Legal Aspects of Blockchain Technology for Industrial Use Cases

Markus Kaulartz[1], Jonas Gross[2], Constantin Lichti[3], Philipp Sandner[4]

Funding authority: German Federal Ministry of Education and Research (BMBF)

Research project: Kollaborative Smart-Contracting-Platform für digitale Wertschöpfungsnetze (KOSMoS)

Funding code: 02P17D020

Publication date: March 2022

[1] CMS Hasche Sigle.
[2] Frankfurt School Blockchain Center at the Frankfurt School of Finance & Management GmbH, Germany.
[3] Frankfurt School Blockchain Center at the Frankfurt School of Finance & Management GmbH, Germany. Corresponding author, constantin.lichti@fs-blockchain.de.
[4] Frankfurt School Blockchain Center at the Frankfurt School of Finance & Management GmbH, Germany.

Preamble

This report discusses important legal topics around blockchain technology for the jurisdiction of Germany. In particular, it addresses legal issues in the context of industrial use cases of blockchain technology. In this vein, it is designed as a handbook for industrial and financial companies that intend to start – or have already started – blockchain-related projects seeking legal input. As both blockchain technology and legal aspects are not always clear and complex, this report seeks to provide clarity around important legal questions in this context. This report covers a wide array of legal questions around blockchain technology, such as: Can a smart contract replace a physical contract? Can an entry on a blockchain be used as evidence in court? How are proper audits ensured? Who is liable in case of a hack? Which important aspects does a company need to consider around blockchain-based identities, data privacy law, and license requirements? If you seek answers to these questions, we highly recommend reading this report.

About KOSMoS

This publication is a joint publication by the Frankfurt School Blockchain Center (FSBC), Datarella, and CMS Hasche Sigle, and is part of the KOSMoS project, a research project funded by the German Federal Ministry of Education and Research (BMBF) under the funding code 02P17D020. The Frankfurt School Blockchain Center gGmbH and Datarella GmbH are part of the “KOSMoS” consortium. Together with partners from the industry (Schwäbische Werkzeugmaschinen GmbH, Alfred H. Schütte GmbH & Co. KG, ASYS Automatisierungssysteme GmbH), academia (Universität Stuttgart, Hochschule Furtwangen), and software development (inovex GmbH, Ondics GmbH), they created a blockchain-based solution allowing manufacturing companies to establish a DLT-based framework for producing machines in order to (a) execute dynamic leasing contracts, (b) provide transparent maintenance documentation, and (c) ensure high-quality documentation of manufactured products. More details about the consortium can be found in Section 9.

Table of Contents

Preamble **II**

About KOSMoS **II**

Table of Contents **III**

About the Authors **V**

1. Blockchain as Evidence in Court **1**

1.1 Introduction 1

1.2 Evidence of a blockchain transaction in civil proceedings 1

1.3 Evidence assessment of a blockchain transaction 5

1.4 Agreements between the parties on the assessment of evidence 5

2. Does a Smart Contract Replace a Physical Contract? **6**

2.1 Introduction 6

2.2 The smart contract as a contract in the legal sense 7

2.3 Use cases for smart contracts 8

2.4 Deviations between smart contract and legal contract 8

2.5 How to connect a smart contract with a legal agreement 9

3. License Requirements for Leasing, Factoring, and Sales Financing **10**

3.1 Introduction 10

3.2 Necessity of a permission for financial leasing 10

3.3 Circumvention of the licensing requirement 11

3.4 Use of a third party's permission 12

3.5 Permission for factoring 12

3.6 Permission for sales financing 13

4. Audits **14**

4.1 Introduction 14

4.2 Audit requirements 15

4.3 Direct obligation for audits 15

5. Data Protection Law **17**

5.1 Introduction 17

5.2 Introduction to data protection law 17

5.3 Location of the computer nodes 18

5.4 Personal data 19

5.5 Machine data 20

5.6 Obtaining "prohibited" data by automatic transmission 20

6. Governance **23**
6.1 Introduction 23
6.2 Legal organization of a collaborative consortium 23
6.3 Cross-border governance 25
7. Liability **26**
7.1 Introduction 26
7.2 Protection in case of misjudgements 26
7.3 Liability in case of incorrect implementation of smart contracts 29
7.4 Liability reasons 29
7.5 Who is liable if the smart contract was audited? 31
8. Identities **32**
8.1 Introduction 32
8.2 Anonymization of identities 32
8.3 Compliance of machine data 34
9. Additional information about the KOSMoS project **35**
Endnotes **37**

About the Authors

Dr. Markus Kaulartz *is a lawyer at CMS Hasche Sigle. The focus of his work is on contract negotiations, the structure of token-based business models, Decentralized Autonomous Organizations (DAOs), token sales, Decentralized Finance (DeFi), crypto exchanges (including DEXes), the metaverse, and legal audits of smart contracts. Besides, he focuses on challenges arising from the increasing digitalization (FinTech, Blockchain, IoT, Smart Contracts, AI, Tokens, SaaS, etc.). He has gained a lot of experience in advising on legal issues regarding future technologies and new business models. As a former software engineer and now lawyer, Markus has particular tech expertise and insights that contribute to his legal advisory practice. His input is often sought where issues emerge at the interface of technology and law. Markus is co-editor of the legal handbook on smart contracts and the legal handbook on artificial intelligence and machine learning.*

Jonas Gross *is a project manager and research assistant at the Frankfurt School Blockchain Center (FSBC) and also works for the KOSMoS research project. Further, Jonas is Chairman of the Digital Euro Association (DEA), co-host of the German podcast "Bitcoin, Fiat, & Rock'n' Roll", and member of the expert panel of the European Blockchain Observatory and Forum. His main research focuses are central bank digital currencies, stablecoins, and cryptocurrencies. You can contact him via email (jonas.gross@fs-blockchain.de), LinkedIn (https://www.linkedin.com/in/jonasgross94/), and via Twitter (@Jonas__Gross).*

Constantin Lichti *is a research associate and project manager at the Frankfurt School Blockchain Center and also works for the KOSMoS research project. As a doctoral candidate (PhD) at the Johannes Gutenberg University Mainz, his research interests include Bitcoin and public blockchain adoption, as well as how the discourse on blockchain technology is reflected in (social) media. He graduated from the Technical University of Munich with a master's degree in industrial engineering and management. You can contact him via email (constantin.lichti@fs-blockchain.de) and LinkedIn (https://www.linkedin.com/in/constantin-lichti-5644b9109/).*

Prof. Dr. Philipp Sandner *is head of the Frankfurt School Blockchain Center (FSBC) at the Frankfurt School of Finance & Management. In 2018, he was ranked as one of the "Top 30" economists by the Frankfurter Allgemeine Zeitung (FAZ), a major newspaper in Germany. Further, he belongs to the "Top 40 under 40"—a ranking by the German business magazine Capital. The expertise of Prof. Sandner, in particular, includes blockchain technology, crypto assets, distributed ledger technology (DLT), Euro-on-Ledger, initial coin offerings (ICOs), security tokens (STOs), digital transformation, and entrepreneurship. You can contact him via mail (email@philipp-sandner.de), via LinkedIn (https://www.linkedin.com/in/philippsandner/), or follow him on Twitter (@philippsandner).*

1. Blockchain as Evidence in Court

This chapter addresses the question of how a blockchain transaction must be structured so that it can be used as evidence in court. Based on the following types of formal evidence – namely (1) expert opinion, (2) documents/deeds, (3) inspection or visual evidence, and (4) witnesses and party hearings – we analyze the evidence assessment of a blockchain transaction in detail. The chapter analyzes the laws and rules of the jurisdiction of Germany.

1.1 Introduction

Blockchain technology is becoming increasingly renowned as more and more companies continue to develop blockchain-based prototypes, e.g., in the context of payments, digital identities, and the supply chain. One use case of blockchain is often seen in the tamper-proof storage of information and documentation of facts. This is due to the fact that **records on a blockchain are "practically resistant" to manipulation as a consequence of the underlying cryptography and the consensus mechanism.**

If a blockchain is used for storing information, the question arises of whether the data stored on a blockchain can be used as evidence in court. In the following chapter, we will analyze this question.

1.2 Evidence of a blockchain transaction in civil proceedings

First of all, it is important to understand that evidence in court is not necessary in every court case but only when the other party contests a fact. In the scope of this paper, this could, for example, be the case with regard to the immutability of blockchain transactions or the source from which a blockchain transaction has been submitted. Before information from/on a blockchain will be considered by a judge, it must be entered into evidence in the court case. In civil proceedings in Germany, the principle of the so-called strict evidence (in German: "Strengbeweis") procedure is typically applied. This means that the parties are bound by the formal evidence procedure reflected in the five different types of evidence (§§ 355 et seq. ZPO): experts, documents/deeds, inspection, witnesses, or party hearings.

Expert opinion

An expert opinion is one way of using information stored in blockchains as evidence in court. If the court considers this request for evidence to be relevant to its decision, it appoints an expert to investigate the facts. The parties have no influence on the choice of the expert but can typically make suggestions.

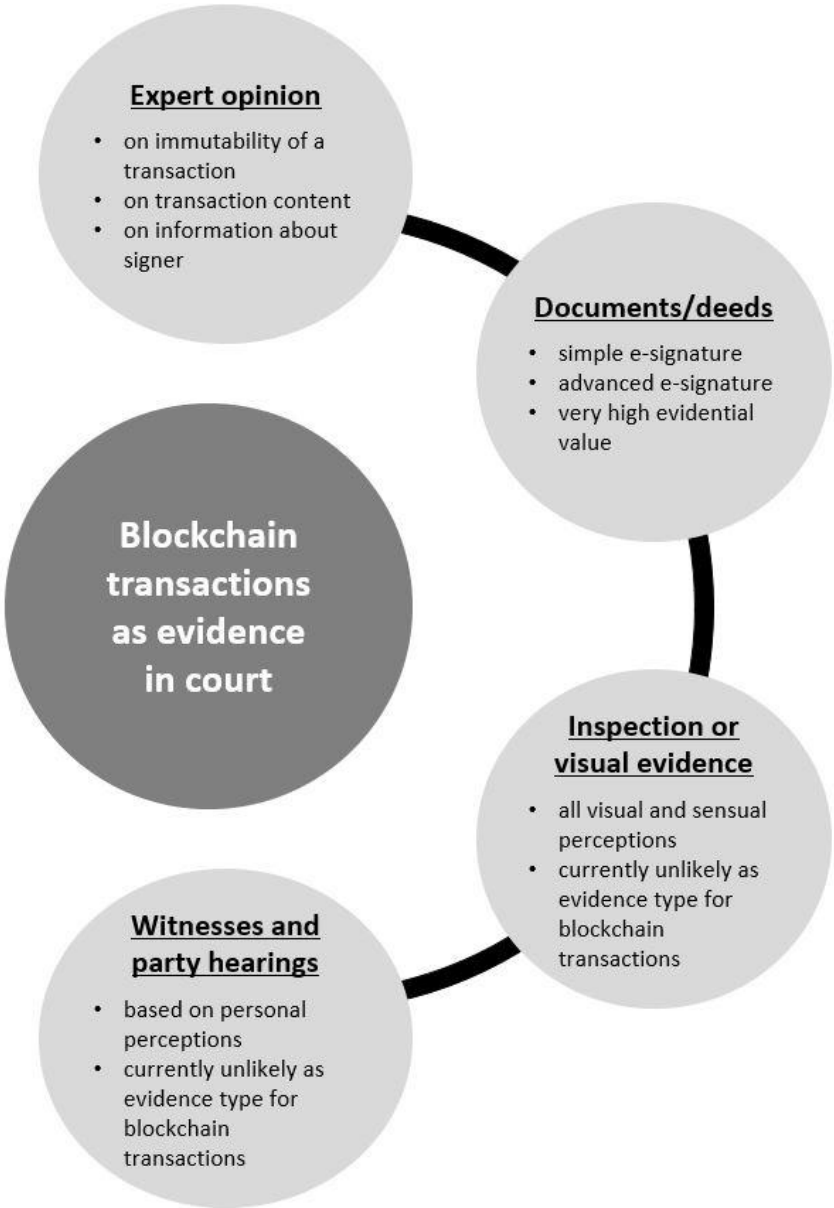
After examining the facts, the expert presents his or her opinion, usually in a written report, and is also invited to an oral hearing. Examples of facts that may need to be proven and

confirmed by an expert include the immutability of a transaction, information about the person who signed a blockchain transaction, or the content of blockchain transactions.

