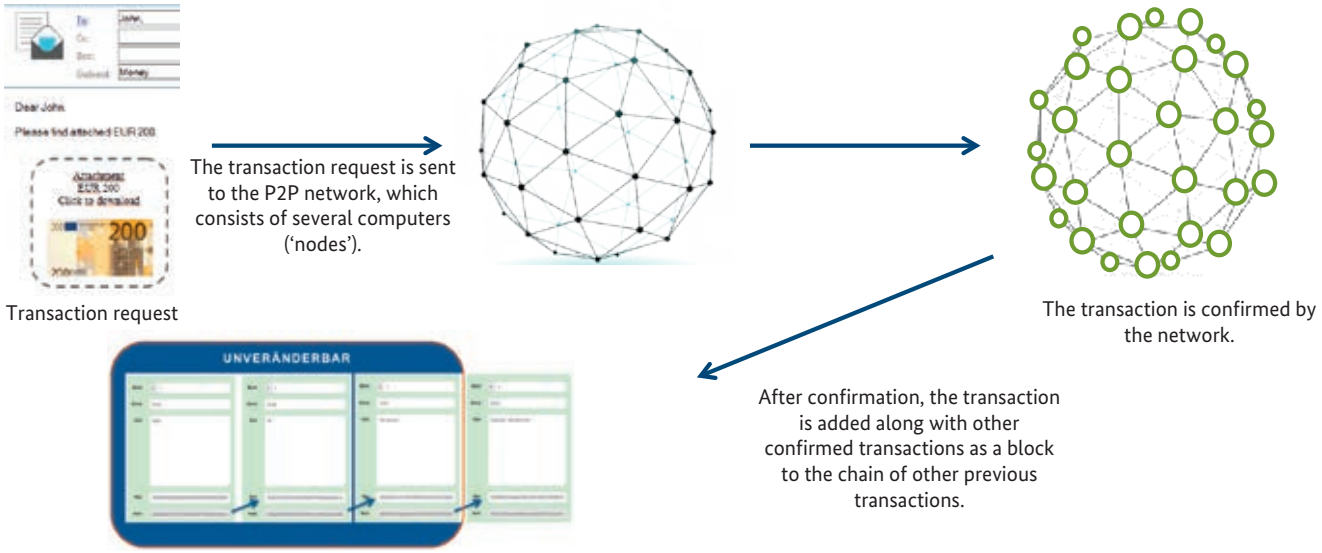
Blockchain is not an application software in and of itself, nor a program, rather a specific, non-manipulable method of storing and exchanging data. A blockchain is similar to an ownership record in which certain procedures and consecutive events are documented, such as the Commercial Register or the Land Register. However, in contrast to conventional ownership records, data in a blockchain is not managed centrally (a 'single ledger'), rather decentrally by all of the parties linked to the register (a 'distributed ledger'). Each participant ('node') has on its computer a copy of the database that constitutes the register. This distributed ledger technology (DLT) is designed to eliminate the risks of the single ledger with a centrally operated database – for example manipulation or loss of data.

DLT is based on chronological, decentralized and cryptographically secure databases. DLT combines cryptography, peer-to-peer networks (P2P), consensus algorithms and smart contracts (see below), and enables a multitude of parties to share and process data without resorting to a central management system. Data can be stored and exchanged using a blockchain. This takes place either within an open network (accessible to everyone by downloading free software) or a closed peer-to-peer network. These different network types are referred to either as a a public or a private blockchain.[1]

Access to the database and the data associated with a participant – for example the ownership of bitcoins – is provided with a 'wallet' containing a public key and a private key. Both are necessary for initiating a transaction. The public key corresponds to the address of the wallet (comparable to an account number) and is assigned to the transaction partner (outside of the blockchain). The private key is a password that corresponds to the PIN (Personal Identification Number) for a bank account and is required to initiate a transaction. A commodity, asset or property (including cryptocurrencies such as bitcoin) are represented on a blockchain by a 'token'.

To register a transaction in the blockchain database, the owner must trigger it with his private key. In addition, this transaction must be confirmed by all participants (or at least a pre-determined majority), that is, it must be validated. To facilitate validation, transactions are grouped into a block. All participants concur in cycles ('consensus') as to when the block is closed, with which transactions and in which order. Each closed block is given a code (hash) and also bears the hash of the previous block. In this way the transaction blocks are linked by the hashes to a 'chain' (hence the term

1 This publication is based on the terminology of the specification DIN SPEC 3103 "Smart Contracts und Sensoren in Bockchains für Industrie 4.0 Anwendungen" (Smart Contracts and Sensors in Blockchains for Industrie 4.0 Applications), which is planned for publication in the second half of 2019, and was provided in a draft version to the Legal Frameworks Working Group. The specification DIN SPEC 3104 ("Blockchain-based validation of documents") was also referenced.



Each block bears i) the 'hash' of the previous block and ii) its own 'hash'. Any subsequent modification in the previous block changes its 'hash', which then does not correlate (any longer) with the hash in the following block, and thus this would interrupt the chain.

The chain of blocks

Source: Legal Framework Work Group (WG 4) of the Plattform Industrie 4.0

'blockchain'). The transaction chain provides information on changes back to the original block, and in the case of bitcoin, account balances can be calculated at any time. The fact that each node contains a copy of all transaction data and, uses this data history to validate a new transaction before giving consent, makes it very difficult to manipulate the blockchain.

Like computers, there are various 'operating systems' for a blockchain. The most familiar are Bitcoin, R3 Corda, Hyperledger and Ethereum. Each system allows for different access requirements for participants, volume of data visible to participants, authorization to initiate a transaction and the validation requirements for a transaction. This makes the blockchain versatile – it can be customized for nearly all industrial applications.

One example for practical use of blockchain-based systems in the mobility sector is storage of vehicle data to ensure an immutable history of that vehicle. This type of vehicle history could for example make it impossible to manipulate the mileage on the odometer of a vehicle before it is sold. The immutable history stored in the blockchain could assure a potential buyer that information provided by the seller is correct.

The (near) immutability of the blockchain and the de facto execution guarantee inherent in smart contracts present many possibilities for industrial applications in the area of process optimization, cost savings and developing new business models. This is especially clear for example in logistics, where there are numerous blockchain-based applications that simplify the complicated documentation and processing of supply chain processes.

