

# BaFin Perspectives

Issue 1 | 2018



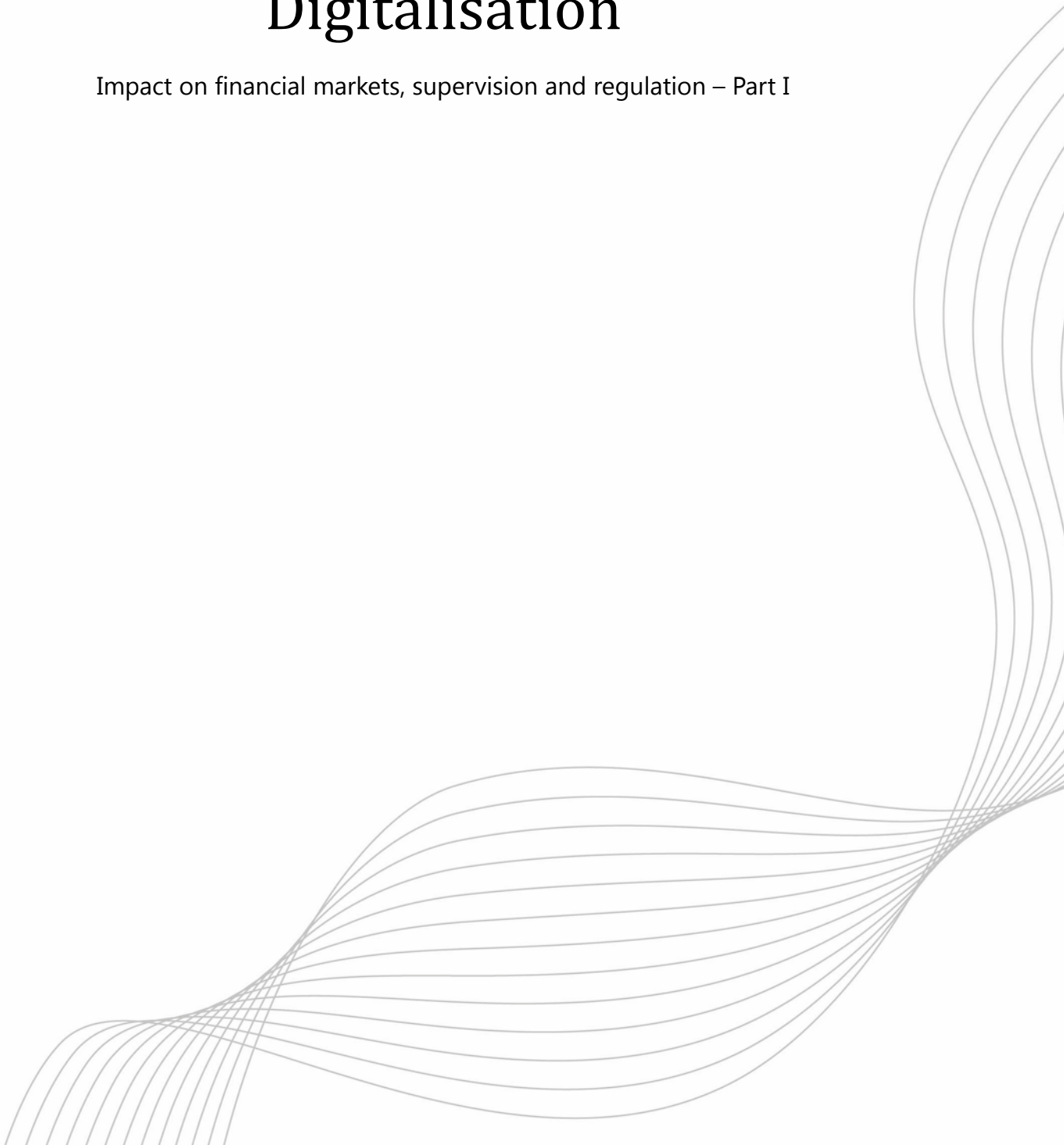
**BaFin**

Bundesanstalt für  
Finanzdienstleistungsaufsicht



# Digitalisation

Impact on financial markets, supervision and regulation – Part I



# Contents

<b>Foreword</b>	<b>6</b>
-----------------	----------

---

## **I. Supervision and Regulation in the Age of Big Data and Artificial Intelligence 8**

---

Big Data and Artificial Intelligence are changing the financial markets and raising supervisory and regulatory questions that need to be answered. Felix Hufeld

<b>1 Introduction</b>	<b>9</b>
<b>2 Prudential regulation</b>	<b>11</b>
<b>3 Consumer protection</b>	<b>17</b>
<b>4 Summary</b>	<b>27</b>

---

## **II. “This black-or-white debate is too superficial for me” 28**

---

The financial world is undergoing profound change because of the impact of Big Data Artificial Intelligence (BDAI). Established banks will hold their ground above all if they systematically work on their strengths, exploit their local presence and offer customers real value added.

<b>Interview with Prof Dr Stephan Paul</b>	<b>29</b>
--	-----------

---

## **III. Distributed Ledger Technology: Blockchain as a Basis for Information Security 32**

---

Blockchain provides an additional logical layer on the internet for transporting assets. The learning curve is steep, but blockchain can make IT both more secure and massively more cost-effective. Christian Flasshoff, Michael Mertens, Prof Dr Philipp Sandner and Sebastian Stommel

<b>1 Introduction</b>	<b>33</b>
<b>2 Advantages of blockchain technology</b>	<b>34</b>
<b>3 Blockchain supports information security</b>	<b>36</b>
<b>4 Blockchain in companies</b>	<b>40</b>
<b>5 Implementation of blockchain applications</b>	<b>42</b>
<b>6 Summary</b>	<b>47</b>

---

## **IV. Blockchain Technology – Thoughts on Regulation** **48**

---

Digital ledger technologies such as blockchain promote the development of new, decentralised structures. Assessing them under the existing legal framework can shed light on numerous uncertainties. Oliver Fußwinkel and Christoph Kreiterling

<b>1 Introduction</b>	<b>49</b>
<b>2 Emergence of decentralised ecosystems and the blockchain economy</b>	<b>51</b>
<b>3 Basic approach adopted by BaFin</b>	<b>53</b>
<b>4 ICOs and crypto tokens: risks and supervisory classification</b>	<b>54</b>
<b>5 Conclusion</b>	<b>66</b>

## **V. Digitalisation and Information Security in the Financial and Insurance Sectors as a Focus of Regulatory Requirements** **68**