> ***Practical note:*** *The technical structure of the system and the use cases based on the blockchain system should be sufficiently documented so that an expert can easily familiarize herself with it in order to work out the desired information.*

Apart from its high evidential value for the court, there is another clear advantage of expert evidences in court: Experts' opinion may, once written down, be used in other proceedings, too (§ 411a ZPO). This can be useful if the same technical question has to be assessed in different proceedings. This can be the case, for example, if several customers sue a blockchain service provider.

Figure 1: Different types of evidence of a blockchain transaction in civil proceedings



Documentary evidence/deeds

Deeds (in German: “Urkunden”) may prove the fact that the declaration contained therein originates from the issuer (§§ 415, 416 ZPO). A deed has a very high evidential value.

Deeds under German laws typically require a (hardcopy) written form. A blockchain transaction, of course, does not fulfill this requirement. According to § 371a ZPO, however, the provisions of the documentary evidence also apply to electronic documents if these have been signed with a so-called qualified electronic signature.

Since blockchain transactions are signed with a private key, they could, strictly speaking, qualify as having such an electronic signature. However, the signatures used in blockchains are generally simple or advanced electronic signatures but not qualified electronic signatures as required by § 371a ZPO.

- A **simple electronic signature** is data in electronic form which is attached to or logically linked to other electronic data and which the signatory uses for signing (Art. 3 No. 10 eIDAS Regulation). Example: Email signature but also typically the signature of a blockchain transaction.

- **Advanced electronic signatures** fulfill the following requirements according to Art. 26 eIDAS-VO:
    - They are clearly assigned to the signatory.
    - They enable the signatory to be identified.
    - They shall be created using electronic signature-generating data which the signatory can use with a high degree of confidence under his sole control.
    - They are connected to the data signed in such a way that any subsequent change in the data can be detected.

- **Qualified electronic signatures** are based on advanced electronic signatures and are distinguished from these by the fact that they are created by a so-called “qualified electronic signature creation device” (Art. 3 No. 23 eIDAS Regulation) and are based on a “qualified certificate for electronic signatures” (Art. 3 No. 15 eIDAS Regulation). The qualified electronic signature creation device itself comes along with high requirements in practice: It is a configured software or hardware solution that is used to create an electronic signature. In particular, the keys have to be created by a so-called “qualified trust service provider”, of which there are currently only a handful in Germany. The reason behind these stringent requirements is to ensure that private and public keys can reliably be assigned to an identified person (Art. 24 (1) subsection (1) eIDAS Regulation).

We believe that blockchain signatures should typically be qualified as advanced electronic signatures in terms of Art. 26 eIDAS-VO. If one assumes immutability of blockchain transactions, the unique public key is suitable to identify the signer, and the private key is typically in the sole control of the signer. However, the requirements for a qualified electronic signature may only apply in individual cases. If a blockchain is actually implemented in such a way that transactions are signed electronically in a qualified manner, and if a trusted service provider has been found who is able to provide the necessary infrastructure, the requirements of § 371a ZPO would be fulfilled, and a blockchain transaction would have an evidential value

similar to a written document. To the best of our knowledge, this has not yet been implemented in practice. Therefore, blockchain transactions “only” have the evidential value of simple electronic documents but not the same evidential value as paper deeds.

The current legal position of blockchain transactions is that they can only be used as documentary evidence if they are provided with a qualified electronic signature.

Visual evidence

The advantage of the visual evidence (§§ 371 ff. ZPO) is, in particular, the low effort required and the resulting lower or non-existent costs. All externally ascertainable facts can be the object of such evidence as long as the judge can perceive them on his/her own. Accordingly, not only visual perception but all sensual perceptions are covered so that the perception of technical recordings, copies, printouts, or data output on a computer screen are also covered. This also includes electronic documents, including advanced electronic signatures (see above).

> ***Practical note****: Blockchain transactions should be structured in such a way that the stored information is provided to the judge easily and in a way that is comprehensive, clear, and simple. The presentation of information must enable a judge to recognize, understand and appreciate all relevant information. If the blockchain system, through simple, structured, and understandable output, allows for verification of the authenticity of all transactions, this data can be used as visual evidence.*

In view of the current complexity of blockchains and the little widespread knowledge about them, it can be assumed that a court will use an expert or even documentary evidence. At the moment, visual evidence is unlikely to be of great importance regarding blockchain transactions.

Proof by witnesses and examination of parties

Last but not least, evidence from witnesses or the hearing of parties is also a valid form of evidence in court. Nevertheless, this kind of evidence will be of rather minor importance, regardless of the concrete form of the blockchain transaction. Although witness evidence is probably the most frequently used means of evidence in practice, only the witness’s own perceptions are subject to evidence. This means that a witness could only report on her perception of the blockchain transaction, and this report would be the basis of the evidence.

It is conceivable, for example, that a developer of a blockchain system could be asked to provide evidence of the functionality and immutability. The court will hear the witness and then assess their credibility. Since solely the testimony of the witness is relevant, the evidentiary value of the blockchain, due to its immutability or the concrete form of the transaction, is not relevant.

1.3 Evidence assessment of a blockchain transaction

If the blockchain transaction was brought to court as visual evidence, by a witness, or through expert evidence, the court is free in its assessment of the information. Deeds provide full proof regarding their originators' declarations. It is important to understand, however, that the court may not deny the blockchain transactions' legal appearance and admissibility as evidence in court proceedings solely with the argument that they have only been presented in electronic form or because they do not meet the requirements for qualified electronic signatures (Art. 25 (1) eIDAS Regulation).

1.4 Agreements between the parties on the assessment of evidence

The parties developing and governing a DLT system could agree on a framework agreement on the blockchain's role as evidence in court. This is advisable as long as the free assessment of evidence by the judge is not limited. The goal of such an agreement could be bringing the evidentiary value of a blockchain transaction close to a paper deed, although a blockchain transaction is no such paper deed (see 1.b, above). This would make it possible to avoid the need for a costly expert opinion.

Of course, such an agreement is more appropriate in private blockchains than in public blockchains, since in private blockchains, all parties involved are known and typically expect their relations to be based on a contractual basis.

> ***Practical note****: In the framework contracts underlying the DLT-based use cases, expert evidence could be excluded, and it could be agreed, for example, that blockchain transactions, if confirmed by a specific number of nodes, are deemed to have been submitted by the party that signed them.*

There may be residual risks in such an agreement, as the court would also be able to take evidence of its own motion. However, this risk seems low if the party burdened with evidence does not, because of such an agreement, file a request for evidence.

2. Does a Smart Contract Replace a Physical Contract?

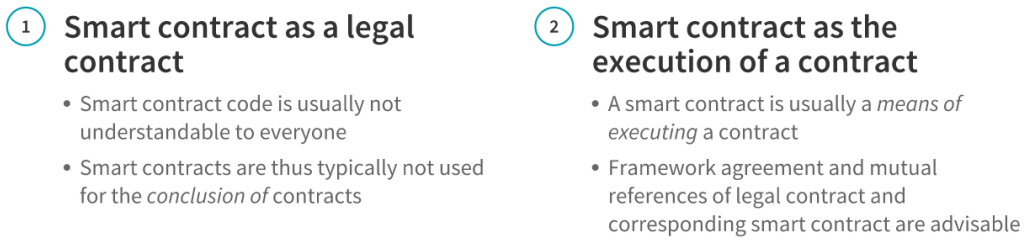
In this chapter, we analyze whether a smart contract can replace a physical contract set up between various business parties from a legal perspective. We differentiate in our legal assessment between 1) the smart contract *itself* being the text of the contract, and 2) the smart contract only being used to *execute* a contract concluded elsewhere. Furthermore, we offer suggestions for practical implementation. The chapter focuses exclusively on German laws.

2.1 Introduction

One of the advantages of using blockchain technology to store information and manage business processes is that smart contracts can be used. Smart contracts specify a set of promises digitally in a protocol that automatically executes the terms of the contract.[1] In programming terms, smart contracts are comparable to “if-then” functions, which define specific actions if a particular event takes place. Technically, smart contracts have three key features: 1) programming capabilities, 2) they can define the properties of money, and 3) they enable tokenization. An example: One can think of a situation in which, if the delivery of a good has been successful (“if”), a subsequent payment is made automatically (“then”). Smart contracts become particularly relevant in the context of issuance and trading of securities because they have the potential to “codify” the rules applicable to such securities.

Due to the term “smart contract” one could assume that smart contracts replace physical contracts. However, this only holds true under very limited conditions. In this chapter, we discuss under which circumstances it is legally possible for a smart contract to replace a physical contract but also outline how smart contracts are used from a legal perspective in practice.

Figure 2: Differentiation of smart contracts in a legal sense



2.2 The smart contract as a contract in the legal sense

Whether a smart contract can replace a physical contract depends on whether the smart contract itself is the representation of the parties' will or is only used to execute a contract concluded with ordinary means. First, we will examine whether a smart contract can constitute a contract in a legal sense, i.e., whether the parties can write a contract text in code and thus conclude a legally binding contract.[2]

Principle: Freedom of contract

A contract in the legal sense is concluded by two corresponding declarations of intent. As a rule, it is irrelevant how such declarations of intent are expressed – apart from possible mandatory formal requirements, such as in the case of real estate purchases. This principle results from the freedom of contract guaranteed in Article 2 (1) of the German Constitution. As an example: If a person in a bakery points silently at a bread, she expresses the intent to conclude a purchase contract for a bread. However, this is different if a hotel guest points to a bread at the breakfast buffet. These interpretations result from the objective view one has to take when assessing legal actions (§§ 133, 157 German Civil Code (BGB)): All circumstances of the individual case have to be taken into account, and it has to be evaluated how the general public would construe the given statement. In principle, therefore, it is irrelevant what exactly the person making the declaration actually intended.

We can apply this principle also to blockchain transactions using smart contracts: If a party signs a blockchain transaction and a smart contract is used in this context, the code of the smart contract could be used to interpret the content of the declaration the signee expresses. **For example, if the smart contract indicates that the blockchain transaction is to be used to pay a leasing rate and the smart contract subsequently gives the party access to a machine, signing the blockchain transaction could be seen as an offer to conclude a lease agreement.** Details could then be read from the code of the smart contract and perhaps other objective criteria.