Example

A blockchain platform developed jointly by Technology Provider A and Transport Company B provides an information platform for shipping information, documents, customs declarations and IoT data. Depending on their role and authorization, forwarding agents, shipping companies, ports and terminal authorities as well as domestic transport and customs authorities can access this information stored in the blockchain in real time. Instead of bilaterally exchanging

documents, the participants have access to information in the form of a uniform immutable data record that enables them to work together securely, efficiently and with confidence. Furthermore, they are in a position to use IoT and sensor data for managing temperatures or container weight, for example. Smart contracts can be used to automatically validate fees and additional expenses.

Smart Contracts

Smart contracts are computer programs (and not actually contracts in a civil law sense) that are built on if-then commands. This type of command is not new. What is new is the fact that smart contracts on the blockchain are run concurrently through many nodes, and the result is "written into the blockchain" after automated validation. Automated, parallel operation of smart contract programs and parallel recording of data in blockchain nodes make it impossible to manipulate the individual programs in practice.

Unlike with single-ledger databases, an individual party cannot prevent execution – implementation is therefore effectively guaranteed.

For example, delivery of goods in exchange for payment of the purchase price can be processed automatically with an execution guarantee within seconds, without counter-party risk, as soon as the pre-defined prerequisites ('triggers') are fulfilled, such as confirmation that the goods are free of defects and the buyer's account has a sufficient balance.

One example for potential use of smart contracts is when Provider A offers a system for managing platooning – when several trucks on a motorway form a line. The special feature of the platooning system is that the distances between the vehicles lined up in the platoon can be calculated at any time and predicted by the system, and also managed to achieve the optimal distances so that the usual 'accordion effect' is avoided as much as possible (one vehicle brakes slightly, the following vehicles brake more strongly, and the same phenomenon when the lead vehicle accelerates). This foresight on the part of the drivers can lead to substantial fuel savings. The blockchain and smart contract system comes into play in calculating platoon performance. This type of system turns on a counter as soon as the platoon is formed, and the moment a vehicle leaves the platoon the smart contract in the blockchain within seconds calculate the performance the vehicle operator achieved and what the compensation should be (for example a certain percentage of the forecast diesel savings).

In general, smart-contract based invoicing could be particularly useful when many transactions with small volumes are involved. These 'micro-transactions' illustrate well how a smart contract can automate the manual effort for executing and verifying a transaction.

In the following text selected observations point out the major legal issues involved. Much of the development is still ongoing, but the possibilities for application are there and should be utilized.

Civil Law Aspects

Code is Law – Law for smart contracts and blockchain applications. How can companies apply legal systems to blockchains and transfer of goods and rights in the international context?

A: Fact sheet

What is involved?

Decentralized blockchain technology is predestined for international use, especially in Industrie 4.0. Existing legal systems are national in structure and apply only in the individual national territories. There have hardly been any efforts made toward international standardization to date, for example, in parts of the EU.

Blockchain participation and activities will require establishing national legal norms that encompass the validity and effectiveness of activities and their consequences.

What are the issues and challenges for Industrie 4.0?

- What legal norms apply to participating in a blockchain in an international context?
- What legal norms apply to activities in a blockchain and their legal consequences in an international context?
- Which legal systems apply to transfer of goods and rights in an international context?

B: Legal Assessment

National legal norms determine whether and to what extent national legal systems apply in the international context. The provisions of such national legal systems may also lead to varying results, because they are only harmonized in some areas.

To answer the question as to which national law applies, two topics must be differentiated. On the one hand there are provisions on creating and executing legal obligations, especially regarding contracts. On the other hand, there are provisions on rights in goods and intellectual property, and on how they are granted and transferred.

Contracting parties can agree on a certain national legal system for legal obligations and contracts. In the EU this is expressly regulated in Art. 3 of the Rome I Regulation. These choice of law agreements are very common in practice. The validity and content of such agreements must always be evaluated in accordance with the law that has been chosen. A critical view is sometimes voiced only if a national law system is chosen that has no connection with the parties concerned and their activities in relation to blockchain.

In contrast, the parties basically have no option to choose which national law should apply to rights in goods and intellectual property and granting and transfer of those rights. Applicable law is the national legal system at the place in which the legal object is currently located. If this legal object is transferred from one country to another, this also gives rise to a shift in applicable national legal provisions. However, for some intellectual property rights, such as copyright, there are international conventions that protect foreign holders of rights in a national legal system as if they were citizens of that country.

Accordingly, due for example to choice of law, a national legal system may apply to an agreement on transferring rights or goods on the blockchain. Nevertheless, the national law at the current location of the object to be transferred applies to the legal situation of the object and its protection under law.

C: Options and Recommendations for Action

- The participants in a blockchain should agree on which national legal system should apply to legal obligations arise and their fulfillment. This is basically possible to a great extent if the choice of applicable law has a connection with the blockchain or the transactions on the blockchain.
- With regard to goods and intellectual property, the legal system of the location of the legal object basically applies. The parties concerned must deal sensibly with this aspect.

How should smart contracts be legally categorized?

A: Fact sheet

What is involved?

Blockchain technology makes it possible to implement transaction rules that can be automatically executed. One example is the declaration of transfer of rights that takes place automatically when a condition (e.g. payment) is satisfied. There are many rules that could be automatically executed, yet they are currently limited to the blockchain itself. Such automatic rules are often termed a 'smart contract' if they are intended to generate legal consequences.

The consequences under German law of the mechanisms triggered by smart contracts must be determined.

What are the issues and challenges for Industrie 4.0?

- Which prerequisites must smart contracts fulfill under German law in order to have legal effect?
- How is a contract typically concluded using smart contracts in Industrie 4.0?
- Can smart contracts replace the existing legal norms for contracts?
- How should the requirement of form for certain legal transactions be dealt with?

B: Legal Assessment

Due to the principle of freedom of contract, each legal person can basically freely decide whether, and if so, which declaration of intent it wishes to make and which agreements to make and which not. Making declarations of intent and concluding contract is possible in any form as long as there is no specific legal requirement of form (for example, notarial form for real estate transactions).

Beyond such specific limitations, transactions on the blockchain can lead to both legally binding declarations of intent and to conclusion of contracts. This means that at all times the natural or legal person who either gives or receives a declaration of intent or who is a party to a contract must be identifiable.

One conceivable example in the context of Industrie 4.0 is using a private blockchain as a consortium. The participants agree – outside of the blockchain – by means of conventional general terms and conditions, on the prerequisites for concluding a contract (including qualifying characteristics defining who is allowed as a contracting party), the content of reciprocal obligations (main performance and consideration) and if necessary, processing individual aspects of the transaction (proof of order papers, payment, etc.) by utilizing the automated mechanism of the smart contract.