---

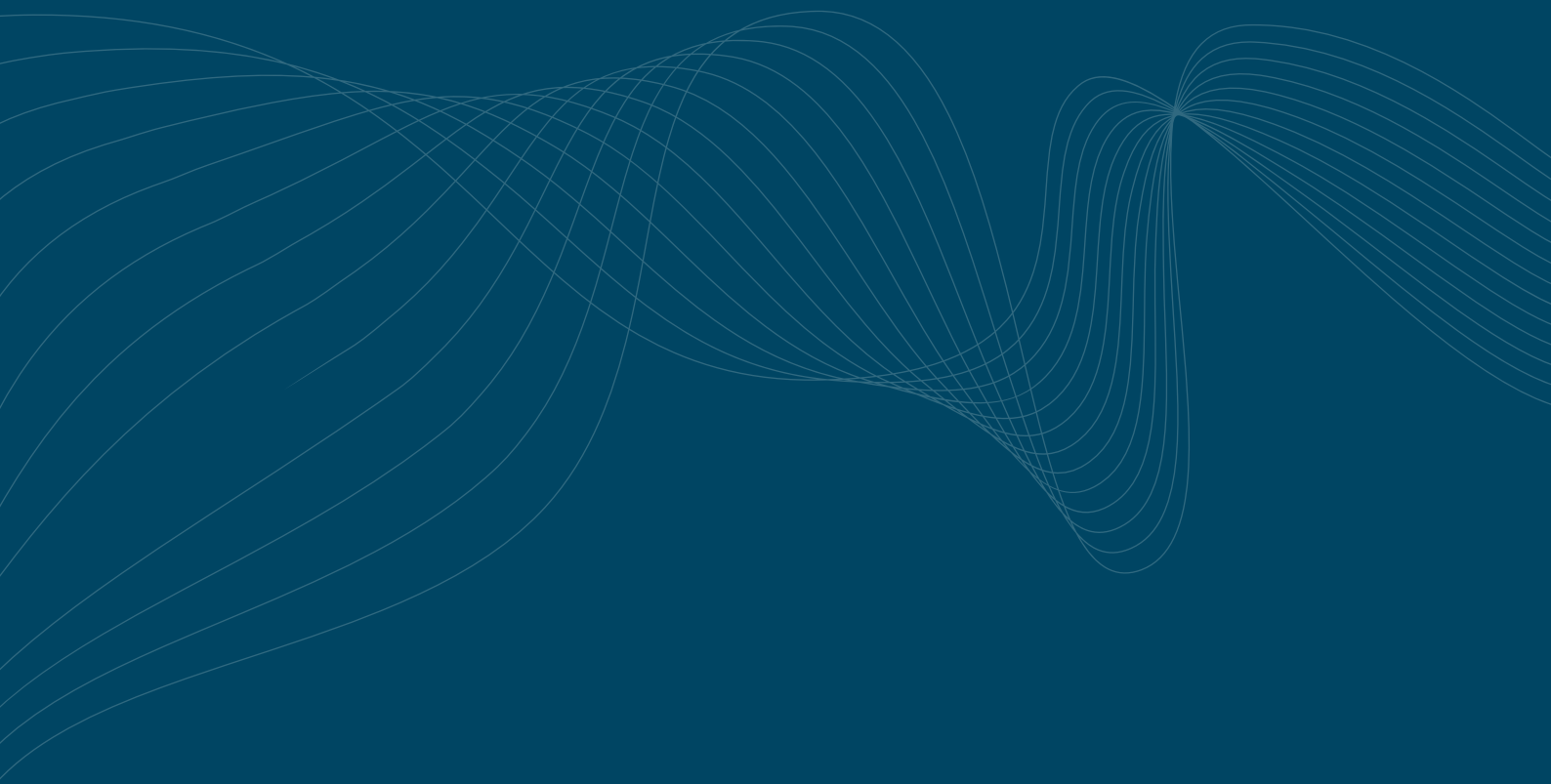
In a globalised financial world in which more and more people pay digitally, transfer money and make their investments online, IT governance and information security now have the same significance for supervisors as ensuring that companies have adequate capital and liquidity. It was therefore a logical step for BaFin to expand on its requirements in this area. Dr Jens Gampe.

<b>1 Introduction</b>	<b>69</b>
<b>2 Changing IT requirements in the financial sector</b>	<b>70</b>
<b>3 Fundamental international supervisory requirements for IT</b>	<b>73</b>
<b>4 IT-related regulation by the EBA</b>	<b>75</b>
<b>5 Supervisory requirements for the IT of institutions with a German banking licence</b>	<b>77</b>
<b>6 Interpretation of supervisory requirements by the BAIT</b>	<b>78</b>
<b>7 Digitalisation of the insurance industry</b>	<b>83</b>
<b>8 Summary</b>	<b>85</b>

## **Imprint** **86**

---

# Foreword



Almost exactly ten years ago, the global financial crisis reached its peak, at least in terms of public perception. Under the pressure of events, the course of financial market regulation and supervision was changed. New, European structures were created and, at the same time, legislators and regulators agreed on more stringent guidelines.

The major regulatory frameworks of the post-crisis era have now been finalised. The change in the financial sector, however, is still ongoing: in the era of globalisation and digitalisation, this will even gain momentum. As a result, supervisors and regulators are faced with ever more complex questions and are being led beyond the traditional fields of law and economics into new areas, such as information technology.

In such a complex and interconnected environment, we need an even greater exchange of information regarding fundamental issues in supervision and regulation with representatives of the financial sector and their industry associations, in addition to consumer protection organisations, experts from academia, journalists and, of course, politicians. With our new series of publications, BaFinPerspectives, which will be published twice a year, we hope to stimulate such an exchange. The articles are intended to bring strategic issues and regulatory projects into the spotlight and to analyse them from different points of view, beyond daily reporting. BaFinPerspectives will be published in German and in English at [www.bafin.de](http://www.bafin.de).

The first edition takes an in-depth look at digitalisation and focusses on issues surrounding Big Data (BD) and Artificial Intelligence (AI) from a supervisory and regulatory perspective: Professor Phillip




Sandner of the Frankfurt School Blockchain Center elucidates questions relating to the security of blockchain, an article by two employees of BaFin addresses the question of how Blockchain might be regulated and, in an interview, Professor Stephen Paul of the Ruhr-Universität Bochum discusses banks' strategic opportunities in the digital era.

I hope you enjoy reading our publication and that the topics addressed in this first edition are of interest to you.

I look forward to hearing your responses and opinions.