However, in order for the smart contract to validly represent the parties' will to conclude an agreement as stipulated in the code, the contracting parties would have to be aware that they make a declaration in the legal sense when signing the contract (so-called "awareness of declaration", *Erklärungsbewusstsein*). In practice, this may typically not be the case.[3] **The code of a smart contract is not easily understandable to everyone** [4] and one may have doubts that a person signing a transaction actually and in detail knows the contents of a smart contract, understands it, and signs it with the intention to conclude a legally binding agreement without any reference to any text written in a natural language like English or German. This, of course, solely depends on the individual case, but we are convinced that in practice such cases will remain outside the norm and it is not advisable to build business models on the assumption that the smart contract code can be the basis for a legally binding contract, solely representing the will of the parties.

Execution of a contract through smart contracts

From a legal perspective, blockchain transactions and thus also smart contracts should be interpreted in light of their operation, for example, the transfer of a token or storage of information. **Smart contracts are thus typically used in the *execution of* contracts, not in the *conclusion of* contracts.** Smart contracts can be used, for example, to transfer a security via an exchange under applicable security terms or to conduct payments in order to fulfill obligations under a lease agreement. The latter is implemented in the leasing use case of the KOSMoS project. These payments can also be made automatically after predefined conditions are met, e.g., after a machine has been used.

2.3 Use cases for smart contracts

Given the role of a smart contract as an instrument of executing a legal contract in a legally compliant way, a smart contract could be used to enforce a physical maintenance contract or a leasing contract. Both use cases are exemplified within the KOSMoS project.

It is not possible to provide a general answer regarding which concrete contractual performance can be executed through smart contracts. One requirement is certainly that the relevant performance stipulated in the legal agreement can be performed via a blockchain, in contrast to obligations that require a real-world action, like repairing a machine. Therefore, smart contracts can be qualified as suitable means if digital assets, which can be represented by tokens, are subject to the agreement. This, for example, applies to all crypto currencies, tokenized securities, or stablecoins.

If a smart contract is used to perform an obligation contractually agreed upon between the parties, it must be ensured that this performance corresponds precisely to what has been agreed upon legally. It is important to understand that the legal and the smart contract can run parallelly but the smart contract executes the performance agreed upon in the legal agreement.[5] If this is not the case, the obligation is not fulfilled. Typical scenarios in which the smart contract code deviates from what has been agreed upon in the legal agreement are those where the legal agreement uses undefined terms (for example “pay duly in advance”), or a statutory provision applicable to the agreement has not been implemented in the code (for example consumer withdrawal rights).

2.4 Deviations between smart contract and legal contract

This raises the question on how to proceed if the smart contract (i.e., the execution of the contract) differs from the contract in the legal sense.[6]

> ***Example**: In a framework agreement, the parties state that the leasing rate for a machine is 5 EUR per minute. However, an amount of only 4 EUR per minute has been coded in and transferred via the smart contract.*

In this case, the creditor is still entitled to the payment of the leasing rate minus the amount already paid. The creditor can enforce this claim beyond smart contracts in the “old

world". The creditor can also withhold her remaining services with reference to the outstanding debt (so-called right of retention), and can, of course, demand default interest on the outstanding amounts (§§ 286, 288 BGB).

In practice, we advise documenting the exchange of delivery and payment so that even if errors should occur, outstanding claims could be fulfilled easily. For this purpose, smart contracts need to be designed in such a way that they can fulfill obligations triggered by single transactions. This would, for example, allow the settlement of monetary claims without having to leave the system.

> ***Practical note****: In case a conflict arises as to which services of the smart contract have been fulfilled and which obligations have been contractually agreed upon, a resolution mechanism can be helpful.[7] Therefore, setting up a framework agreement with various stages for conflict resolution is crucial. In the first stage, it should be agreed upon which party's representatives will bindingly decide on conflicts, as well as on the basis of which procedures and databases these decisions will be made. In the second stage, a mediator could try to resolve the conflict. In the last stage, an arbitration tribunal would be called upon. The basis would be an arbitration clause included in the framework agreement. Through this solution, the conflict does not need to be brought before a state court but can be decided by a private arbitration court, which would ideally be staffed with arbitrators who have the necessary expertise and technical knowledge.*

2.5 How to connect a smart contract with a legal agreement

In principle, it is irrelevant how debtors fulfill their obligations, i.e., whether they pay a monetary debt in cash, by bank transfer, or by using a smart contract (unless explicitly agreed upon otherwise). **The challenges are, therefore, the same as with physical contracts**: Thus, it must be possible to clearly assign the requirements to a concrete obligation or contract but also to a concrete debtor and creditor.

There are no legal requirements on how this connection should be made. Rather, based on practical considerations and concrete implementation, it should be examined how a smart contract and a legal agreement can be connected in the most sophisticated way. This is possible by drafting the document which represents the legal agreement in such a way that there is no doubt regarding the debt to which the smart contract corresponds.

> ***Practical note:*** *We recommend attaching references to the corresponding contracts i.e., clearly connect the legal agreement through its text (code) with the smart contract and vice versa. The smart contract could also be included as an appendix to the text of the legal agreement. Furthermore, debtors and creditors should be clearly identifiable, for example, through their public keys.*

3. License Requirements for Leasing, Factoring, and Sales Financing

In this chapter, we analyze under which circumstances companies providing specific financial services require regulatory approval from a legal perspective. We differentiate in our legal assessment between (i) finance leasing, (ii) factoring services, and (iii) sales financing. Furthermore, we offer suggestions for the practical implementation. The chapter assumes the application of German laws.

3.1 Introduction

Blockchain technology enables various new and innovative business models, e.g., related to pay-per-use. As one example, dynamic leasing use cases can be implemented efficiently on a blockchain. The lessor provides a machine to the lessee. In the case of dynamic leasing, the leasing fee is variable and depends on the use of the machine, the maintenance, material used, etc. In contrast to current leasing arrangements, the leasing fee is dynamic. This can easily be implemented by using smart contracts.

As such pay-per-use business models have been getting more and more attention in the German industry, in this chapter, we analyze related legal requirements. We focus on the situation wherein the lessor has to get a license in order to provide such leasing services. Furthermore, we discuss license requirements for factoring services and sales financing.

3.2 Necessity of a permission for financial leasing

According to § 32 (1) of the German Banking Act (KWG), companies that intend to provide financial services in Germany on a commercial basis or to an extent that requires a “commercially-oriented business operation” require the written permission of the Federal Financial Supervisory Authority of Germany (BaFin). **Financial leasing** is one such financial service. As described in § 1 (1a) sentence 2 no. 10 KWG, companies offer financial leases if, among others, they conclude finance lease contracts as lessors. The requirement of a commercial operation is fulfilled if the business is intended to run for a certain duration and the operator intends to make profits. Whether the business in question can be seen as a “commercially-oriented business operation” depends exclusively on whether or not the setup of said operation is objectively necessary for the financial services business.

Let us consider the following example: We assume that there is a company B, which operates a blockchain, and a financial lease company A, which is in contact with customers and possesses a corresponding license from BaFin in the sense of the earlier discussed § 32 (1) KWG. Since in this given case company A conducts financial leasing, but company B does not, the latter does not require permission under § 32 (1) KWG. Company B only acts as a third party whose infrastructure is used by the contracting parties to execute the financial lease. The situation is comparable to a software company making a software product available to a customer who uses it to provide services. All regulations applicable to these services,

including any licensing requirements, apply only to this customer as only this customer is responsible for the execution of the services. The software provider is only obliged to provide its software free of errors. Thus, as long as company B itself does not act as lessor in any way and only operates the blockchain infrastructure, B is not subject to the licensing requirement of § 32 (1) KWG. It is not even relevant whether A and B are affiliated companies.[8]

> ***Practical note****: A permit to conduct financial services is required by the party providing the service, not by whoever operates the technical infrastructure.*

This is also in line with the *ratio legis* of the obligation to obtain a permit under § 1 (1a) sentence 2 no. 10 KWG in conjunction with § 32 (1) KWG. From a purely economic point of view, a financial lease is a loan from the lessor to the lessee. However, this loan does not fall in the scope of the banking supervisory laws for the lending business under § 1 (1) sentence 2 no. 2 KWG because th**e financing** is legally not a loan. The reason is that the lessor acquires the legal power of disposal over the leased object and arranges the financing in such a way that the lessor acquires the right of use against payment. Therefore, a leasing agreement is similar to a rental agreement that is extended by elements for an eventual purchase. Due to the central importance of financial leasing (and also factoring, which will be discussed later in the chapter), the legislator sees risks that may cause disruptions in such transactions that could affect not only the lessee but also major parts of the economy.[9] This is the reason why providers of financial leasing are subject to the supervision of BaFin. Thus, the critical aspect of the licensing requirement under § 32 (1) KWG is solely the **financing function** within the contractual relationship of a leasing agreement. Consequently, only A as a financier and not company B as a pure auxiliary party to the contract is placed under supervision.

> ***Practical note****: The company operating the blockchain or providing other technical services must ensure that in its advertising and product description, as well as in the contracts, the service is clearly limited to a technical service not regulated under the KWG.*

An example *of where the activity indicates that a permit is required: "We finance your car. Secured with the help of blockchain technology!"* An example *of where the activity does not indicate that a permit is required: "We offer the necessary IT infrastructure for your finance leasing business!"*

3.3 Circumvention of the licensing requirement

No permission is in general required in the following cases:

1. Legal exceptions

Under § 2 (4) of the KWG, BaFin may exempt a company from the requirement for a license as long as the company does not require supervision based on the nature of the conducted business. Such an exemption will only be considered in exceptional cases.

§ 2 (6) of the German Banking Act (KWG) stipulates general exceptions for certain types of companies. A large majority of the companies that fall under the term **financial services institution** due to their business being financial leasing are thus exempted from the licensing requirement.[10] § 2 (6) sentence 1 no. 17 KWG contains an exception to the licensing requirement for leasing property companies (Leasingobjektgesellschaften) that only operate for a single leased object. A precondition, however, would be that the company is in turn managed by a leasing company, which itself has a license from BaFin.[11]

2. Change of the business model

Furthermore, there is no licensing requirement if no financial leasing within the meaning of § 1 (1a) sentence 2 no. 10 of the KWG is being offered at all. The decisive factor for the existence of such a lease is whether or not the lessee is contractually integrated in such a way that he or she ultimately finances and amortizes the asset while the lessor only pre-finances the asset. Consequently, the manufacturer of a leased asset, for example, who uses leasing as a distribution channel and/or sells his product directly through leasing, does not fall under § 1 (1a) sentence 2 no. 10 KWG. This is due to that fact that the focus here – similar to an installment plan – is not on financing in general but rather on selling the product.[12] Similarly, a rental agreement or hire-purchase agreement for real estate can be structured in such a way that no license is required. However, the title of a contract does not play a role. Rather, it depends on its concrete content. The tenant or hire-purchaser is not allowed to be contractually integrated in such a way that he or she ultimately finances and amortizes the asset as well as bears the investment risk, as this would require a license.

3.4 Use of a third party's permission

The use of a third party's permission is not possible in the case of finance leasing. Therefore, the use of third party’s permission as in investment brokering in accordance with § 2 (10) KWG does not apply.

3.5 Permission for factoring

According to § 32 (1) half-sentence 1 in conjunction with § 1 (1a) sentence 2 no. 9 KWG, companies that wish to provide **factoring** services in Germany on a commercial basis or to an extent that requires a “commercially-oriented business operation” also require the written permission of BaFin. Factoring, i.e., the ongoing purchase of claims on the basis of framework agreements with or without recourse, thus constitutes a financial service in the sense of the KWG according to § 1 (1a) sentence 2 no. 9 KWG. Therefore, the aspects discussed in the previous paragraphs for finance leasing also apply to factoring.