Beyond this, there has been discussion about completely integrating the effect of declarations of intent and the conclusion and execution of contracts as much as possible into automatically executing clauses on the respective blockchain. In principle, such clauses could also be validly agreed in the scope of the freedom of contract. However, there are specific statutory provisions that apply to declaration of intent and contracts (also consumer protection laws). The blockchain does not exist in a "legal vacuum".

C: Options and Recommendations for Action

- It is advisable to apply existing rules for declarations of intent and contracts, even if these are made using machines or automatically.
- The currently conceivable applications are typically implemented according to contractual terms based on conventional general terms and conditions. The parties (sometimes also within a consortium) agree upon those conditions in advance for users of a private blockchain.
- Accordingly, there is no need to take action regarding existing legal provisions for contracts and their execution on the blockchain. The statutory provisions always apply to activity on a blockchain.

How blockchain and the law interact, and the implications for business

A: Fact sheet

What is involved?

Existing legal provisions are not oriented toward blockchain technology. Much less are there any statutory provisions for specific legal situations and their application in connection with a specific blockchain. Possible uses and implementation of blockchains are developing just as quickly as the blockchain technology itself.

Accordingly, there is an even greater need to agree specific provisions for a specific blockchain with and vis-a-vis the participants. Where specific blockchains are used to execute transactions in Industrie 4.0, the applicable provisions must apply uniformly to all participants, that is, they must contain essentially standardized content for this particular blockchain. However, any business intending to use such pre-formulated business terms will find that German law on standard terms poses a considerable challenge, because German case law limits the freedom to contract using pre-formulated terms in many ways – also when these businesses contract with other business – and the law is becoming ever more restrictive. These restrictions are relatively extensive by international standards and may put a damper on innovation, for several reasons.

What are the issues and challenges for Industrie 4.0?

- Is German law on standard business terms a hurdle to innovation for business?
- How can businesses avoid the negative effects of the law on standard business terms without restricting consumer protection?

B: Legal Assessment

There is a great need for agreements with specific provisions to be identical for all participants of a particular blockchain by means of pre-formulated contractual terms, that is, 'Standard Business Terms' (AGB: Allgemeine Geschäftsbedingungen) pursuant to Section 305 of the German Civil Code.

German law on standard business terms considerably restricts businesses' creative freedom. This is also true in comparison to other legal systems in the EU and elsewhere. Any provisions deviating from legal rules applicable to pre-formulated contracts (purchase, lease, etc.) will render the provision invalid. Furthermore, case law is becoming even more restrictive in its interpretation of these restrictions. These rules are aimed at protecting consumers and are also applied increasingly to B2B contracts, with practically no changes. This restriction on freedom to contract hampers innovation in German companies relative to the options open to business abroad. The contract categories in the German Civil Code of 1900 do not proactively meet the needs of innovative business models of the 21st century involving blockchain, or even take them into consideration. In addition, there are considerable concerns whether future case law will consider standard business terms previously considered valid to now be invalid.

C: Options and Recommendations for Action

- The more and more restrictive interpretation of restrictions on standard business term law for B2B contracts should be made more flexible. There is no alternative if the disadvantages to business in Germany regarding innovation and competitive position are to be reduced compared with other countries.
- The continually restrictive application of consumer protection rules of German law on standard business terms and also in B2B contracts is increasingly restricting creativity in business, especially for innovative business models.
- The consequences of these restrictions affect small and medium-sized businesses in particular, also regarding suitable provisions for guarantees and liability.

- These disadvantages of German law for business-to-business activity abroad should be eliminated, or at least substantially reduced, Otherwise, innovative companies in particular will be forced to move abroad to realize new business models.
- Consumer protection should remain untouched.

Terms of use in the context of blockchain: Dealing with legal obstacles, defaults in performance and the possibility of reversal

A: Fact sheet

What is involved?

To create the same rules for all participants in a particular blockchain, it is advisable to agree specific terms of use. This gives rise to a number of issues regard conclusion of contracts, the ability to conduct a planned transaction and the possibility of mistakes in a planned transaction on the blockchain.

What are the issues and challenges for Industrie 4.0?

- How can specific terms of use for a specific blockchain be agreed between participants?
- How can terms of use be agreed with participants in a particular blockchain?
- What are the means to deal with hindrances to validity and default in performance on the blockchain as well as legal requirements for reversing a transaction?

B: Legal Assessment

Basically, terms of use can create the basis for specific rules for a particular blockchain. This applies both to the question of participating in this blockchain and to the transactions initiated by the participants in this blockchain. Freedom to contract means that there is leeway in creating provisions in response to these questions, as long as there are no binding legal restrictions (for example, under German law on standard business terms for transactions between businesses or between them and consumers).

To validly agree terms of use for a particular blockchain with the individual participants, the participant must be able to take note of them and provide its consent. This consent is not subject to formal requirements, unless there are special requirements of form for exceptional cases. If the contract conclusion – including corresponding declarations of intent or accepting the terms of use – should take place within the blockchain itself, it is absolutely imperative that this transaction be clearly linked to a legal person and be verifiable (including the possibility of enforcement, see below).

The immutability of the data or information stored in the chain is a major feature of the blockchain. This does not prevent the transaction on which the data is based ("Kausalgeschäft": undertaking) from being free of errors – for example, if it was invalid from the beginning (it should have never been executed for legal reasons), not does it prevent the transaction from subsequently being contested or a party having a claim to reversing the transaction for reasons of withdrawal (for poor performance or other reasons for default of performance).

Conceivable situations in which the transaction is invalid are if the legal transaction is invalid from the start because it constitutes money laundering (financial transactions) or violates any other legal prohibitions, or if it is successfully contested on the grounds that it constitutes fraudulent misrepresentation.

This transaction is indeed executed automatically and irreversibly – however, under German law, this transaction would have no legal effect, or had no legal effect from the beginning ("ex tunc"), or must be eliminated retroactively. That is, if it is not possible to "delete" a completed transaction from the blockchain, it must be reversed by means of a "reverse transaction", by creating a new block 'in reverse'. This allows for removal of the economic consequences of the transaction, even if the transaction history is still visible due to the nature of the record.