A handwritten signature in blue ink, which appears to read "F. Hufeld". The signature is written in a cursive style.

Felix Hufeld  
President



# I

Big Data and Artificial Intelligence are changing the financial markets and raising supervisory and regulatory questions that need to be answered.

# Supervision and Regulation in the Age of Big Data and Artificial Intelligence

Author

**Felix Hufeld,**

President, Federal Financial Supervisory Authority (BaFin)

## 1 Introduction

Big data (BD) and artificial intelligence (AI) are currently the subject of many social and academic discussions. Big data – which involves the emergence and rapid collection of large volumes of data from different sources – is a key element for applications of AI analytical methods. Significant progress is being made thanks to new technological developments, e.g. when identifying and processing language, faces, texts and images, and in the context of robotic process automation. The same is true for natural language generation. The productivity of artificial intelligence depends significantly on the scope and quality of the available data with which algorithms are trained and tested. For this reason, big data and artificial intelligence are not to be viewed in isolation and are referred to collectively in this article as "BDAI".

BDAI is also becoming increasingly relevant in day-to-day business operations due to three factors: technological progress, as mentioned above, market competition and changing consumer behaviour. Technological progress is setting the framework for continuous decreases in the cost of BDAI and making it easier to use in practice. For instance, the processing power of computers has

increased exponentially, a growing amount of inexpensive storage space is available, and hardware performance is improving. Overall, these developments are resulting in a decrease in technology costs and are also removing barriers to BDAI usage.

As far as competition is concerned, one can observe that many companies are increasingly relying on the analysis and use of data to optimise their business models and processes. This market situation has led to the emergence of many data-driven business models<sup>1</sup>. In addition, the user-friendliness and rapidity of new technological means have allowed many consumers to turn to digital applications, resulting in a self-reinforcing cycle of data and applications, and we can expect this trend to continue. The number of networking possibilities between humans, machines and processes is constantly growing.

---

<sup>1</sup> Data-driven business models that use BDAI to increase value added have allowed a number of tech companies to rise among some of the highest valued companies worldwide.



BDAI technologies have the potential to fundamentally change the financial sector as well. The risks and opportunities are enormous. In its report "Big data meets artificial intelligence – Challenges and implications for the supervision and regulation of financial services"<sup>2</sup>,

BaFin analysed the changes that an increased use of BDAI could bring for the financial market as a whole, firms, consumers – and also supervisors. These changes require supervisory and regulatory attention at an early stage – including the risks that BDAI applications could potentially involve. The main challenges that BDAI could entail for prudential regulation and consumer protection are described below.

---

2 BaFin, Big data meets artificial intelligence – Challenges and implications for the supervision and regulation of financial services, [https://www.bafin.de/SharedDocs/Downloads/EN/dl\\_bdai\\_studie\\_en.html](https://www.bafin.de/SharedDocs/Downloads/EN/dl_bdai_studie_en.html), retrieved on 10 July 2018. The study was prepared in collaboration with PD – Berater der öffentlichen Hand GmbH, Boston Consulting Group GmbH and the Fraunhofer Institute for Intelligent Analysis and Information Systems. Parts of the article "Supervision and Regulation in the Age of Big Data and Artificial Intelligence" are based on this report.



© iStock/from2015

# 2 Prudential regulation

If we look at how BDAI works and the impact it has from a bird's eye view, it is quickly clear why BDAI applications have the potential to fundamentally change the financial market. Financial services heavily depend on information and evaluations thereof. With BDAI, it is possible to obtain a growing amount of increasingly precise information. With this information, new evaluations can be made thanks to BDAI, for instance, in relation to asset prices, creditworthiness or risk profiles in the context of health insurance.<sup>3</sup> If these evaluations surpass conventional processes, the providers making use of these evaluations will have a competitive advantage. For instance, if a company is able to better assess the creditworthiness of an individual than its competitors, it can demand a more risk-adequate price and gain an edge over its competitors in the long term. Thus, BDAI is a phenomenon that will result in a certain amount of competitive pressure, and companies that intend to remain on the market will have no choice but to prepare themselves for the use of new BDAI methods.<sup>4</sup>

As BDAI is making some information accessible that was previously unavailable and is facilitating more precise evaluations, providers are able to offer new products and services – with a potentially unlimited reach. For example, predictive analytics can be used to forecast the likelihood of events that could not be predicted or were very difficult to predict in the past. Insurers can thus offer products for such events if there is sufficient demand. But it is mainly the customer information that can be gained thanks to BDAI that is now allowing for more personal contact and personalised products. Many users are already familiar with these seemingly personal interactions via computer or smartphone based on their experiences with many online service providers outside the financial services sector, and their expectations for these services are the same for other areas as well, particularly financial services.

At financial companies, too, there are many processes where data is generated and needs to be evaluated before decisions can be taken. In the case of payment

transactions, for instance, huge amounts of data are generated and analysed to detect money laundering, among other things. Patterns and connections that could not be identified in the past can now be identified using BDAI – at a significantly lower cost. To give another example, BDAI could also be used for settling claims at insurance companies. A growing number of decisions can be automated and prepared using BDAI. In the past, it was essential that procedures were extensively predefined when automating processes – and algorithms were unable to adapt. But in the context of BDAI, self-learning algorithms are increasingly being used. As a result, increasingly complex processes can be (partly) automated. Competitive pressure – in terms of costs – could be another catalyst for the use of BDAI.

Using BDAI could thus result in key competitive advantages on the financial market, too. Firms that are supervised by BaFin will also take advantage of this, especially to increase their effectiveness and efficiency. Financial supervisors are therefore faced with the question of whether and how supervision and its foundations – regulation – need to be adjusted, and they will also have to examine which established principles should continue to apply. A number of key aspects are examined below:

## 2.1 Who is to be held accountable: algorithms or humans?

In the case of firm supervision – e.g. the supervision of banks – there is a common thread running through the requirements that supervisors impose. All of the decisions that are taken within a bank must be embedded in a proper business organisation. Section 25a of the German Banking Act (*Kreditwesengesetz – KWG*) stipulates the following: “An institution shall have in place a proper business organisation which ensures compliance with the legal provisions to be observed by the institution as well as business requirements.” Under section 25a of the KWG, the management board is responsible for ensuring the institution's proper

---

<sup>3</sup> See also Section 3.3.

<sup>4</sup> See also Section 4.

business organisation. Supervisors will ensure that this common thread, which similarly runs through insurance supervision, continues to apply as BDAI spreads and the use of algorithms increases: humans are and will continue to be held accountable.