Necessity of a permission

Parties who merely provide the technical infrastructure but do not operate factoring themselves do not require permission from BaFin. The licensing requirement is exclusively linked to the fact that claims are continuously purchased based on framework agreements (§ 1 (1a) sentence 2 no. 9 KWG). Therefore, analogically, the licensing requirement is solely linked to the financing function.[13]

Circumvention of the licensing requirement

In the case of factoring, there is no sectoral exception as for single object leasing companies (§ 2 (6) sentence 1 no. 17 KWG), but individual exemptions under § 2 (4) KWG would be possible in certain cases (see legal exceptions for financial leasing).

Furthermore, it would also be possible to adjust the business model to avoid the licensing requirement for factoring. If the requirements of § 1 (1a) sentence 2 no. 9 KWG are no longer fulfilled (and if there is also no credit business as defined by § 1 (1) sentence 2 no. 2 KWG), the business in question is no longer subject to license requirements. There are essentially two possibilities for avoiding a license requirement:

- If a purchase of claims does not take place "on an ongoing basis and on the basis of framework agreements", the business process will not qualify as factoring within the meaning of § 1 (1a) sentence 2 no. 9 of the KWG.[14] One example would be that the company providing factoring services does not offer a financing service to the customer in general or wants to consider this on a case-by-case basis.
- Moreover, in the case of the assignment of claims already due (so-called maturity factoring), § 1 (1a) Sentence 2 No. 9 KWG does not apply if the company providing factoring services assumes the risk of loss of claims.[15]

Use of a third party's permission

The use of permission from a third party is not possible for factoring. Therefore, it is similar to the case of finance leasing.

3.6 Permission for sales financing

The term 'sales financing' refers to the conclusion of a loan agreement where the loan is exclusively used to finance a specific contract for the acquisition of certain goods or services. Sales financing is typically not subject to a permission or a license. If a seller credits his own sales by deferring the price (not: converting into a loan), it is not engaged in the lending business. This applies even in case the seller charges interest on the deferred amount. The reason for this is that, although the seller gives the buyer a credit, this credit is not based on a loan agreement, but solely on an “atypically structured” purchase agreement. [16] A differing legal understanding applies only to special constellations, for example, when an existing debt, e.g. from a purchase contract, is not only deferred but converted into a loan.

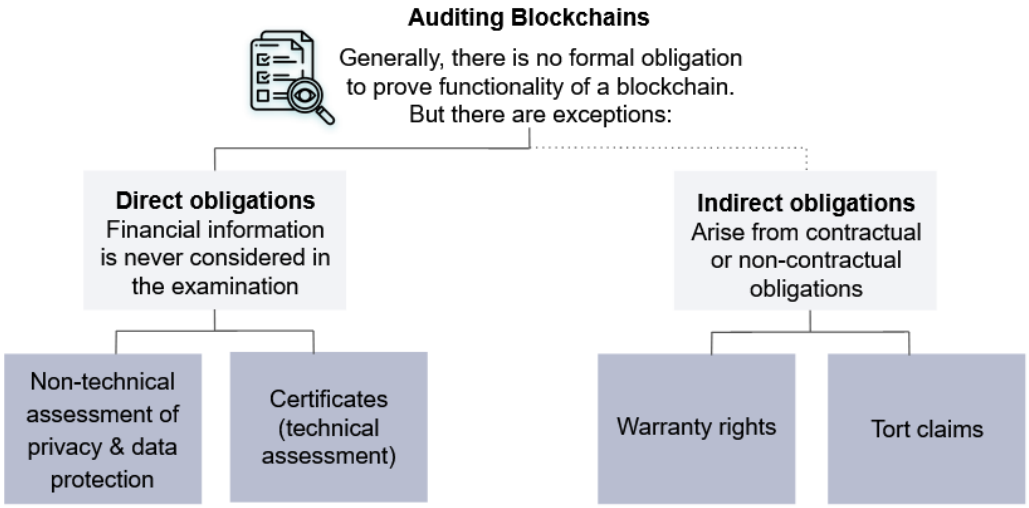
4. Audits

In this chapter, we analyze whether information systems such as computers or IT infrastructure technologies such as blockchain technology are subject to a legal obligation for audits or some other form of functional verification prior to their use. In addition to general audit requirements, we examine in particular the direct obligation and the indirect obligation for the execution of audits. Also, we address further aspects such as privacy and data protection consequences, the role of certificates, warranty rights, and claims based on tort. The chapter assumes the application of German laws.

4.1 Introduction

Blockchain technology holds immense potential and will be an important building block advancing digitization in the future due to its wide range of possible applications. However, as blockchain applications become more and more important in the business world, fundamental questions arise for both consumers and companies regarding issues such as audits, guarantees of functionality, and possible legal claims in the event of non-compliance regarding certain functionality. In order to ensure a legally secure basis for all parties and participants, it is therefore important to clarify any questions of liability, for example, in the event of damages. Without absolute certainty in these matters, companies will find it difficult to implement blockchain-based business models. Therefore, in this chapter, we discuss related issues and draw conclusions based on current German law.

Figure 3: Auditing Blockchains – An overview



4.2 Audit requirements

In principle, there is no formal obligation under German law to test a computer, IT infrastructure or blockchain (hereinafter simply referred to as the "system") prior to using or verifying its functionality otherwise. However, there are some exceptions, which will be discussed in the following sections. Furthermore, there can also be an indirect obligation to audit such systems under certain circumstances, which will be analyzed in the second part of this chapter.

4.3 Direct obligation for audits

When an audit is conducted to assess a company, the audit is always an independent examination of its financial information. Regardless of its size or legal form, and regardless of whether the company being audited is a for-profit company or not.[17]

Assessment of privacy and data protection consequences

The party responsible for privacy and data protection must, if necessary, carry out an assessment of the consequences of the intended processing operations for the protection of personal data before commissioning a system in accordance with Section 35 (1) of the General Data Protection Regulation (GDPR). This is primarily the case when a form of processing, in particular when new technologies are used, is likely to present high risks concerning the rights and freedoms of natural persons due to the nature, scope, context, and purposes of the processing. The **data protection impact assessment** is mainly a legal assessment of the processing situation, including, for example, risks and measures that can be taken (Art. 35 (7) GDPR). Its focus is, therefore, not on the technical assessment of a system. In any case, it also requires that personal data is processed in the first place, i.e., information relating to an identified or identifiable natural person (Art. 4 (1) GDPR). This is not the case for machine data without any reference to a natural person.

Certificates

Certificates can play a role in proving compliance with certain rules or minimum standards. Article 32 GDPR, for example, stipulates the technical and organizational measures that are to be implemented to protect personal data. Such measures can be verified, at least in part, by ISO 27001 certification.[18] Certificates can also help prove that the **statutory requirements for IT** have been implemented, for example, with regard to the BAIT [19], which must be implemented by financial service providers (including companies that offer factoring or finance leasing). However, certificates are typically not strictly mandatory, as IT compliance can also be demonstrated by other measures.

Warranty rights

If a company sells or rents an item or produces a good, it must be done in such a way that the item or product has the agreed quality at the time of the transfer of risk, e.g., the act of purchase and/or exchange of goods (Kaufrecht, § 434 (1) 1 (BGB) and Werkvertragsrecht, § 633 (2) 1 BGB). Further, the suitability for contractual use must not be reduced (Mietrecht, § 536 (1) 1 BGB). Otherwise, the person concerned may have warranty rights, such as the right to subsequent performance, reduction, withdrawal, or even claims for damages (purchase: § 437 BGB, rent: §§ 536, 536a BGB, contract for work: § 634 BGB). A notice period is typically required. Claims for damages based on product liability law are also possible if a product is defective, i.e., if it does not offer a level of safety that can reasonably be expected, taking into account all the circumstances, in accordance with § 3 of the German Product Liability Act (ProdHaftG).

With regard to the law on sales and contracts for work and services, only the **moment of handover or acceptance** is relevant, whereas, with regard to a rental contract as a continuing obligation, the suitability of the rented object must even be ensured for the **entire duration of the contract**. The same applies to product liability law for a period of ten years after placing the product on the market (§ 13 (1) 1 ProdHaftG).

If an audit is carried out before handover and the system is thus tested in advance to ensure that it is free of defects, such warranty rights and claims for damages could possibly be avoided. Consequently, an indirect obligation to audit systems can be derived from this.

Tort claims

In addition to contractual claims for damages due to insufficient performance (see warranty rights), a claim against the operator of the system could also arise from the fact that he or she unlawfully and wrongfully violates the legal duty to ensure safety. Another scenario is that he or she markets software that does not meet the state of the art. In contrast to contractual claims, a tort claim is generally available to any injured party, regardless of whether or not this party has priorly concluded a contract with the operator of the system. An audit that checks the security of the systems in advance can prevent claims against the operator.

5. Data Protection Law

In this chapter, we analyze how the topic of data protection, in particular the General Data Protection Regulation (GDPR), plays out specifically in the context of blockchain-based databases from a legal perspective. In our assessment, we distinguish between 1) personal data and 2) machine data. In addition, aspects such as the different legal frameworks and levels of data protection in different countries are addressed. Also, the question of handling company and trade secrets will be discussed. In each scenario, special attention is drawn to the issue of liability. The chapter assumes the application of German laws.

5.1 Introduction

With the General Data Protection Regulation (GDPR), the issue of data privacy has attracted attention in the public debate. On the one hand, every person and every company operating on the Internet provides and possibly discloses data. Data is produced through, e.g., search behavior using search engines. A vast amount of data is created and stored within companies. How does this relate to blockchain technology?

One way to describe a blockchain is to think of it as a decentralized database. Information can be stored on a blockchain in a decentralized way, and it can also be used to manage and automate business processes, e.g., through smart contracts. Therefore, the topic of data protection is closely related to the field of blockchain. There must be clarity on liability issues for all parties involved to ensure smooth, efficient, and, above all, secure handling of data. In this chapter, a distinction is made between personal data and machine data. Scenarios and issues as when private data such as trade secrets are obtained through automatic transmission on a blockchain shared by multiple actors will be addressed. The chapter also examines how the decentralized character of a blockchain, with nodes located in different countries with differing data protection laws, affects liability issues in the event of a potential damage claim.

5.2 Introduction to data protection law

With the GDPR, data protection law has been mostly standardized throughout Europe. The regulation only protects defined personal data (Art. 2 (1) GDPR): Personal data is information that relates to an identified or identifiable natural person (Art. 4 (1) No. 1 GDPR). In this context, it is sufficient if there is only a certain probability that a person can be identified.

Personal data includes, for example, the following information:

- Jane Sample lives in Any City.
- Description of persons: The boy with shoulder-length hair from Class 1b of school ABC in XYZ has a fountain pen.
- Text in exams: using text analysis, conclusions about a person can be derived.[20]

- IP addresses for website providers: via the Internet Service Provider, a specific person can be identified with reasonable effort.[21]

In contrast, no personal data are:

- 35 persons live in Any City (not referable to one person)
- Machine X is worth EUR 454,323 (not related to a person)

Data accrued by an industrial machine is typically not personal data. For instance, it is impossible to conclude from the information "machine was switched on from 8 am - 6 pm" which worker operated the machine and for how long. It would be a different case if information about the person operating the machine during a specific time was stored or if such information were otherwise obtainable. In this case, this data would be personal data. In the following, the term "machine data" refers to data that does not relate to natural persons and also does not allow for personal identification.