To enforce secondary claims afterwards (e.g. reducing compensation on the grounds of poor performance), suitable guarantees of reimbursement could be anchored beforehand in the code of a smart contract. However, if the goal is construction of indefinite legal terms and leeway in interpretation (e.g. non-performance on the grounds of material defects – contrary to non-material deviations from the promised performance), the automatic mechanism contained in a pre-programmed reversal of the transaction has natural limitations.

This becomes even more challenging if the initiator of the transaction – especially in a public blockchain – is not personally identifiable and/or the invalidity of the contract was triggered on a much earlier part of the blockchain. Then all of the following transactions that build on the invalid transaction would have no legal basis, triggering a reversal throughout the whole chain that would be incom-

patible with the system. A possible remedy would be an automatic dispute resolution mechanism directly integrated into the block.

Ultimately it follows (at this point in time) that smart contracts in private and permissioned blockchains appear relatively feasible if based on standard terms of business or terms of use (if necessary, agreed outside of the blockchain), if the legal treatment of nullity and reversal claims and measures for enforcement and dispute resolution are clearly stipulated for named or identifiable participants. This of course means that there is a great deal of new territory to be worked through, both from a legal and a technical aspect.

C: Options and Recommendations for Action

- There is no need to take action for creating an agreement on terms of use. The conditions for making it possible for participants to acknowledge terms of use and to provide consent can be fulfilled with suitable technical means, both outside and inside the blockchain.

- Dealing with legal obstacles ("ex tunc" invalidity) poses a substantial legal challenge, because a transaction that has already taken place is by definition always visible in the blockchain. This requires further clarification as to whether in a private blockchain for example the problem has already been solved with terms of use, or if a legislation is required that would allow for the consequences of invalidity to be dealt with legally by means of one (or more) 'reverse transactions'

Transfer of rights in the blockchain

A: Fact sheet

What is involved?

Rights in goods and rights can also in principle in particular be transferred through the blockchain, if this is allowed under applicable national law and requirements of form and other formalities (see in the aforegoing questions on applicable law). For Industrie 4.0 applications the question is whether the blockchain can provide easier solutions, for example by verifiably documenting the purchase of goods for all participants to see, or by avoiding the risks of a good faith purchase of goods based on pretense of legality.

What are the issues and challenges for Industrie 4.0?

- How can rights and goods be transferred using the blockchain?

- How can a physical object be verifiably and clearly linked to a code stored in the blockchain so that any acquisition of ownership is also unmistakably linked to the object in question?

B: Legal Assessment

If transfer of rights in intangible goods or data is involved – for example in the case of contractually agreed exchange of machine data – a self-executing transaction is easy to facilitate using the blockchain. Data exchange in the form of access or downloads is started automatically depending on an automatically triggered payment, for example, or another type of release instruction.

However, transfer of ownership or rights using a smart contract is also possible for tangible assets. For example, it is conceivable that the object is actually transferred outside the blockchain or that constructive possession is agreed (within the meaning of Section 929 sentence 1, 930 of the

German Civil Code) and that in the smart contract the exchange of declarations of intent for transfer of property (in rem agreement) is dependent on the technical possibility of digital verification of payment. A clear link of tangible goods to their respective right-holders can be facilitated in the blockchain with corresponding digital identities ('digital twin').

C: Options and Recommendations for Action

- The blockchain and smart contracts are suitable means for tracking transfer of rights in goods and digital goods. This requires a clear link between the physical item and its counterpart stored in the blockchain.

Liability for programming mistakes

A: Fact sheet

What is involved?

If the projected use of blockchains in Industrie 4.0 is based on pre-defined terms of use in private blockchains, the question arises as to the possibility of faulty programming of the blockchain or a smart contract and, as a possible result, a faulty transaction.

What are the issues and challenges for Industrie 4.0?

- What liability scenarios are conceivable and who is liable for faulty functioning of the blockchain or smart contract?

B: Legal Assessment

Regarding the question of any 'errors' in smart contracts it is important to differentiate clearly between technical and legal aspects. An individual block in the chain is deemed error-free if it can be successfully linked with other blocks in the blockchain. Executing a smart contract transaction cannot technically go wrong in this sense – the transaction will either be successfully executed from a technical standpoint or not at all. However, whether the transaction corresponds in legal aspects to the contract on which it based from the viewpoint of the participants, is a different issue. The smart contract does not allow interpretation – the interpretation only refers to what was intended outside of the smart contract, in order to assist the parties, if necessary, in facilitating the success they jointly aim for.

The authenticity or correctness of the data on which a transaction is based and the economic motivation behind the transaction in a block is first and foremost the responsibility of the company that stored this data in the blockchain. A legal problem that needs closer attention arises if data is incorrectly entered over several blocks, the following blocks are initiated by the other side and third parties believe that the data is correct. Here we could ask if, in case errors become apparent, this would lead to liability of several participants or to joint or several liability of several participants.

C: Options and Recommendations for Action

- Given complete transparency of the preceding transactions and the contractual assumptions and data on which they were based, the issue of may arise that content is adopted in the subsequent transaction and – in case of erroneous data – possibly cumulated or liability "throughout the chain" becomes communitized. Terms of use should exclude this effect as much as possible to ensure the reliability of blockchain-based transactions.

Enforcing claims to or outside of a public or private blockchain

A: Fact sheet

What is involved?

When smart contracts or other transactions executed on the blockchain lead to defects in performance, the enforceability of civil law claims is essential to provide reliable security for blockchain use.

What are the issues and challenges for Industrie 4.0?

- How can claims to or outside of a public or private blockchain be enforced?

B: Legal Assessment

The smart contract, a self-executing transaction, is typically based on a previously concluded contract or related standard business terms outside (and also conceivably on) the blockchain. Whereas the binary function of a smart contract – in the sense of "if-then" logic – can be easily linked to a pre-defined, measurable occurrence of the main performance in order to trigger automatic payment (thereby also addressing the problem of "who can tell me that my customer will pay?"), it gets more complicated when secondary claims are involved (guarantee, damages, etc.). So that these claims can also be easily asserted, they must be taken into consideration from the very beginning, in the program code ('law programmed in'). However, due to the complexity and extent of possible interpretation, as well as to the relevance of non-standardized legal terms (e.g. "substantial deviation from the contractually agreed quality"), this is decidedly more difficult for secondary claims.