This does not mean that the use of algorithms is to be prohibited. But every single algorithm, just as every single employee within an institution, must be part of a proper business organisation. Those within and outside the institution need to be able to understand and check their decisions – especially when reaching or at least making preparations for important and thus risk-entailing decisions. Neither humans nor algorithms should be able to do whatever they want unchecked within an institution.

Decision-making and evaluation processes can be complex. If BDAI is to be used, it is important to ensure that the reasons behind decisions can still be traced. If new types of algorithms or highly complex ones are used, companies often quickly refer to black boxes as an argument: for instance, an innovative algorithm is generating highly precise forecasts, but the reasons why and the basis on which it operates cannot be traced and, unfortunately, cannot be verified by supervisors. This line of argument is unacceptable for supervisors, and management boards, too, would be well-advised not to accept this within their organisations as this potentially points towards a dysfunctional business organisation.

Experts in academia and (applied) research have also confirmed how important the explainability and transparency of algorithms is when they are used and have developed processes and tools for this purpose. It is now possible to ensure the explainability of complex analytical processes as well. Complex algorithms and automated processes do not need to be ruled out for the financial sector, but it is important not to forget that it is necessary to invest in their transparency and explainability as well. It should serve as an incentive for firms that only sufficiently transparent algorithms are able to identify errors in the analytical process at an early stage and rectify them, extending the possibilities for BDAI applications even further.

## 2.2 Supervisory standards for self-learning systems

Will supervisors need to define supervisory standards for self-learning systems in the near future? Will there soon be Minimum Requirements for Algorithms/Data – based on the Minimum Requirements for Risk Management (*Mindestanforderungen an das Risikomanagement – MaRisk*) at financial institutions? One thing has to be said first: creating additional regulations is not the main objective. Just because one step of the process, which has not been subject to BaFin's supervision so far, is now being executed by an algorithm and not a human does not mean that the entire process needs to be regulated and supervised. The question of whether and the extent to which financial regulation is to be amended is to be discussed in another context. Here, we are discussing aspects for which BaFin is already responsible as a supervisory authority as part of its legal mandate. The key question is: how do supervisors and regulators need to change their approach when examining these aspects if an algorithm is involved instead of a human?

In the previous section, we argued that the explainability and traceability of an algorithmic solution are key prerequisites for embedding them within a proper business organisation. Results and processes also need to be sufficiently documented.

Assuming that these basic requirements for algorithms (explainability, transparency and embedding them within a proper business organisation) are fulfilled, which standards should apply in regular operations or in (re-)calibration phases? When and to what extent supervisors must intervene should, of course, depend on the risk relevance of the application concerned.

This section outlines a number of ideas on how firms could use self-learning algorithms carefully and wisely. For example, institutions could calibrate, test and validate innovative approaches in a secure environment before using them in customer operations. In such an in-house test environment, the behaviour of an algorithm can be observed and traced in various situations – without resulting in any damage. Before BDAI solutions



© iStock/from2015

are used, one option would be to run them separately at the same time as existing systems. Potential risks could be isolated, quantified and eliminated in these parallel operations. Live operations should begin only after this has taken place. And if these algorithms are successfully implemented in live operations, further monitoring and ongoing validation are essential. This is especially due to the fact that self-learning systems are constantly evolving when they are fed new data.

In live operations, algorithms often make use of many different data flows which may have been generated by algorithms themselves. This can result in self-reinforcing decision-making cascades. It could be worth taking a look at the tools available on the capital market: technological safeguards such as automatic volatility interruptions are common practice there. Such automatic interruptions could also be useful safeguards for algorithmic decision-making processes – provided that they are also properly calibrated otherwise the number of mistakes and problems could increase even more.

### 2.2.1 Specific calibration of requirements

In the previous sections, a number of examples were provided to describe the general basic conditions that would be needed when using algorithms. However, in some situations, it could be necessary to also set detailed and, in some cases, quantitative requirements for the results of BDAI applications. For example, if BDAI is to be used to detect money laundering, supervisors should be able to assess whether the algorithm that is being used is sufficiently effective, i.e. whether it is capable of detecting money laundering if there is reason to believe that there is suspicious activity, and whether it is sufficiently efficient, i.e. whether it is capable of screening out activities that are less suspicious. But supervisors will be able to intervene in justified cases and request model readjustments only if they have defined clear standards on this basis that set out the requirements for efficiency and effectiveness.



## 2.2.2 Data integrity

Just as supervisors are required to clearly define the quality of the results that is expected, algorithms need feedback for their calibration. Algorithms need to know which predictions are right and which are wrong. Accurate data that is relevant to the results needs to be available. If Minimum Requirements for Algorithms are to become necessary, Minimum Requirements for Data will also be necessary. This, however, is not trivial in terms of BDAI as BDAI is largely characterised by the fact that key (and correct) information is generated from unstructured data.

Companies therefore need to continue to ensure that only accurate data that is relevant to the results is used for algorithms. It is a myth that business decisions based on algorithms yield objectively better results for this reason only. The opposite could be true as the production of wrong decisions reached by algorithms or unsuitable input data may be more difficult to detect than errors in conventional decision-making processes.

This problem can also multiply as the reach of algorithm-based decisions – i.e. the number of people concerned – is typically significantly higher than in a paper-based world. Ongoing quality checks – not only with regard to the embedded algorithms but also the data used – will therefore play a significantly

more important role than in the past. Supervisors and regulators will have to derive solid supervisory standards on this basis.

### 2.2.3 Model changes and approved applications

As described above, BDAI models are also characterised by the fact that they take into account large amounts of data to make predictions or reach decisions, often in real time. In particular, self-learning elements can allow models to continue evolving by taking into account additional data input and the information it contains. Models and their calibration are constantly changing and improving. Supervisors need to keep an eye on the fact that models they have already approved may continue to develop. This raises a few fundamental questions: for example, in relation to the extent to which a supervisory approval is valid and when developments may be deemed model changes in the supervisory sense. But this particularly also raises the question of how much dynamic change in a model may be deemed admissible in order for an approval to be granted. Supervisors will need to find answers to these questions – based on concrete cases and as part of a dialogue with all those concerned.

### 2.2.4 BDAI and systemic risks: who will we be supervising in the future?

Promising processes – such as deep learning – require huge amounts of data (“the more, the better”) in order to generate interesting results that can form the basis for product and process innovations. The advantages that BDAI processes bring will continue to grow if companies collect not only information on customer preferences but also information on their spending behaviour – for example, information relating to their current accounts or other payment accounts. Their BDAI algorithms could then be fed with far more accurate data. This shows that those who have the right to use abundant amounts of data, preferably also financial data, have huge advantages when developing new, promising BDAI-based products and services – especially outside the financial sector. And the use of these products, in turn, helps generate new data.