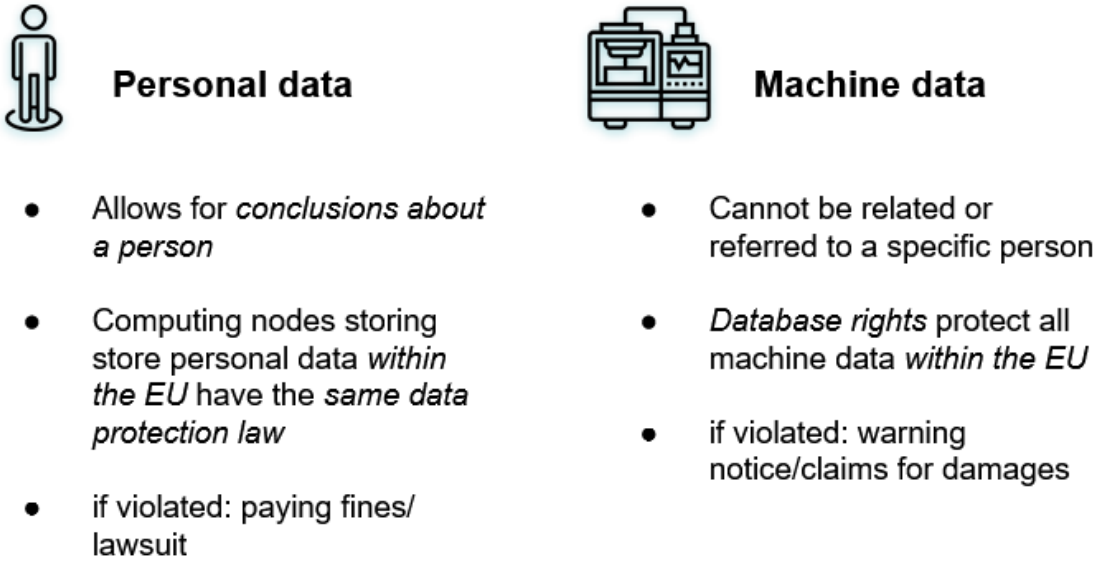
If there is personal data in the sense of the GDPR, a so-called "permission requirement" applies: it may only be stored, transferred, and used (processed) if this is permitted by data protection law (Art. 6 GDPR). The natural person in question("data subject") has various rights, e.g., the right of information according to Art. 13, 14 GDPR and the right of deletion according to Art. 17 GDPR. Also, the company is subject to certain obligations under Art. 5 GDPR. For example, personal data may only be collected and stored to the extent necessary for processing (Art. 5 (1) c GDPR).

Assuming a blockchain is to store, for example, information on which a natural person has carried out maintenance on a machine, for this purpose, only pseudonyms should be used, such as hash values. The decoding of these pseudonyms from raw data is carried out outside the blockchain using a conventional database. Suppose an affected person requests the deletion of his or her data. In that case, it is sufficient for the data to be deleted from the conventional database because this means that the pseudonym in the blockchain loses its personal reference and becomes anonymous.

5.3 Location of the computer nodes

In most cases, the nodes of a blockchain network are widely dispersed around the world or at least rarely located in a single country. This dispersion is a major factor behind the resilience and decentralized nature of blockchain networks. Legally, it is important to discuss, especially in terms of data protection, how data stored on a blockchain in multiple countries, each with different data protection laws, should be handled. As this could quickly lead to significant complexity, we assume that the nodes in question are mostly all physically located in EU territory.

Figure 4: Differentiation within the question of liability



5.4 Personal data

In the EU, the location of computing nodes is irrelevant since personal data is equally protected throughout the area (cf. Art. 44 GDPR). However, personal data may not be transferred to third countries unless their protection is also guaranteed in these areas (Art. 44 GDPR). If, for example, data protection in the third country is equivalent to the GDPR, data may be stored there in the same way as in the EU. This is specified by the EU Commission in a specific list.[22] Otherwise, according to Art. 46 GDPR, special contractual clauses, or organizational guarantees are required to protect personal data from unauthorized access. In most cases, this is done by inclusion of the so-called EU standard contractual clauses [23] in agreements between the data exporting and data importing companies in the third country. If these are included, the level of data protection in this third country is considered adequate, and personal data may be transferred and processed there.

In the U.S., a special rule applies according to which data may also be stored there if the storing company is certified according to the so-called EU-US Privacy Shield and thus offers sufficient assurance that the data is also protected in the U.S.[24] If this is the case – as with Amazon, for example – no EU standard contractual clauses need to be considered.[25]

> ***Practical note:*** *When storing personal data on a blockchain, the nodes are only supposed to be located and operated in countries that offer an adequate data protection level according to the GDPR. This particularly applies to all countries of the European Economic Area (EEA), but currently also to other third countries such as Andorra, Argentina, Canada (only commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay, and Japan.[26] Companies from all other countries must implement so-called EU standard contractual clauses before operating a node.[27]*

5.5 Machine data

From a legal perspective, there are far less restrictions regarding where computing nodes are located that process machine data rather than personal data. On the assumption, however, that machine data is protected within the EU, for example, by certain database rights, this protection no longer exists if the data is stored on computer nodes abroad, and the respective foreign legal system does not have a corresponding database right.[28] While other jurisdictions may provide database protection comparable to that in Europe, this would have to be clarified on a case-by-case basis. Furthermore, the parties are, of course, free to agree on contractual confidentiality clauses which contribute to the protection of machine data.

5.6 Obtaining "prohibited" data by automatic transmission

On a blockchain, data is usually synchronized and stored fully automatically. In the future, several companies will likely use one and the same blockchain for their database. Thus, scenarios may occur in which, for example, illegally obtained data is stored on a blockchain that is also used by a German company, with this data then ending up in their database. Such specific considerations and scenarios need to be discussed, and the corresponding legal situation examined.

As such, data is not protected. It can only be "prohibited" to the extent that law regulates it as impermissible to collect, transmit or use.

Personal data

The processing of personal data by a company without a legal basis is inadmissible. It may result in fines and other measures by data protection supervisory authorities (Art. 58, 83 GDPR) as well as lawsuits by affected persons, e.g., for damages (Art. 79, 82 GDPR).

Sole or shared responsibility. If a company is responsible for the processing of personal data depends on whether it decides on the purposes and means of the processing of personal data (Art. 4 No. 7 GDPR), i.e., on what grounds and how data is collected, transmitted and otherwise processed. There may also be more than one company responsible at the same time. In the case of such a so-called "shared responsibility", several companies have an influence on the decision for what purpose and how data is processed (Art. 26 GDPR), such as in the case of Facebook and the respective operators of Facebook fan pages.[29] The shared use of a blockchain can result in shared responsibility, but this depends on the individual case and the contractual constellation. Suppose several companies in a consortium jointly decide to operate a blockchain. In that case, there are strong indications that they bear joint responsibility and are thus also liable for all data protection violations, for example, if the storage of certain personal data on the blockchain violates the law. If a consortium member is held liable by a third party but is not responsible for an infringement, the consortium member can seek recourse from the responsible consortium member.

> ***Practical note:*** *For contracts between consortium members, it is important to delineate responsibilities precisely.*

Commissioned processing. In a client/contractor relationship, i.e., when only the client decides on the purpose and means of processing personal data, but the contractor acts on his instructions, this is known as commissioned processing (Art. 28 GDPR). Thus, the contractor (processor) has no influence on the purpose for which and the manner in which personal data is processed and therefore cannot be held responsible for the unlawful processing of personal data. An example of a processor is a company that merely hosts a node but does not decide who participates in the blockchain and what it is used for. Since the responsibility in such cases lies solely with the client, the contractor would have indemnification and possibly recourse claims against the client if third parties assert claims against him. Besides, he or she is only liable for the breach of certain obligations. In particular, a processor may only process personal data on the documented instructions of the person responsible (client) (Art. 28 (3) 2 lit. a DSGVO). He or she must indicate if, in his opinion, the processing is unlawful (Art. 28 (3) GDPR a.E.).

In the event of data protection violations, the person responsible (client) is the addressee of fines (Art. 58 (2) lit. i, 83 GDPR) and can be sued for damages and for failure to act (Art. 79, 82 GDPR). However, he or she is not liable if a processor breaches the agreement with him and determines the purposes and means of processing himself/herself (Art. 28 (10) GDPR). For example, the hosting company itself would be responsible and liable if it did not merely store and make available the blockchain node as agreed upon but instead evaluated the data for its own purposes in breach of contract.

Machine data

In the case of machine data, a risk may exist under certain circumstances. If this machine data originates from third-party databases and can possibly be classified as trade secrets, there is such a risk.

Database rights. Database rights may exist for machine data. If a consortium member adopts substantial parts of external databases without permission, it could infringe the database right of the producer of the original database (Section 87b (1) UrhG). A company is liable if it is a perpetrator, participant, and disturber within the meaning of § 97 (1) UrhG. However, this depends on the individual case. A disturber is someone who intentionally and adequately causally contributes to the infringement of the protected right.[30] For example, if reasonable inspection obligations are violated, this is the case.[31]

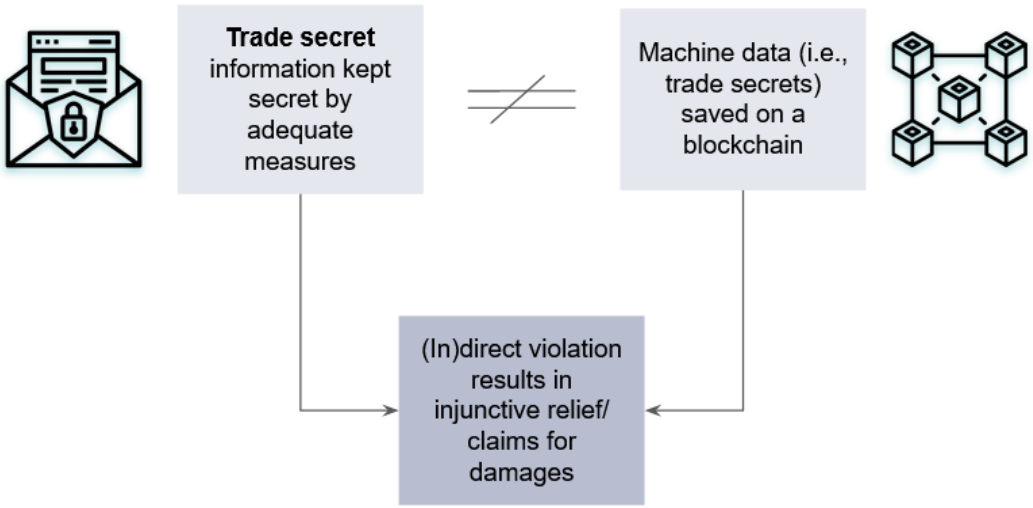
A violation of database rights may result in costs for a warning notice (Section 97a UrhG), wherein the amount depends on the economic significance of the database producer. Claims for damages exist only if the infringing company itself has acted negligently or intentionally (Section 97 (2) 1 UrhG). Intent means knowledge and intention with regard to the violation of the database rights. Negligence means a breach of due care and diligence (Section 276 (1) BGB). If a company is liable as an interfering party, it will usually also be found to have acted negligently. A reasonable amount of license costs can be claimed as damages (§ 97 (2) 2 UrhG).