The enforcement of all secondary claims not reflected in the smart contract or that cannot be integrated into the smart code when it is being written must take place the "customary way" – that is, like in the "real world", on the basis of standard business terms in a private blockchain whose participants – usually – would be identifiable by name with the help of signatures, in contrast to a public blockchain. The contract on which the transaction is based determines which claims actually exist and under what conditions they can be enforced ("Kausalgeschäft": undertaking). However, the smart contract could be of assistance in enforcing these claims if a mandatory arbitration tribunal, ombudsman or a so-called oracle is included in the code, thereby indicating in advance a suitable dispute resolution process. If there is no programmed component for dispute resolution to which the parties can resort, enforcement of claims against a party to the contract is only possible if that party can be identified (outside of the blockchain). In this sense, using a private/permissioned blockchain is obviously preferable.

C: Options and Recommendations for Action

- Effective enforcement is a decisive and trust-building factor in using the blockchain.
- When using a private blockchain – that is, in the realm of currently foreseeable situations – dispute resolution mechanisms anchored in customary terms of use are the usual choice.
- The public blockchain throws up considerable roadblocks to solving disputes between participants within the blockchain – even if they are identifiable with digital identities. In such cases, there should be more effort put into creating automated dispute resolution mechanisms for simple, binary decision situations.
- Regarding complex dispute resolution, in particular cases that rely on the interpretation of non-standardized legal terms, an automated dispute resolution process within the blockchain will likely be impossible for the near and mid-range future, and as a rule, remain problematic with regard to the principle of a state governed by the rule of law.

Blockchain and Data Protection

A: Fact sheet

What is involved?

Blockchain technology promises great potential for digitalization of industry. IoT services, logistics or smart contracts – there are many areas of Industrie 4.0 in which the decentralized architecture of the blockchain can be helpful in connecting the many participants.

Using blockchain technology raises quite a few issues regarding data protection. The EU General Data Protection Regulation (GDPR) that came into effect in May 2018 is based on a central server architecture and data-based business models of individual data processors. The provisions of this regulation therefore appear somewhat out of date in view of the new, decentralized technologies.

Especially the immutability of the blockchain and its sometimes numerous and nameless participants are at the focus of legal discussions on this topic. Deleting or modifying data after it has been entered is an anomaly in the blockchain – the very fact that data is continually added creates the trust that is inherent in this technology.

Permissioned/private blockchains that are preferred in the area of Industrie 4.0 prove to be less problematic than solutions that are available to anyone and are "permissionless".

What are the issues and challenges for Industrie 4.0?

- Can personal data be stored on the blockchain?
- Of the blockchain participants, who is the controller, who is the processor and who is the data subject?
- How can companies preserve the rights of the users (data subjects)?
- Where is legislation necessary to enable the blockchain technology to reach its full potential in the Industrie 4.0 context?

B: Legal Assessment

The potential conflict between blockchain and privacy is a prime example for the sometimes negative effects of a rigid data protection framework. This affects not only businesses and innovation, which are impacted to a certain extent by the uncertainties brought about by blockchain use. The Blockchain itself, as a "Privacy Enhancement Technology" – a means for giving users control and independence regarding use of their data – is also affected.

Politicians have already taken notice of this conflict, which is the subject of a report of the EU Blockchain Observatory ("Blockchain and the GDPR"), guidelines (Bitkom: "Blockchain and Data Protection – Fact Sheet"), position papers, (Blockchain Bundesverband (Federal association promoting blockchain technology in Germany: "Blockchain, data protection, and the GDPR") and scientific observations (Finck: Blockchain and Data Protection in the European Union, Max Planck Institute for Innovation & Competition Research Paper No. 18-01.). The French data protection agency CNIL has also published opinions on the topic of blockchain and data protection (Premiers éléments d'analyse de la CNIL: Blockchain, September 2018).

All observations point out that private blockchains in which the participants are known and sometimes additional agreements on use are made are easier to deal with from a legal standpoint than are public blockchains. This is beneficial to use in the context of Industrie 4.0.

In addition, from a practical point of view we must not forget that blockchain is a very young technology. Its technology is being continually improved, also to better meet data protection law standards.

Applying the GDPR Personal data on the blockchain

Data processed on a blockchain containing references to persons is subject to the provisions of the GDPR. This involves information relating to an identified or identifiable natural person (the "data subject", Art. 4 para. 1 of the GDPR). Pseudonymised data that with additional information can be linked to a natural person is still personal data in the sense of the GDPR. Only anonymised data does not fall under the GDPR (see Recital 26). However, supervisory authorities have begun to tighten the requirements for a valid anonymisation. In particular, encrypted data is often viewed only as pseudonymised, not anonymised.

The question is which data that are typically used in the blockchain are personal:

Public keys: A public key that is regularly publicly visible is inherent to many blockchains. As soon as these keys can be linked to a natural person, they are personal data as defined in the GDPR.

On-chain data: In principle, data of any type can be written into the blockchain, for example names of natural persons and other information that is personal and thus subject to the provisions of the GDPR.

Hash values: A hash is a short string of characters that represent a unique fingerprint of a (usually) larger amount of data. This is a way of clearly identifying data, files, documents, etc. Hash values are also useful for verifying whether a document has been altered (if data has been changed, a different hash value would emerge when the data is hashed again). The question is whether this "fingerprint" is really personal data.

To link a hash to specific data, that information must be available and an authorized individual must compare the hash and the original document. This linkage is simply not possible for many participants in the blockchain. This applies in particular if the original data to which the hash value refers (e.g. Delivery data of a natural person) is stored outside the blockchain and is later deleted. The hash value stored in the blockchain would therefore "hit a dead end", and would no longer indicate an identifiable person (or the corresponding data). The Article 29 Working Party on data protection set up by the EU Commission saw hash values as pseudonymised personal data (see WP216, Opinion 05/2014 on Anonymisation Techniques, p. 20). However, total legal certainty regarding the use of hashes in the blockchain can only be provided by a clarifying statement from the European Data Protection Authorities, and ultimately, case law.

What are the data protection roles for the blockchain

Another area of uncertainty is the how to categorize the participants in the blockchain under data protection law. Assigning to blockchain participants the roles of a data subject (Art. 4 para. 1 of the GDPR), a controller (Art. 4 para. 7), a processor (Art. 4 para. 8) or of a joint controller (Art. 26) determines their corresponding rights and obligations under data protection law.

In private/permissioned blockchains, there is usually a (contractual) consensus that stipulates who is responsible for processing what data and where. This is an advantage compared with a public/permissionless blockchain architecture. Here, the individual participant is not aware what blockchain data other participants are processing and in what part of the world. This makes it impossible to agree on rules, such as regarding data processing or in the scope of joint controlling pursuant to Art. 26. In the industry sector, there are defined conditions for blockchain use. Accordingly, it is possible to determine in a particular case whether the participants are controllers, processors or joint controllers.