This self-reinforcing cycle is also driven by the “pay-with-data” business model<sup>5</sup> implemented by a number of bigtechs. Natural data and analysis monopolies could emerge and could foster a “winner-takes-it-all” market structure. By serving constantly new markets, companies are able to link constantly new data from various sources. BDAI applications can help achieve portfolio and conglomerate effects<sup>6</sup> and make use of economies of scope and scale.

Due to the wide spread and high number of users, dominant data and algorithm providers that are entering the financial market with their own financial services – that may also be cross-subsidised – could very quickly become systemically important directly. However, such providers could also become important in the financial system indirectly, for instance, if they sell information on how to calculate risks more precisely to a large number of players on the financial market. However, interconnectedness does not necessarily have to arise through the sale of information. It is also possible that providers will make algorithms and infrastructure (services) available to players on the financial market (see also “Pooling and utilities”, page 16).

But if stakeholders on the financial market increasingly use the data or algorithms offered by only a few large providers, this could also have macroprudential consequences. Firstly, this would result in a strong reliance on these providers. What would happen, for example, if data and models contain errors or these providers' infrastructures are inoperative? Secondly, this could lead to procyclical effects if a large number of players on the financial market draw the same

---

5 With this model, users are offered services which are supposedly free and cannot be competed with. But in fact, they are paying for these services by giving providers the right to use their data. What is particularly problematic is that many users are not sufficiently aware of the value of their data and thus the price that they are paying for this.

6 Data-driven business models that use BDAI to increase value added have allowed a number of tech companies to rise among some of the highest valued companies worldwide.

conclusions and strategies for action based on certain events because they are using the same algorithms. An analogy to the role of rating agencies comes to mind.

Such risks can arise as a result of insourcing, outsourcing or other BDAI-supported services obtained by third parties. And if these risks are no longer within the organisational structure of supervised firms, there is a risk that they can no longer be fully identified or managed. It is therefore necessary to examine whether the definition of systemic importance in the supervisory sense and thus the possibility of introducing mitigating measures need to be revised to accommodate the new circumstances described above.

This is closely linked to the question of who and what needs to be subject to (financial) supervision and how this should be done. For example, will providers that offer structural expertise and information on the financial market need to be supervised although they are not providing financial services themselves? One well-known idea from the field of market supervision could be applied here: establishing conduct of business rules for companies that are not supervised by BaFin and monitoring compliance with these rules.

#### Scenario

### Pooling and Utilities

BDAI could facilitate the pooling of data, technology and expertise in addition to the use of utilities as the success of BDAI applications depends on two key criteria: data and technology (and the relevant analysis expertise). Both of these criteria are not always fulfilled. If some companies do not have enough data in order to make the most of BDAI, it may be useful to combine data packages in pseudonymised or anonymised form. For example, some companies may not have enough data points for providing the necessary feedback for (self-learning) algorithms and/or their calibration may be difficult to perform. But if multiple companies pool their data, the critical mass of data that is needed can be achieved. This allows enough data to be available for data-driven innovations.

However, pooling data, technology and expertise is only possible if the technical, organisational and legal requirements for this are met. It is also essential that the data sovereignty of the individual firms can be guaranteed, especially when pooling data.

One example is the Industrial Data Space initiative jointly launched in 2014 by members of the fields of business, politics and academia.

BDAI applications could thus lead to an increase in the importance of utilities, i.e. vehicles in which multiple companies come together to allow for better analyses, achieve cost advantages and pursue similar interests. In the financial sector in particular, supervisory and regulatory requirements could be met in a more targeted way by combining expertise and co-developed solutions (e.g. regtech applications, money laundering prevention, know-your-customer processes). And BDAI could drive this trend. The objective is to achieve economies of scope and scale.

Supervisors now have to examine the question of how new risks are to be taken into account accordingly and addressed when pooling is on the rise and the use of utilities is growing.

# 3 Consumer protection

## 3.1 The digital revival of the traditional corner shop model

It should first be noted that the use of BDAI could result in huge advantages for customers and consumers. This is evident by taking a look at the more recent past. Up until the 1980s, small stores mainly provided local residents with food and other everyday products. Shopkeepers had their customers' trust and deep insights into their private lives. They were also aware of what their customers wanted and needed, made offers that were tailored to them and conducted business quickly and easily. If someone wanted to buy fresh salmon at the weekend – a product that wasn't available otherwise due to low demand – these shopkeepers would have a certain amount of salmon every Friday as part of their product range. Such tailored offerings were beneficial to both sides. Customer satisfaction and customer loyalty were high. Customers could even

pay for items at a later date if they didn't have any or enough money on them. These advantages disappeared with the arrival of supermarkets, and there was a typical trade-off between information breadth and information depth. Internet and digitalisation are now making it possible to dismantle this paradigm.

The traditional corner shop model can now essentially be applied and scaled to all areas of life. But this requires a deep understanding of the requirements and needs of the customer. BDAI provides the tools for this without having to build personal relationships between individuals while still gaining access to highly personal data. In simplified terms, BDAI is enabling the large-scale revival of the traditional corner shop model – in all sectors. The key question is whether providers and customers will equally benefit from this revival.

Let's take another look back at the time when smaller stores were more common: what made the relationship between customers and retailers so special back then? Customers were always the ones who decided





whether and what they wanted to reveal to retailers. In addition, information, which was highly personal at times, was (ideally) only available to the relevant retailer, and customers kept control and had an overview of what they knew about them. The solid relationship that customers and retailers had was, in some cases, comparable to the relationship they had with their doctor, pastor or lawyer. Retailers were able to gain an overall impression of the personality of their customers, their circumstances and their needs and wants. Breaching their customers' trust could have considerable business implications – in addition to personal and social implications. In the analogous world, there was a balance of power between customers and retailers, and retailers used the information they had almost exclusively in order to pursue their own business goals. This information was worthless to third parties because it could not be sold to other people.