Trade secrets. Furthermore, machine data can include trade secrets. A trade secret is information that is kept secret by effective protective measures and which is not accessible

without restrictions (§ 2 No. 1 GeschGehG). Trade secrets may only be obtained within the limits of §§ 3, 5 GeschGehG (e.g., through independent discovery). Any violation results in a claim for injunctive relief (Section 6 GeschGehG) and damages (Section 10 GeschGehG). These claims always exist only against the violator, i.e., the legal or natural person who obtains, uses or discloses the trade secret (Sec. 2 No. 3 GeschGehG). A person who indirectly obtains a trade secret via a third party is only considered to be in violation if he or she knew or should have known about the violation of the law in accordance with § 4 (3) GeschGehG.[32] “Should have known” corresponds to the negligence described above.[33] However, there is no general obligation to check all information obtained.[34]

Should data not be classified as trade secrets regardless of whether it is stored on a blockchain, it does not become trade secrets merely because it is stored in that way. As for the reverse case, where trade secrets are stored on a blockchain, it should be examined who has access to this data and how it is protected from access by third parties. In this context, it is also important to take into account that data can never be deleted from the blockchain.

Figure 5: Trade secrets on chain



A company based in Germany is only exposed to claims if it is aware that the transmitted data are trade secrets or if this fact should have been apparent. For instance, if the machine data clearly originates from the competitors' factories and could not realistically have been obtained legally.

> ***Practical note:*** *A qualification as a trade secret also presupposes the implementation of appropriate protective measures. If machine data is so important that it should be protected as trade secrets, the consortium members must take appropriate technical and, in particular, contractual measures to protect the data.*

6. Governance

This chapter addresses the question in which manner a consortium using a collaborative blockchain can be organized legally. In this chapter, we distinguish between the (1) "contract solution" and the (2) "legal person solution". Not only national but also cross-border collaborations can essentially be organized in these ways. Furthermore, we illustrate the advantages and disadvantages of bilateral and multilateral contractual governance in detail. This will be done against the background of the laws of Germany.

6.1 Introduction

An increasing number of companies are using blockchain technology in their business models and operations, integrating blockchain technology into the core of their organisational structure. This raises the need for legal backing of increasingly complex organisational structures that include a blockchain, e.g., in terms of auditing, leasing, privacy questions, or consortial use. The current legislation around blockchain technology is getting clearer and provides the legal boundaries of possibilities and restrictions for the organisation of these business models.

There is a responsibility for members that have access to a blockchain and operate on it as well as responsibility for legal governance e.g., towards third parties. The distributed nature of blockchains divides the responsibility of operating and running the network amongst the various nodes. Depending on the architecture of the blockchain, the nodes have equal or differing degrees of responsibility in operational governance matters (e.g., altering the protocol). Analogously as there can be various nodes that run a blockchain and share the blockchain's operational governance, there can be a consortium with several members which share the blockchain's legal liability.

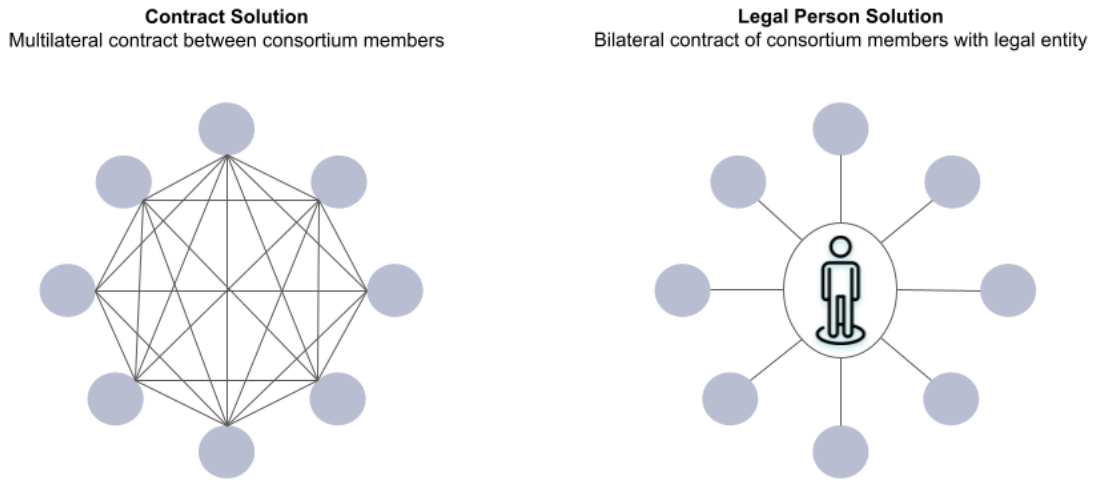
If a blockchain is used by a consortium, the question arises of how the consortium members should be organized legally to distribute liabilities. We will analyze this question in this chapter.

6.2 Legal organization of a collaborative consortium

Regardless of which of the two legal organizational structures is chosen, the governance of a collaborative consortium has the goal of protecting its consortial members. Disputes can arise either amongst members or with parties external to the consortium.

Network participants, consortium members, and, if applicable, the consortium entity as the alliance of the individual members in such a consortium are the participants that make use of the collaborative blockchain. Non-compliance with either the network agreements and policies or pertinent law are examples of how litigation bringing charges against a consortium might occur. The governance provides the framework to resolve such litigations. There are, in principle, two ways in which the consortium could be organized legally (see Figure 6): a "contract solution" or a "legal person solution".

Figure 6: Different types of legal organizational structures involving a blockchain



Contract Solution

The consortium members specify a multilateral contract agreed upon by all consortium members. This contract contains extensive provisions on governance. Instead of a multilateral contract, a contractual chain is also possible to be set up. In Figure 6, this is indicated by the lines that connect every consortium member with one another individually. Here, the consortium members enter into a bilateral contract and, if needed, can selectively assert rights against single members. However, the latter is likely more complex due to the mutual rights and obligations. In addition, it is also possible to accept service providers as contractual partners, for example, for the technical maintenance of software necessary for the operation of the blockchain.

The key advantages of the contract solution are that company law regulations do not necessarily apply. This means that members are free to covenant their relationship with each other as well as the structure of governance. The disadvantage of this solution is that there is no single entity responsible for the operation of the blockchain. The more members the consortium has, the less responsibility individuals typically feel for themselves. In addition, the contract has as many contracting parties as it has consortium members. This could be an obstacle, especially for the service provider, to sign the contract as well since the contractual partner risk is higher with more parties involved. Instead of one collective lawsuit, several individual ones with possibly differing contractual rights and obligations make it more complex. Furthermore, the coordination of litigation becomes more paperwork-heavy and more logistically challenging to set up.

Legal Person Solution

As an alternative to the contract solution, the consortium members have the possibility to establish their own legal entity. This involves bilateral contracts between the legal entity and each consortium member as well as with external service providers.

A legal entity can be an association, a cooperative, or a foundation. Companies such as GmbHs or AGs are also possible, but practice has shown that consortium members are rather reluctant to the possibility of becoming shareholders of another company for accounting reasons. Therefore, they prefer being a member of an association, a cooperative, or even entering the contractual commitment of a foundation. The selection of the suitable legal entity is further complicated by the choice of a suitable legal system – German, Liechtenstein, and Swiss foundations often compete with each other, meaning that depending on the contractual specifications the strategic choice of a suitable legal entity can be decisive for whether the consortium will be successful or not.

The key advantage of the legal person solution is evidently that the consortium has "one face" to the outside world. Moreover, there is no need for a contract with a large number of contracting parties, as shown in Figure 6. It may also be more convenient for the service provider to have only one contractual partner instead of the entire consortium. However, establishing a separate legal entity also implies higher costs. Even if the costs of setting up a company seem negligible, the company has to be managed and may need an employee and may have to file a tax statement at the end of the year.

6.3 Cross-border governance

In principle, it is possible to admit foreign companies as "members" in both contractual and legal person solutions. Even if the contract (contractual solution) and the legal entity (legal person solution) may be subject to German law, the law of the country in which the foreign company has its registered office is generally applicable to the foreign companies. If the consortium operates a blockchain, this could indirectly affect the operation of the blockchain, for example, if individual aspects of the blockchain were regulated differently in the respective foreign legal system. In addition, special tax law questions may arise.

The contracts with the foreign companies could, therefore, for example, stipulate that the respective foreign company ensures that the operation of the blockchain is in accordance with applicable foreign law and that there is a special right of termination in the event of irreconcilable conflicts.

7. Liability

Which influences do new technologies have on the existing liability regime, which is already complicated without the use of distributed systems? This chapter sheds light on contractual and product liability in general before addressing the liability question of smart contracts. A legal claim of one contractual party against another might arise due to 1) contractual breach of duty or through 2) producer and 3) product liability. The chapter analyzes the laws of Germany.

7.1 Introduction

Decentralized blockchain business models based on decentralized finance (DeFi) are flourishing. DeFi applications are mostly built on the Ethereum blockchain by use of smart contracts. One of their main features is the automatization of payment execution. Smart contracts function in a decentralized manner, i.e., the responsibility in legal and technical terms is distributed amongst multiple participants instead of one single entity. They enable interoperable, transparent, and open protocol pendants to existing financial services and products. Their technical design is inherently different from existing financial services and products. However, their legal liability compares to a great extent to their more traditional counterparts. Predictive models are another emerging product that also needs to be embedded in the existing regulatory framework. They include learning algorithms that are capable of approximating any kind of relationship in the data that they examine. They are used to extract repetitive and consistent patterns across a dataset. Predictive models focus on information that is relevant and useful for the prediction of important outcomes. One such use case for predictive models is the maintenance of cars. Since the reliability of these models can only ever be asymptotically close to being 100% correct, misjudgements need to be accounted for. This means predictive models will always have a certain margin of error in their forecasting.

If a smart contract is implemented incorrectly and claims would be asserted, the question arises who is liable. Similarly, the likelihood of success of predictive models must be legally secured in advance. These questions shall be addressed in the following chapter.

7.2 Protection in case of misjudgements

Mathematical models used for predictions in an industrial context (e.g., in the field of predictive maintenance) are based on statistical assumptions and are by their very nature never able to make a 100% reliable prediction. They are rather best guesses. How can one protect against misjudgements? The answer to this question depends on the individual case since liability is influenced by the applicable legal relationship (what type of contract, tort) and this, in turn, depends on all circumstances of the individual case. In the following, we will have a closer look at a breach of duty, limitation of liability, and producer liability.

Breach of duty

In principle, liability always requires a breach of duty. The obligation to perform can be described within certain limits. The obligations that parties have to fulfill are contractually predetermined and depend on individually agreed terms and also on the type of contract that the parties concluded. The obligations arising from the type of contract are defined by law:

Example A: In a car repair contract the agreed obligation to perform is: "Fixing of damage of the car".

In example A, one concrete success is owed, namely that the car is free of damage, i.e., the car must be repaired. If the car is not well repaired, the contract has been violated and warranty claims (e.g., supplementary performance or reduction) and, if applicable, liability claims (e.g., damages) can be claimed. The concrete type of contract is a contract for work (§ 631 BGB).

Example B: In a car repair contract, the agreed service obligation is: "Search for faults and, if faults are found, carry out repair work".

In example B, no success is owed, but an activity, i.e., the car garage, must make an effort to repair the car but does not owe any success. If the car is not repaired, the contract has only been breached if the fault was not searched for at all, if no repair work was carried out at all in the case of a fault, or if one of the two was not carried out carefully (which includes, for example, the state of the art). The specific type of contract is a service contract (§ 611 BGB). Warranty claims (e.g., supplementary performance or reduction) are not part of the law of service contracts. If there is a breach of duty, however, a claim for damages is possible.