Asserting rights

The blockchain environment may pose a challenge to data subjects wishing to assert their rights, for example data deletion (or the 'right to be forgotten', Art. 17 GDPR) or data rectification (Art. 16 GDPR). After all, the blockchain is not designed to enable deleting data in individual blocks of the blockchain (not even in an architecture designed for such).

In a public/permissionless blockchain environment in particular, it is often not at all clear to which processor such a request should be directed. In this constellation, even reconstructing the consent under data protection law and therefor making it available as the basis for processing, would be very complicated. This problem is much easier to solve in an industrial, private blockchain.

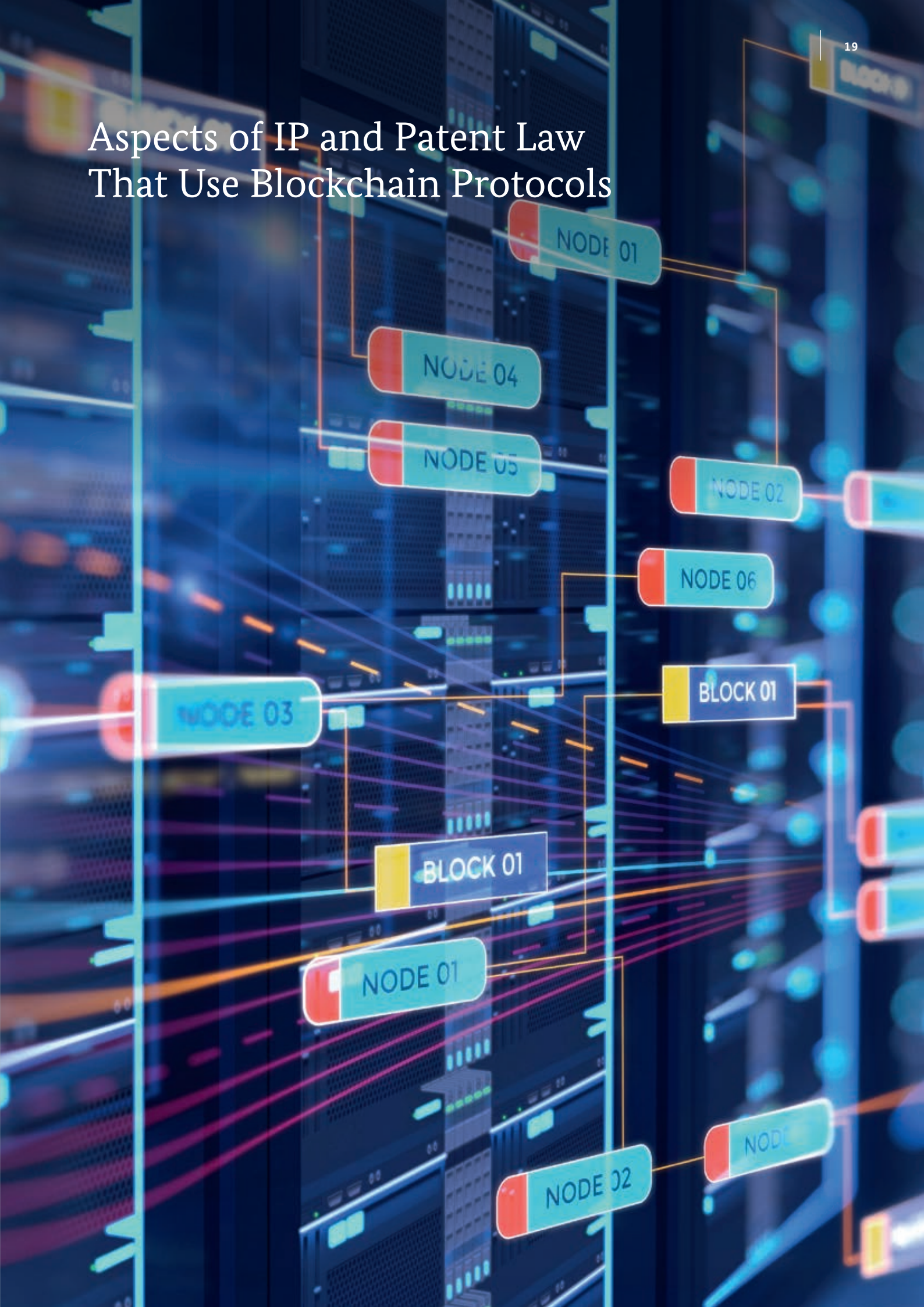
The right to have data deleted or to be forgotten is difficult in the blockchain – yet it is not impossible. Hash values are modern encryption methods used when the corresponding key is destroyed that could provide a solution to this problem (this was the opinion presented by the French supervisory authority CNIL, Premiers éléments d'analyse de la CNIL: Blockchain, September 2018).

Basically, there is a need, even in a private blockchain, for additional technical solutions in the context of Industrie 4.0, as well as a practical interpretation and application of the GDPR by supervisory authorities.

C: Options and Recommendations for Action

- If possible, Industrie 4.0 should use private/permissioned blockchains. This reduces data protection risks. As a rule, the participants in these blockchains are known. It is possible to specify where the data will be processed. In addition, when data is processed outside of the EU, data protection law provides for instruments for transfers to non-member states.
- Personal data should (also) not be stored (encrypted) in the blockchain, rather in special "off-chain" databases. Hash values are a suitable means for creating a link to the blockchain.
- In order to determine which participants have which role, binding (contractual) agreements should be made. These agreements make it possible to define roles and duties of the (joint) controllers in a private blockchain.
- Data protection authorities and the European Data Protection Authorities must prepare guidelines that strive to achieve a reasonable balance between the possibilities provided by the blockchain and the constraints of data protection.
- The right to data protection is not an absolute given. Data protection must always be considered in the context of societal developments and in balance with other basic constitutional rights.
- In this context, when the European Commission reviews the GDPR, consideration should be given to making the data protection framework more flexible regarding innovative technologies such as blockchain.
- This specifically involves legitimate use of public keys and limiting the right to have data deleted in cases in which this is technologically not possible, but could be achieved by blocking access to data, for instance.

Aspects of IP and Patent Law That Use Blockchain Protocols



A: Fact sheet

What is involved?

Blockchain is also getting a good deal of publicity, which has spurred many companies to look at which blockchain applications could improve their internal and external processes.