All of this fundamentally changed with digitalisation and the emergence of new business models (e-commerce, platform business and virtual networks). Even without face-to-face interactions, the needs and wants of customers can be extensively and automatically analysed nowadays. The use of BDAI makes personal relationships – but not personal data – superfluous for gaining information. Consumers are not dealing with an actual person they know and trust and that analyses them precisely. They are also unaware of what their data could be used for and what it is worth. In addition, it is very difficult for consumers to find out whether they are potentially being discriminated against as a result of the data they have provided.<sup>7</sup>

Instead of seeking personal contact, reaching a critical mass of users and achieving network and conglomerate effects is particularly crucial for gaining the aforementioned information in the world of BDAI. As massive amounts of user data becomes available, the required amounts of data are generated as an input for new analytical methods (e.g. deep learning). Companies can initially use information on customer preferences for targeted product marketing or getting in touch with

customers. But what is new is that this information is now also valuable for third parties and companies can sell it. Highly personal information can be monetised – also by selling it to third parties. Customers can quickly lose their overview of what companies know about them and what the data they originally gave will ultimately be used for. Gone are the days when there was a balance of power: BDAI could result in significant power and information asymmetries between customers and companies.

In this context, companies are particularly interested in financial data because it reveals a person's economic core (income, assets, payment transactions/spending behaviour, contractual relationships, health status etc.). Shopkeepers would also have been interested in this detailed information but would have only been able to draw imprecise conclusions, e.g. based on the clothes or profession of their customers. As financial data is particularly sensitive data, customers gave and are giving their data only reluctantly to a limited extent – and to just a number of people they trust. In addition, shopkeepers would have had a difficult time making the most of their customers' willingness to pay since they would not have been able to constantly adjust their pricing, for instance, if a solvent and demanding customer entered the store while another less solvent customer was still being served. But on the Internet, this is all happening very fast. Financial data as a commodity can also represent a key means to maximise profits for companies nowadays – potentially at the expense of the customer (see "Making the most of consumers' willingness to pay in order to maximise profits", page 18).

However, from a consumer protection perspective, customers must, even today, be able to decide who they want to give their data to and for what purpose. Data sovereignty is important, especially when this involves financial data. It is also necessary to ensure that new ways to gain information are not used against consumers. There is a thin line between legitimate and authorised differentiation and prohibited discrimination.<sup>8</sup>

---

7 See section 3.3.

---

8 See Section 3.3.



Collection and analysis activities that are common in some online services and other data-driven business models certainly cannot be applied to financial data in the exact same way.

Two key questions are therefore addressed below:

- How can customers keep control over their data in the new world of BDAI? In other words: how can data sovereignty be ensured in the context of mass and self-learning data analyses?
- And how can discrimination-free access to financial products be ensured, even in the context of BDAI?

## 3.2 Data sovereignty within the context of mass and self-learning data analyses

How can we ensure data sovereignty within the context of mass and self-learning data analyses? The main requirements for data sovereignty are suitable and

transparent information on data usage and the potential consequences, reliable options for controlling how data is used (also after data has been released) and actual freedom of choice.

### 3.2.1 Suitable and transparent information

In order to be able to reach sovereign decisions, customers need to initially understand why they need to provide data and what companies may potentially use it for. They should be able to assess the potential consequences of releasing their data. Customers need to be informed of this appropriately and transparently. It should be noted that in most cases customers do not read data protection policies if they consider them to be unclear or difficult to understand. Data protection policies therefore need to be clearly formulated and tailored to the specific decision-making situation. For example, the FZI Research Center for Information Technology (*Forschungszentrum Informatik – FZI*) suggests in its report “Smart Data – Smart Privacy?” that consumers be given the results of data protection impact assessments (as referred to under Article 35 of the European General Data Protection Regulation

(GDPR) in simplified form as the basis for deciding whether to provide data or not.<sup>9</sup> The FZI is also of the opinion that a uniform scale system that is easy to understand or an intuitive traffic light system that highlights the risks that are associated with data usage would be a good way to inform customers.

Germany's Advisory Council for Consumer Affairs (*Sachverständigenrat für Verbraucherfragen*) suggests

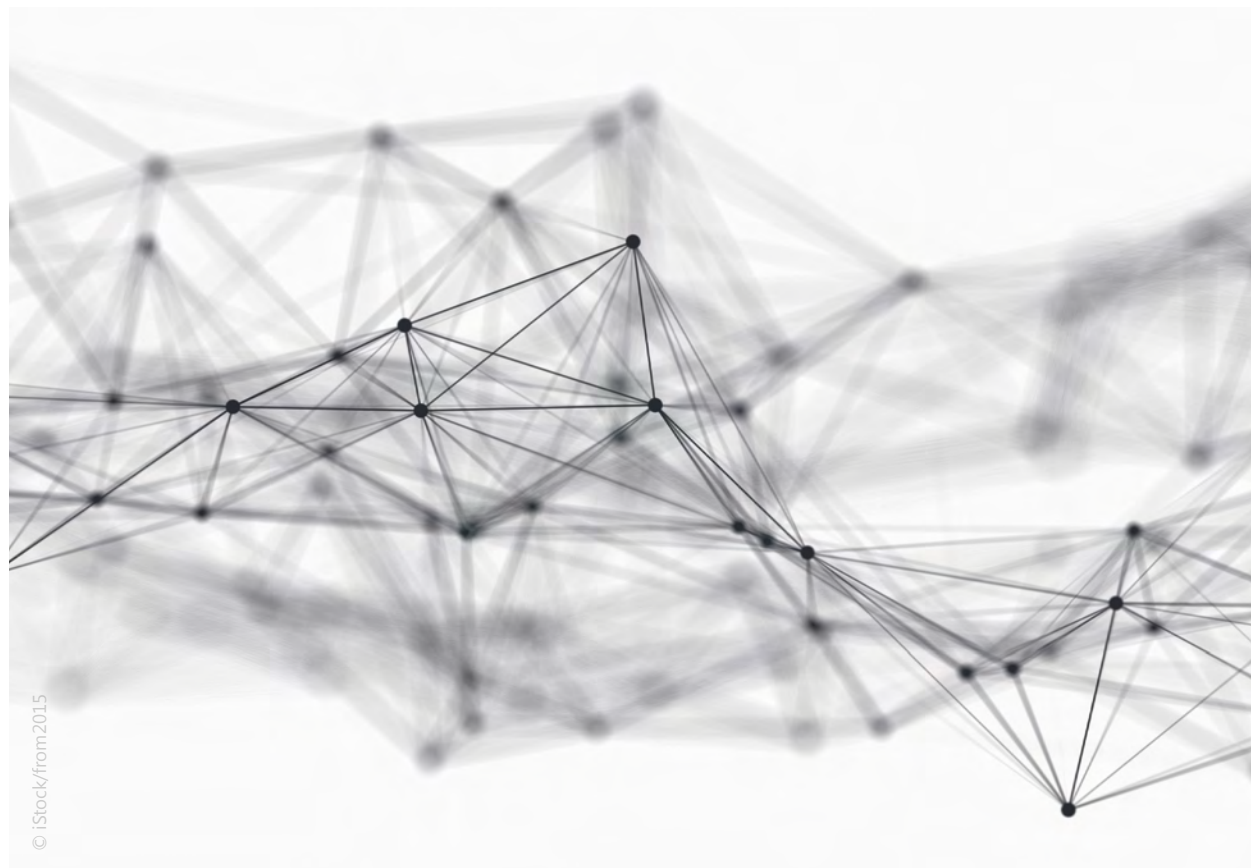
using a one-page privacy policy to inform customers quickly and easily.<sup>10</sup> From a supervisory point of view, such simplified options seem to be – at least as supplementary information to data protection policies as we know them today – promising and should be given further thought (see “Areas where financial supervision and data protection issues could meet”, page 21).