In both examples, the breach of duty underlying a claim for damages is different, although the facts of the case are quite similar (defective car is taken to a garage for repair). This example shows that in the case of predictive maintenance, a breach of duty depends largely on how the obligation to perform (i.e., the "what") was agreed between the parties in the contract. In case A, the obligation is to repair the car. The car garage owes the successful completion of this contract and repair of the car. In case B, the obligation is the service of checking whether the car needs repairing and only if found to have any defect, to do repair work. When drafting contracts, particular attention should be paid to describing the technical background of predictive maintenance, e.g., the purpose of the models and how the models are trained. It is important that this never contradicts other statements, e.g., in advertising for the respective product. Not only the terms and conditions are legally binding, but also every piece of information in any shape or form that the parties objectively and recognizably base their agreement on, including advertising statements.

> **Practical note:** Even if the terms and conditions were perfectly designed, an advertising brochure should not contain phrases like "our software predicts all necessary maintenance".

Limitation of liability

Irrespective of the question of whether a breach of duty exists, the question is whether liability for a breach of duty can be limited or even excluded. In principle, debtors are only liable if they

are responsible for a breach of duty, i.e., if they are at fault (§§ 280 (1) 2, 276 (1) 1 BGB). This includes intent and negligence. If a debtor has neither intentionally nor negligently violated a duty, for example, if damage has occurred despite the application of the greatest care, the BGB does not provide liability coverage (in principle). However, there are a few exceptions, such as in tenancy law in the case of defects existing at the time of conclusion of the contract (§ 536a (1) BGB) or in the case of guarantees; in such cases, a debtor is liable regardless of whether he is responsible for a breach of duty, i.e. whether intent or negligence is involved.

Liability for intent cannot be excluded by contract (§ 276 (3) BGB), but liability for negligence can. However, there is also a relevant exception to this rule: in General Terms and Conditions (GTC), liability for gross negligence cannot be excluded at all (§ 309 No. 7 lit. b BGB), and liability for simple negligence cannot be excluded a) in the case of injury to life, body or health (§ 309 No. 7 lit. a BGB) and b) in the case of essential contractual obligations (cardinal obligations). These include obligations whose fulfillment is essential for the proper execution of the contract and on which the contractual partner may regularly rely on. Within these limits, not only an exclusion of liability but also a limitation of liability, e.g., a cap, is not permitted.

Whether or not a clause is to be considered as general terms and conditions (GTC) does not depend on whether it is in a document titled GTC. The only decisive factor is whether it has been provided by the other contracting party for a number of contracts (§ 305 (1) 1 BGB). It is already sufficient that the clause should be used at least three times. Whether the contract parties are consumers or companies is irrelevant in this respect. If the conditions for GTC are met, the specific clause falls under the so-called “GTC control” and the limitations of liability and liability exclusions mentioned above apply. The inadmissibility of an exclusion or limitation of liability can also result from legal regulations: For example, in product liability law or in the case of a violation of the general data protection regulation (GDPR), exclusion of liability is generally not possible.

> **Practical note:** In the case of predictive maintenance, for example, it is important to specify the data on which the model is trained and the predictions it will be attempting to make in the contract. It must be made clear that machine learning-based predictive maintenance is a probabilistic, not a deterministic method. Therefore, it is advisable that the algorithm represents the probability value it calculates and does not just answer with "yes"/"no". In this way, one can circumvent being sued for incorrect forecasts as "yes"/"no" are absolute statements while probability values are more nuanced and therefore cannot be held against the accused party as easily.

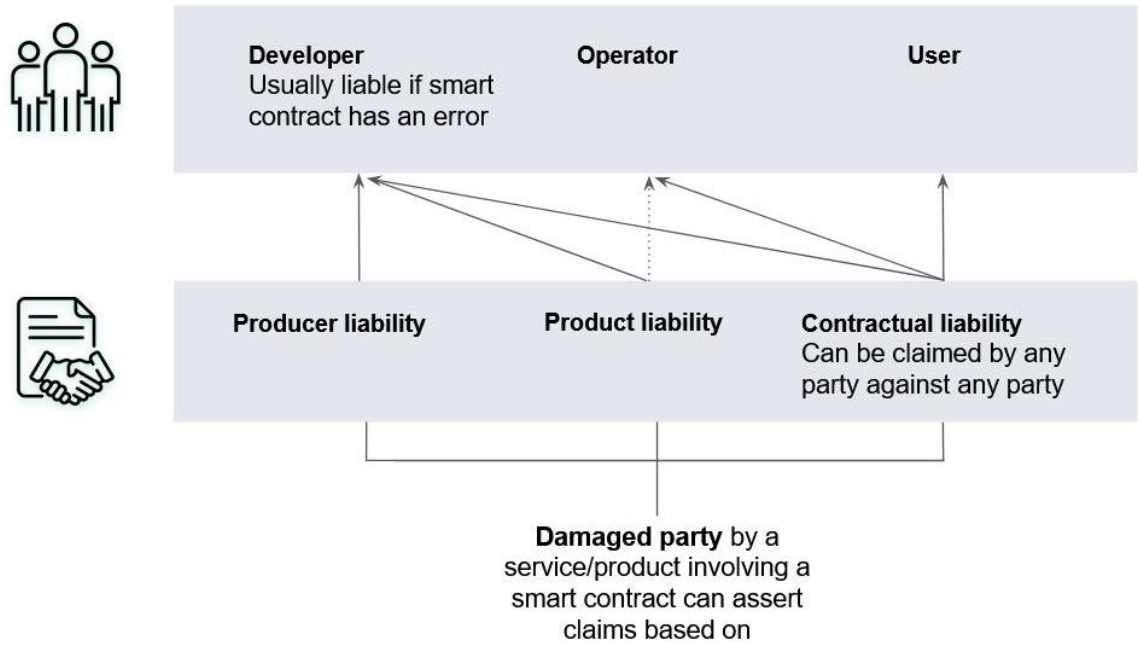
7.3 Liability in case of incorrect implementation of smart contracts

If there are errors in smart contract code: Who is liable?

In scenarios with smart contracts, we differentiate between at least four roles, whereby overlaps are possible:

1) The **developers of** the smart contract create the code (analogy: manufacturer of a vehicle)
2) The **operators of** the smart contract put it into operation and are perceived by third parties as responsible (analogy: holder of a vehicle)
3) The **users of** the smart contract access it, regardless of purpose and reason for doing so (analogy: driver of a vehicle)
4) **Damaged parties** are those who suffer a loss, e.g. due to an error in the smart contract (analogy: e.g., passengers of another vehicle, passers-by)

Figure 7: Question of liability for services/products including smart contracts



7.4 Liability reasons

Three different liability scenarios are conceivable (see Figure 7):

Contract

Any liability arising from a breach of a contractual obligation (§§ 280 ff. BGB) shall initially require the existence of a contract. If the damaged party is the user, only a contract between the operator and the user can be considered, but not between the developer and the user. If the injured party is the operator, however, they will invoke a contract with the developer.

Product liability

The German Product Liability Act ("ProdHaftG") also gives third parties who are not bound by a contract the opportunity to claim damages. The term product within the meaning of § 2 ProdHaftG arguably also includes software and, thus, also smart contracts. The term “manufacturer” of § 4 ProdHaftG is very broad and includes anyone who has manufactured the end product, a basic material, or a partial product. Thus, the term “manufacturer” includes, in particular, the developers of the smart contracts, but typically not the pure operators of the smart contracts.

Product liability is a liability for consequential harm caused by a defect, which is why it also includes, according to § 1 (1) 1 ProdHaftG, any injury to body or health or another object – but only if the manufactured item in question is not used in connection with a company or business, § 1 (1) 2 ProdHaftG. Since both will typically not occur in local scenarios, the relevance of the ProdHaftG for smart contracts is rather low but by no means excluded.

It, therefore, does not include liability for subsequent development work on the smart contract, nor does it include liability for financial losses. Furthermore, the injured party always has to bear a deductible of 500 euros (§ 11 ProdHaftG), liability is limited to 85 million euros in the case of personal injury (§ 10 (1) ProdHaftG), the liability claim expires according to § 13 (1) 1 ProdHaftG 10 years after the product is put into circulation (here: smart contracts) and the right to enforce a contract expires three years after the injured party had to become aware of the damage (§ 12 (1) ProdHaftG). The claims arising from the ProdHaftG are indispensable and can therefore neither be excluded nor limited by contract (§ 14 ProdHaftG). Since the ProdHaftG does not require fault, the manufacturer is liable regardless of whether or not he acted negligently or intentionally. The ProdHaftG thus also provides for liability even when the greatest possible care is taken.

Producer liability

The producer's liability under tort law is specified in §§ 823 ff. BGB. The producer (manufacturer) is also liable to third parties, a contractual basis is not required. Just as in the case of product liability under the German Product Liability Act, producer liability does not protect the interest of equivalence (i.e., the usability and functionality), but the interest of integrity (integrity of the injured party's legal interests in the form of life, body, health, and property).

The tort producer's liability is based on the placing of a defective product on the market (here: smart contracts) and the violation of either a safety obligation or a separate protective law. Case law has identified the following categories:

- **Design flaw**: The smart contract does not meet the legitimate security expectations of an average user.
- **Manufacturing defects**: Although the manufacturing process was correct, there is an unplanned deviation in individual pieces – in the case of software this is rather rare, for example in the case of damaged data carriers.
- **Errors in instructions**: The manufacturer omits necessary warnings and instructions for use.
- **Product monitoring obligation**: After the product has been placed on the market, the manufacturer must monitor the product and, if necessary, initiate a recall in order to prevent risks emanating from the product – this also seems rather unlikely in the case of a smart contract, but may still occur if security gaps subsequently arise.

Only those persons are considered manufacturers who are also responsible for compliance with the above-mentioned obligations. These are especially the developers of the smart contract but rarely the operators of the smart contract.

In contrast to the German Product Liability Act (ProdHaftG), fault is also required in this case, i.e. the manufacturer is not liable if he has exercised the greatest possible care and, in particular, acted in accordance with the latest state of the art in technology and science. In contrast, there is no deductible, and no maximum liability limit in the case of producer liability, the statute of limitations is similar to the ProdHaftG, liability can be limited by contract, but only between those parties between whom a contract exists, i.e., in particular not in the case of third parties as injured parties.

> **Practical note:** Against this background, the developer of the smart contract is typically responsible if the smart contract contains errors. An exception may apply where damage is caused by incorrect application of the smart contract (e.g., by incorrect transfer of parameters). In practice, it is particularly important to specify in the relevant contracts which is subject to which obligations. In the event of damage, it is easier to trace back who has violated a duty and may therefore be liable to pay damages.

7.5 Who is liable if the smart contract was audited?

Apart from the fact that third parties find errors in smart contracts and thus make damage scenarios less likely, the procedure when an auditing company or law firm examines a smart contract remains unchanged. This is because it seems quite untypical for them to assume their own liability towards users of the smart contract. Legally, this would be possible, but the matter at hand is a contract in favor of third parties (§ 328 BGB): The operator of the smart contract and the accounting firm or attorney conclude a contract and agree that users of the smart contract are entitled to claims against the accountancy firm or attorney under this contract. The latter would, however, be offering a kind of insurance, which would be untypical for the profession. It seems more likely that such an insurance would be taken out to cover claims against the operator of the smart contract.

8. Identities

Considering that information is seen as the oil of the digital age, data protection is a powerful tool that does not spare blockchain-based data. This chapter outlines the lawful obligation for anonymization of different data that can be stored on a blockchain. These different data types comprise 1) personal data, which refers to data of natural persons and 2) machine data which refers to machines and objects. We analyze the requirements for such sensitive data to be conformably stored on a blockchain in detail. The chapter analyzes the laws and rules of the General Data Protection Regulation (GDPR).