The first steps a company usually makes into the blockchain world is to invest in a blockchain startup, or to set up a company task force to develop an in-house product on the basis of the blockchain. In-house products are made easy by the fact that the blockchain 'community' provides blockchain frameworks and protocols that, like an operating system, can be used as the basis for new blockchain applications.

These protocols are software, which means that the typical software issues must be addressed, such as copyright and licenses. Blockchain protocols are usually available under open source software licenses. Proprietary licenses also play a role, because open source basic versions of the protocol are not always sufficient for a business application, rather the licensed 'professional' version is necessary. It is also important to consider that blockchain applications are usually used for solving technical processes and accordingly, may be patentable.

What are the issues and challenges for Industrie 4.0?

- What must users bear in mind when using open source blockchain protocols?
- What are the snares in using licensed blockchain protocols that could lead to dependency on blockchain protocol providers?
- When is a blockchain application patentable?
- What are the consequences of patentability?

B: Legal Assessment

What must users bear in mind when using open source blockchain protocols?

Like conventional operating systems, open source blockchain protocols are frequently used as the basis for programming new, individualized blockchain applications, also known as decentralized applications, or DApps. Familiar open source blockchain protocols include Ethereum, Hyperledger Fabrics and R3 Corda. These protocols are used widely and are available to the public and are therefore suitable as a basis for developing blockchain-based software. DApps can be quickly and easily developed and tested.

A common feature of these blockchain protocols is that they are provided for use under what is called open source licenses. That is, they are available in source code and can be modified, improved or otherwise processed or used, without a license fee. However, open source software is not free of copyright. Anyone using open source software is subject to the provisions of the open source software license applicable to that software. In particular, the 'copyleft' obligations often contained in software licenses are particularly important. These provisions stipulate that the user of open source software must sell its 'modifications' of the open source software under the same open source license. How far the term 'processed' goes varies between open source software licenses. Processing in this sense however might mean the entire software the user developed, possibly even if the newly developed software "only" accesses open source software. The consequence is that the user of open source software that is subject to strict copyleft must theoretically make the software it newly developed for a DApp available as open source software. The DApp would accordingly not be proprietary, which would possibly make the planned business model unattractive.

Of the blockchain protocols mentioned above, Hyperledger Fabrics and R3 Corda are available under the Apache 2.0 License as open source software. The Apache 2.0 license is a "permissive license".[2] This means that there is no copyleft, that is, the licensee is not obligated to publish under the Apache License 2.0 any software it created with the licensed software. The Apache 2.0 license therefore does not preclude using these blockchain protocols for creating proprietary applications. It is unclear which open source license applies to Ethereum, one of the most commonly used protocols. The various components of Ethereum were published under various open source licenses, including GPLv3. This is the license that triggers alarm signals in open source compliance guidelines if proprietary software code is developed for commercial use. Yet other open source licenses apply to other blockchain protocols.

For this reason, when choosing a blockchain protocol for in-house development and also when investing in a blockchain startup it is important to carefully evaluate which licensing rules apply to the software being used and to what extent the company's own proprietary software code could become 'infected'. Without this assessment, the commercial use of the affected blockchain application is at risk.

What dependencies on blockchain protocol providers should be avoided?

The same principles apply here that apply to any other software required for important business functions. The company must ensure long-term availability of the software and sufficient cost monitoring.

If development takes place solely on the basis of open source licenses and the software can be used by the user on its own systems, there are no substantial risks. However, there are a few open source blockchain products that are only suitable for testing purposes. If the test application is to be introduced to normal operation, these products lack key functions, especially regarding IT security, that are only available in an 'enterprise version' that costs money. These

2 Also see Auer-Reinsdorff/Conrad, IT- und Datenschutzrecht, Teil B. Immaterialgüterrecht § 9 Open Source und Open Content Rn. 50.

enterprise versions are made available only for a license fee and under very one-sided license terms, up to now. This creates a dependency on the software provider, because switching to a different blockchain protocol would mean that, due to the current incompatibility of the various blockchain protocols, the application would have to be developed once again for the other protocol.

When is a blockchain application patentable?

The principles developed for software also apply to patentability. According to the provisions of the European Patent Convention (EPC) – the legal basis on which the European Patent Office (EPO) grants patents – software is basically not patentable.

However, according to case law and the EPO's patent examination practice, this rule must be interpreted narrowly. Exclusion from patent protection applies only to software per se. In other words, patents are not granted to the source code itself. This protection is reserved for copyright. However, the abstract technical teaching on which the software is based is definitely eligible for patent protection – this is referred to as computer-implemented inventions (CIIs).

The EPO has a two-step patent examination scheme for CIIs. In the first step the examiners determine whether the claimed subject-matter is software. This examination always leads to a positive analysis as soon as the technical system 'computer' is involved. In a second step of the scheme developed for CIIs, the claimed CII must be novel and be based on an inventive step.

Only those novel features are taken into consideration that contribute to the technical character of the claimed subject matter. To establish such a technical character, a "further technical effect" is necessary that goes beyond the "normal" physical interaction between the program and the computer on which the program is run.

The guidelines for the European Patent Office[3] examination provide examples of further technical effects in Part G Chapter II-16: 3.6. Furthermore, in Part G Chapter VII-8, 5.4.2 practical examples of technical and non-technical features of CIIs.

The European Patent Office has already awarded patents to blockchain applications in the recent past. For example, the following applications were seen as patentable – that is, especially as being novel and inventive:

- In a process for monitoring a smart contract the use of an unspent transaction output (UTXO) as a data record was found to be an inventive step if the UTXO is used to interpret whether the contract should be considered open or valid.

- Computer implemented processes for determining whether a software product is licensed and therefore is being used properly was seen as inventive, because special public keys were compared using a transaction data record stored in the ledger.

These examples demonstrate that the EPO is open to providing patent protection to blockchain applications. However, it remains to be seen whether the patents granted up to now will be confirmed as effective in any opposition proceedings or national cancellation proceedings.

What are the consequences of patentability?

There are huge opportunities for innovative firms that develop patentable products. Whereas the usual protection for software only protects the actual implementation but not the idea, abstract ideas on which blockchain applications are based can be protected by patent. This can strengthen the competitive position of a company and increase its turnover from license fees, due ultimately to licensing the technology. However, it seems that here time is of the essence, because a number of basic applications have already been applied for or already have patent protection, especially in other countries such as the USA and China.