---

9 FZI Research Center for Information Technology, „Smart Data – Smart Privacy? Impulse für eine interdisziplinär rechtlich-technische Evaluation“, pages 13-14, [https://www.digitale-technologien.de/DT/Redaktion/DE/Downloads/Publikation/SmartData\\_Thesenpapier\\_smart\\_Privacy.pdf?\\_\\_blob=publicationFile&v=7](https://www.digitale-technologien.de/DT/Redaktion/DE/Downloads/Publikation/SmartData_Thesenpapier_smart_Privacy.pdf?__blob=publicationFile&v=7), (only available in German), retrieved on 11 June 2018. This research paper was supported by the Federal Ministry for Economic Affairs and Energy (*Bundesministerium für Wirtschaft und Energie*) by resolution of the German Bundestag.

---

10 German Advisory Council for Consumer Affairs, „Digitale Souveränität – Gutachten des Sachverständigenrats für Verbraucherfragen“, [http://www.svr-verbraucherfragen.de/wp-content/uploads/Gutachten\\_Digitale\\_Souver%C3%A4nit%C3%A4t\\_.pdf](http://www.svr-verbraucherfragen.de/wp-content/uploads/Gutachten_Digitale_Souver%C3%A4nit%C3%A4t_.pdf), retrieved on 11 June 2018.



## Note

### Areas where financial supervision and data protection issues could meet

One of BaFin's legal duties is to ensure that market participants and consumers can trust the functioning, stability and integrity of the financial market. If customer data is to increasingly become a commodity, customers will become data suppliers at the same time. It is vital that the interests of all market participants (including those of consumers) are equally taken into account. Data protection authorities are primarily responsible for ensuring that this is the case. However, there may be cases where financial supervisors could directly be called on to take action.

- Following the entry into force of the European General Data Protection Regulation (GDPR) at the

end of May 2018, firms supervised by BaFin may face large fines if they breach data protection regulations. As these fines may also have a significant impact on a firm's solvency in extreme cases, data protection violations are also an issue for financial supervisors.

- If data protection violations become more frequent, this could raise doubts as to whether business operations are running properly and supervisors could be called on to take action.
- If a firm supervised by BaFin systematically and intentionally violates relevant regulations when using customer data, this could also raise doubts in relation to the suitability of management in some specific cases.

### 3.2.2 Reliable options for controlling how data is used

Users should still be able to keep control over their data even after it has been released. Users must be able to keep an overview of the data they have provided and who they have provided it to, be able to obtain information on how their data is going to be used and should be able to easily withdraw their consent to their data being used. The right to delete data and for it to be forgotten must be ensured.

One idea to ensure that customers have an overview of how their data is used and to allow companies to enable this involves the implementation of automated protocols when setting up databases and data management systems. For example, a note could be attached to each piece of data. This note would provide information on the analyses this piece of data is to be used for and by whom. If an algorithm wants to have access to the piece of data, this would only work if the note grants the algorithm access to it. And for each piece of data,

a corresponding log file would automatically be kept as a record on when, for what use and who (e.g. which algorithm) the relevant data unit has been accessed by.

With solutions like these, which are commonplace in traditional data management and in other contexts, firms can keep an overview of how customer data is used and can manage both data and user profiles. As a result, companies that have such a data management system can find out very quickly how, when, for what purpose and who customer data has been used by. If the customer withdraws their consent for data usage, this can be implemented relatively quickly. Germany's Advisory Council for Consumer Affairs also recommends setting up a consumer-oriented data portal.<sup>11</sup> Such a portal could give consumers more control over how various providers use their individual data.

<sup>11</sup> German Advisory Council for Consumer Affairs, loc. cit. (footnote 10).



© iStock/From2015

The objective is that consumers can delete and change their data in a centralised manner and also centralise access rights management.

### 3.2.3 Actual freedom of choice

In addition to information and monitoring, it is vital that customers are given actual freedom of choice as to how their data is used to ensure data sovereignty. The basic principle of any sovereign decision is a feasible alternative: if people do not have real freedom of choice, they cannot reach any decisions, especially sovereign ones. Customers should not actually be forced to agree to an extensive use of their data and must have (at least) an alternative. One burning question is what these alternatives will need to specifically involve in order to ensure that sovereign decisions can actually be made. Is it enough if products are available on the market and customers have to give less data for them? Or should every single company offer alternative products as well? How should these alternative products look like? They probably wouldn't have the same features as the products available to customers who provide more data. And yet they should not be fully unattractive for the customer because this would mean that there would be no actual freedom of choice.

Companies may also give customers the opportunity to approve the use of some data for a clearly defined purpose and within a limited timeframe. Many BDAI applications could also run via privacy-preserving data mining on the basis of anonymised data. Sink-or-swim situations, where the customer can only choose between

providing an extensive amount of data and not using a product or service has nothing to do with freedom of choice. It is essential that customers can generally decide not to provide their data if this goes beyond what is necessary for meeting the terms of the contract they are seeking to enter into.

And when people also have to give access to data from social media, apps and portals to gain access to financial products at better conditions, this cannot be described as a sovereign decision. This is because customers that do not want to do this or do not have this data (e.g. customers who are not familiar with digital processes and systems) would be at a huge disadvantage.

## 3.3 Discrimination-free access to financial products within the context of BDAI

Differentiations based on personal data are common and make sense in principle. For example, if a customer wants to take out vehicle insurance, the insurer is explicitly required to request a risk-adequate price under the applicable supervisory law. The difficult question is: when does useful and desirable risk adequacy and differentiation stop and when does discrimination aimed only at maximising profits begin? (see also "What can differentiation lead to?" page 23).