8.1 Introduction

The GDPR's purpose is to ensure individuals' right to informational self-determination and privacy. It aims at protecting personal data within the European Union (EU) as well as ensuring the free movement of data within the EU with no exceptions for blockchain-stored data. Blockchain-based use cases have to comply with the GDPR. The GDPR is directly legally binding for the EU member states, however, they have the possibility to change some specific predetermined clauses if they deem it necessary.

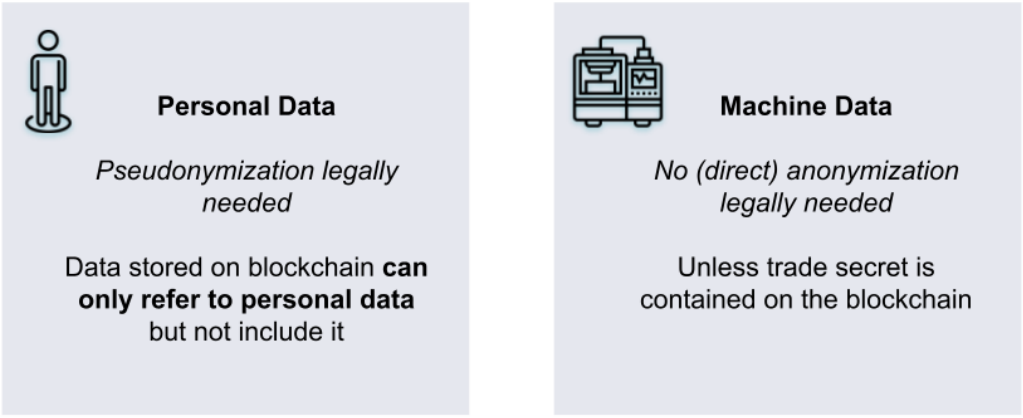
In connection with Bitcoin and the use of public and private keys, full anonymity of a natural person is often said to exist. While private keys are only available to the end-users and not visible to the public, public keys can be analyzed and used to infer information about the persons involved e.g., by the police if they suspect illicit activities. Full anonymity is therefore not completely irrefutable, which would make the GDPR obsolete in such an explicit case. Other blockchain or DLT-based databases, especially enterprise blockchains, do not necessarily render personally identifiable information anonymous.

Not only natural persons but also machines can participate in blockchain ecosystems, making the matter of data protection even more complex since data protection for machine data differs from that of natural persons. This provokes the question of how different types of data are to comply with the GDPR if stored on a blockchain. In the following chapter, we will analyze this question.

8.2 Anonymization of identities

Natural persons are to be distinguished from machines in terms of data protection measures. The reasons for data anonymization are to protect basic human rights (ie., right to informational self-determination) and ensure data privacy of individuals in the digital age. But is there a need for anonymization of such identity or is the use of privacy-enhancing features, such as private channels on Hyperledger, already a sufficient decoupling of trusted (possibly personal) information? A distinction must be made between keys that refer to machines (machine data) and keys that refer to natural persons (personal data) as is shown in Figure 8:

Figure 8: Legal storage requirement differentiation by data types



Keys with a personal reference

Keys with a personal reference should be pseudonymized using a lookup table [35]: The actual IDs are then assigned to a key in the lookup table and only this key, but not the ID, is stored on the blockchain. In this way, a company can respond to any deletion requests by deleting the data in the lookup table. The data on the blockchain then loses its reference and is thus anonymous. If the actual IDs are not relevant and could also be deleted, they could be stored directly on the blockchain. This could be the case when a company only cares about the amount of keys but not about who they belong to. Recordkeeping of the number of subscribers for the sake of internal marketing statistics is one such example. The eWpG bill for the law on the introduction of electronic securities and crypto securities in Germany seems to follow the same path – it talks about the "data used for pseudonymization".[36] Under the GDPR, whether private channels are sufficient to achieve anonymity depends on whether re-identification is possible using proportionate means. Whether a mean is considered proportionate differs from case to case. It can be determined by assessing the level of difficulty and effort needed for re-identification to be successful.

Article 26 of the GDPR states:

> *In order to determine whether a natural person is identifiable, account should be taken of all means likely to be used by the controller or by any other person in the general interest to identify the natural person directly or indirectly, such as segregation. In determining whether means are, in general, likely to be used to identify the natural person, all objective factors, such as the cost of the identification and the time required, should be taken into account as well as the technology available at the time of processing and technological developments. The principles of data protection should therefore not apply to anonymous information, that is to say, information which does not relate to an identified or identifiable natural person, or personal data which has been rendered anonymous in such a way that the data subject cannot be identified or can no longer be identified. […]*

Keys without a personal reference

Keys without a personal reference do not have to be anonymized for reasons laid out in the data protection law because they are not considered personal data. However, an obligation to make them anonymous may arise (indirectly) from the fact that the data may constitute trade secrets. For example, machine data could be used to read the times and intensities of use which might allow conclusions to be drawn about the order situation of a company.

Whether private channels are sufficient to achieve anonymity depends on the desired level of protection. For example, it may be sufficient if only "proportionate" measures do not lead to re-identification. That means that an active effort to re-identify keys without a personal reference has to be made to count as sufficient and proportionate in terms of the data protection law. If the machine data is more critical, it could also be contractually agreed that precautions must be taken to ensure that even when using the most advanced procedures, no conclusions can be drawn about the raw machine data during the period of use of the consortium blockchain.

> **Practical note:** An appendix to the contract should specify which categories of data may be stored and how. The requirements for storing highly sensitive business secrets may be higher than those for storing personal data, and these, in turn, may be higher than those for storing non-critical data.

8.3 Compliance of machine data

Data protection laws only apply to personal data (e.g., for the GDPR: Art. 2 GDPR). However, machine-related data may also be personal data in certain circumstances (see the answer to question 3). Machine data may also be subject to database rights (see the answers to questions 3 and 5). They can also constitute trade secrets (see the answers to question 3).

9. Additional information about the KOSMoS project

You can find further details about the KOSMoS project on the following page [GERMAN]: https://www.kosmos-bmbf.de/.

The consortium consists of the following partners:

PROJECT PARTNER		FOCUS
ASYS GROUP	**ASYS Automatisierungssysteme GmbH** *Dornstadt*	Maintenance concepts; product-accompanying proof of quality
DATARELLA	**Datarella GmbH** *Munich*	Development of blockchain and smart contracts
Frankfurt School Blockchain Center	**Frankfurt School Blockchain Center** *Frankfurt*	Blockchain development; cross-company business models
HOCHSCHULE FURTWANGEN UNIVERSITY HFU	**Institut für Cloud Computing und IT-Sicherheit** *Furtwangen*	Data protection / security in the acquisition of production data
inovex	**inovex GmbH** *Karlsruhe*	Analysis services for collected data; predictive maintenance solution
Universität Stuttgart Institut für Steuerungstechnik der Werkzeugmaschinen und Fertigungseinrichtungen ISW	**Institut für Steuerungstechnik der Werkzeugmaschinen und Fertigungseinrichtungen (ISW)** *Stuttgart*	Process modelling; linking digital and physical components

	**Ondics GmbH** *Esslingen*	Edge-solutions for the communication between shopfloor and blockchain
	**Alfred H. Schütte GmbH & CO. KG** *Cologne*	Cross-company, transparent maintenance concepts
	**Schwäbische Werkzeugmaschinen GmbH** *Schramberg*	Audit-proof billing models through dynamic leasing

Endnotes

[1] https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html

[2] For further information on this question see in detail Möslein in Braegelmann/Kaulartz, Rechtshandbuch Smart Contracts, Chapter 8.

[3] In addition, there are also concerns resulting from the application of the laws on general terms and conditions (*AGB-Recht*), see Riehm in Braegelmann/Kaulartz, Rechtshandbuch Smart Contracts, Chapter 9.

[4] Möslein in Braegelmann/Kaulartz, Rechtshandbuch Smart Contracts, Chapter 8, para. 24.

[5] Möslein in Braegelmann/Kaulartz, Rechtshandbuch Smart Contracts, Chapter 8, para. 23.

[6] Blocher in Braegelmann/Kaulartz, Rechtshandbuch Smart Contracts, Chapter 10.

[7] Kaulartz/Kreis in Braegelmann/Kaulartz, Rechtshandbuch Smart Contracts, Chapter 19.

[8] BaFin, information sheet on finance leasing, dated 19.01.2009.

[9] See BaFin, Merkblatt Finanzierungsleasing, dated 19.01.2009, citing BT-Drucks. 16/11108, of 27.11.2008, p. 66 f.

[10] BaFin, leaflet on finance leasing, drafted 19.01.2009.

[11] See BaFin, Merkblatt Finanzierungsleasing, dated 19.01.2009, citing BT-Drucks. 16/11108, of 27.11.2008, p. 66 f.

[12] Report of the Finance Committee, dated 26.11.2008 (BT-Drucks. 16/11108 of 27.11.2008), p. 67

[13] Detailed BaFin, Factoring Information Sheet, dated 05.01.2009.

[14] BaFin, Fact Sheet Factoring, dated 05.01.2009.

[15] Ibd.

[16] BaFin, Leaflet on Lending Business, dated 08.01.2009 (amended on 02.05.2016).

[17] Gupta, Kamal (November 2004). Contemporary Auditing. McGraw Hill. p. 1095.

[18] https://www.iso.org/standard/54534.html

[19] https://www.bafin.de/SharedDocs/Downloads/EN/Rundschreiben/dl_rs_1710_ba_BAIT_en.html

[20] ECJ, 20.12.2017, *Nowak,* ECLI:EU:C:2017:994.

[21] ECJ, 19.10.2016, *Breyer,* ECLI:EU:C:2016:779 recitals 31-49.

[22] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

[23] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

[24] List of certified companies available at: https://www.privacyshield.gov/list

[25] https://www.privacyshield.gov/participant?id=a2zt0000000TOWQAA4&status=Active

[26] See approximately here: https://datenschutz.hessen.de/datenschutz/internationales/angemessenheitsbeschl%C3%BCsse.

[27] Further information can be found here: https://datenschutz.hessen.de/datenschutz/internationales/eu-standardvertragsklauseln.

[28] Wiebe, GRUR 2017, 338, 345.

[29] ECJ, 05.10.2018, *Wirtschaftsakademie Schleswig-Holstein,* ECLI:EU:C:2018:388.

[30] BGH, judgment v. 16. 5. 2013 - I ZR 216/11, *Children's High Chairs on the Internet II,* GRUR 2013, 1229, 1231.

[31] BGH, judgment v. 16. 5. 2013 - I ZR 216/11, *High Chairs for Children on the Internet II,* GRUR 2013, 1229, 1231f.

[32] Köhler/Bornkamm/Feddersen/Alexander GeschGehG § 2 margin no. 115.

[33] BeckOK GeschGehG/Hiéramente GeschGehG § 4 Rn. 73.1.

[34] BeckOK GeschGehG/Hiéramente GeschGehG § 4 Rn. 73.1.

[35] This is recommended e.g., by the French data protection authority: CNIL, Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data, 06.11.2018: "these solutions enable stakeholders to come closer to the GDPR's compliance requirements".

[36] See the reasoning to § 4 (6), page 42, available at https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/RefE_Einfuehrung_elektr_Wertpapiere.pdf?__blob=publicationFile&v=1.