3 http://documents.epo.org/projects/babylon/eponet.nsf/0/2A358516CE34385CC125833700498332/$File/guidelines_for_examination_2018_hyperlinked_de.pdf

On the other hand, when blockchain applications are being developed, attention should be paid to whether patents have already been applied for or granted in the area of the application in order to minimize risks.

Some observers[4] of the situation see the blockchain area as a future "battlefield" for patent disputes.

C: Options and Recommendations for Action

- Before even selecting a blockchain protocol for a test application, it is important to assess very carefully whether the protocol chosen will stand up to the requirements of normal operation later. This includes not only technical requirements, but also and in particular copyright aspects.

- When using open source protocols subject to a copyleft, it is important to assess whether this will "infect" the user's own development. This is not always the case, but it could happen.

- A blockchain app developer should research the patentability of the app early on, especially before disclosing details.

- Patent publications relating to the blockchain should be monitored by a service. This will help identify at an early phase whether the app infringes on patent rights applied for or already granted. This can make it possible to take appropriate measures to counteract this, such as workarounds, the assertion to the legal status of the patent or opposing a patent already granted.

4 https://cointelegraph.com/news/is-blockchain-about-to-become-a-patent-war-battleground

The Importance of IT Security for Blockchain

A: Fact sheet

What is involved?

One of the advantages of the blockchain mentioned most often and also of currently popular cryptocurrencies is that blockchain technology is secure. However, on June 20, 2018, the German business journal Wirtschaftswoche reported that up to that point in time, "a total of one million bitcoins had been stolen – and at the current rate [June 20, 2018] this is equivalent to a theft of USD 6.6 billion". How do these two statements square up, and how relevant is this topic to legal considerations for Industrie 4.0? Are there any other IT security risks specific to the blockchain?

What are the issues and challenges for Industrie 4.0?

- Any potential IT security risks must be identified so that they can be included in the risk analysis and the risks for each of the parties to a contract are taken into consideration when drafting the contract. This applies for example in respect to financing agreements for investing in or acquiring a blockchain startup. It also applies however to ensuring that important – yet commonly ignored – legal counsel is consulted when blockchain applications are being developed.

B: Legal Assessment

IT security: Blockchain-specific risks

Confidentiality of data

Data security aims to protect data integrity (no unauthorized or not completely verifiable alterations of data), data availability (access to data is possible) and confidentiality of data (only authorized individuals may access the data). To summarize, blockchain technology provides a degree of IT security previously not possible regarding data integrity and accessibility, due to its distributed database structure and immutability of the transaction blocks acknowledged with a consensus mechanism. If data is corrupted or blocked at a particular node, this is irrelevant because this data is available at the other nodes and the blockchain protocol ensures that the corrupted data can be corrected again at the affected node.

However, the blockchain is not as secure regarding data confidentiality. Blockchain technology is based on the fact that all of the data blocks of a specific blockchain protocol are available to each operator of a node. Encryption is the only tool used to maintain confidentiality of participants or transaction data.

As things stand at the moment, the encryption technology currently used is secure – this however will change. The progress being made in developing a "quantum computer" poses a substantial threat in this context. Quantum computers will be able to conduct complicated computations much more quickly than today's computers. As soon as this technology becomes available for use, we must assume that today's coding methods will no longer provide any security.

For instance, if a company develops blockchain applications today, a risk analysis must factor in the fact that in just a few years it will possible to decrypt the data and make it visible. If the data is to remain confidential, the blockchain application must be designed such that new and more secure coding systems can also be subsequently applied to the current and historic transaction blocks. This also means that there must be clear contractual obligations for participants in a blockchain application, so that the known risk can be monitored with joint obligations for blockchain activities. However, such enforceable contractual obligations are only conceivable for private blockchains. The identity of individual participants of such blockchains is always known, in contrast to typical public blockchains. The implementation and use of a private blockchain must be contractually specified in detail between these participants.

Data authenticity

The data availability and integrity inherent in blockchain applications does not however mean that the data stored on the blockchain is correct. Data availability and integrity only means that the data stored on the blockchain is available and cannot be modified. If "false" data is entered on the blockchain, this data remains "false". This may sound trivial at first, but it is very important. Especially in the industrial sector, blockchain applications depend on data being "true". For example, if it is important to track whether a medication really comes from the manufacturer, there must be certainty that the transaction data stored in the data blocks was confirmed by a reputable source. This involves the transaction data that was entered, for example, by the product manufacturer directly into the blockchain. It also involves the data transmitted to the blockchain from external sources, from an oracle (e.g. a data provider outside of the blockchain, or also sensors). If for example proof must be provided that the refrigeration chain for a certain product has been continually maintained, it is necessary to verify that the sensors transmitting the temperature to the blockchain have not been corrupted.

This must be factored into the contract and may not be ignored under the (false) assumption of unlimited data security.

IT security: known risks that remain

The usual security mechanisms of IT compliance observed in many companies must still be applied when using the blockchain. Non-compliance (and not a lack of "blockchain security") has in the past regularly caused IT security gaps and is the reason why it was possible to steal cryptocurrencies in such massive amounts. If the operator of a trading platform for cryptocurrencies does not observe (standard) IT security requirements, it is easy (despite the per se secure blockchain) to steal a digital asset such as a cryptocurrency.

Accordingly, the most common IT security threats still exist for software, even in the blockchain. Because a blockchain application is nothing other than a software product used to solve a technical task, programming errors can be provide a gateway to penetrate systems.

Furthermore, the principles of safe handling of access data must be observed. To execute transactions using a blockchain application, the participants must identify themselves with a 'private key'. The private key is actually simply a password. If the private key becomes accessible to third parties, they can conduct transactions in place of the authorized individual.

C: Options and Recommendations for Action

- IT security threats must be identified so that they can be allocated when drafting contracts, and minimized when designing a blockchain application.
- Previous issues of IT security still also apply to the blockchain, but not with respect to data integrity and availability.

AUTHORS

Dr. Duisberg, attorney-at-law (Bird & Bird) | Dr. Philipp Haas, attorney-at-law (Robert Bosch) | Dr. Nils Hullen (IBM Germany) | Thomas Kriesel (Bitkom) | Ted Kroke, attorney-at-law (Jones Day) | Martin Schweinoch, attorney-at-law (SKW Schwarz Rechtsanwälte) | Dr. Nick Wittek, attorney-at-law (Jones Day)

This publication is a contribution to the debates of the Platform Industrie 4.0.
It is based on the results of the Legal Framework Work Group (WG 4).

www.plattform-i40.de