## Scenario

### What can differentiation lead to?

The new forecasting options that BDAI offers can be compared with the zoom-in function of high-definition screens. Where it was previously only possible to get a vague picture, highly precise information is now available and can be analysed and “zoomed in” almost endlessly. The differentiation opportunities associated with BDAI are thus not completely new but they are significantly better and more precise than less recent processes.

Risk assessment in health insurance is one example. BDAI could possibly allow human health risks to be predicted with even greater precision. Conventional information channels alone such as medical reports could be better evaluated thanks to BDAI. But BDAI also allows information from medical reports to be combined with information from social media. With this additional data, which in many cases is provided by customers themselves, it is possible to achieve increasingly precise risk differentiation. Irrespective of this, it is possible that BDAI will further improve medical diagnosis and forecasting possibilities (e.g. predictive analytics). What will these developments lead to?

Will such precise risk forecasts and differentiation result in significant customer groups being excluded from the community of policyholders that are paying the right price because they can no longer afford to insure their risks (as these could be better assessed)? Will humans with “good” risks be the only ones who will be able to get insurance? Who will then bear the risks of those that were previously part of this community? Will this be society, or in other words, taxpayers?

It can be assumed that extensive BDAI-supported risk selection will give rise to social debates, which in fact would be nothing new – think of the insurability of terrorism risks. However, the magnitude of the debates and the impending issues resulting from BDAI-supported risk selection could reach a whole other level. It is possible that not everything that is technically possible will be useful or acceptable, also in the financial sector.

In the context of BDAI, the right balance needs to be found between necessary differentiation and undesired discrimination, and discrimination-free access to financial products needs to be ensured. As mentioned above, BDAI provides deep insights into the private sphere of customers, for instance, their preferences, wishes and their willingness and ability to pay. This information can be used in the customer’s interest to tailor products and services to their needs. But it can also be used deliberately against consumers or at least to disadvantage them. A provider that knows a great deal about a person can use this information in order to make the most of their willingness to pay, for instance, also based on specific life situations (see also

“Making the most of consumers’ willingness to pay in order to maximise profits”, page 24). They can also deliberately exclude (groups of) customers by setting prices that exceed their willingness and ability to pay. In addition to the deliberate discrimination against certain consumers (or consumer groups), this could also lead to unintentional discrimination if the algorithm reaches discriminatory decisions even if the user has not explicitly programmed this.

Both types of discrimination and the question of how this can be avoided are addressed below:

## Scenario

### **Making the most of consumers' willingness to pay in order to maximise profits**

Let's imagine what online stores will look like in the future. As soon as the customer enters the store, they are offered a wide range of products and services that are almost always tailored to their preferences, life situation and current needs. The customer is impressed. They only need to click on "buy". The price is right even if it is close to the price that the customer is just about prepared to pay. However, as the product or service is specifically tailored to the customer, it is more difficult to compare prices directly.

This hypothetical scenario highlights another advantage that companies could have thanks to BDAI applications – in addition to growing product ranges and market shares. BDAI offers unprecedented opportunities to extract the consumer surplus.<sup>12</sup> This would be a blessing for companies but a curse for users and consumers.

In particular, linking data on customer needs and preferences to financial and behavioural data using BDAI can provide deep insights into previously unknown consumer characteristics, such as their (situational) willingness and ability to pay. This private information can also be used against consumer interests. It is in the economic interest of consumers that at least their willingness to pay and (to a certain extent) their ability to pay are not disclosed to providers.

Otherwise, consumers or consumer groups may end up buying products that are overpriced when BDAI is used. BDAI can help companies gain detailed information on the maximum price that larger consumer groups are willing to pay – either because they themselves have this data or because they

can buy it. There is a risk that companies will use this information specifically to increase earnings as extreme price differentiations (segment-of-one) can enable them to make a much higher profit (by setting higher prices) without having to fear decreasing sales volumes.

This does not concern the payment of higher prices for better or more suitable services, such as higher insurance premiums for hedging higher risks. This would be a different form of differentiation encouraged by supervisors. Rather, this relates to individual and situational pricing for products that are (almost) the same. BDAI applications could make it easier to develop (mass) individualised products and services at a low cost. Providers could add individualised components to standard products – at no additional cost – making it more difficult for consumers to compare or switch to other offers or providers.

What is clear is that price differentiation is neither prohibited per se nor illegitimate in principle. It is a key element of healthy competition, also in the financial sector. Although this is similar to the phenomenon described above, where risk adequacy is perfected on the basis of BDAI, differential price strategies in competition based on the customer segment, geographical location or life situations are, however, questionable if they result in extreme asymmetries in the context of BDAI. Put simply, how much of an uneven playing field can there be between omniscient providers and customers whose information is available and literally predictable before society starts to fight back and legislators and, in the case of financial service providers, regulators need to intervene? These complex issues will need to be discussed and the pros and cons will need to be evaluated. Financial regulation has been undergoing such cycles for decades. The industry would be well advised to anticipate them.

---

<sup>12</sup> Consumer surplus is the difference between the maximum price that a consumer is willing to pay for a product or service and the price that they actually have to pay on the market.



### 3.3.1 Deliberate discrimination

Linking information from a variety of sources using BDAI can help to reveal consumers' willingness and ability to pay for specific products and services with a relatively high level of precision. Another specific feature of BDAI applications is that characteristics that are not directly gathered can also be revealed. In simplified terms, if nine customer characteristics are available, the tenth characteristic no longer needs to be gathered because it can be derived from the nine characteristics with great precision. If this gives rise to discrimination, consumers would not be able to make a connection with the personal data they have provided. And they cannot do anything about this type of discrimination

either. Companies have to ensure that there is no such discrimination and allow outsiders, such as supervisory authorities, to check this. Algorithm-based decisions need to be explainable. This is the only way to establish a corporate structure and culture that tackles discrimination effectively.

### 3.3.2 Unintentional discrimination

Even if companies or software developers have no bad intentions, algorithms can still display discriminatory behaviour or reach discriminatory decisions. Algorithms learn from data. And if this data suggests a discriminating view to the algorithm or suggests discriminatory decisions to reach the optimal solution,





© iStock/from2015

i.e. to maximise profits, (groups of) individuals could be discriminated against unintentionally. To solve this problem, technical approaches can be used, such as non-discriminatory data analysis and evaluation processes. In these processes, it is necessary to overcome the challenging hurdle of translating the ethical/legal concept of discrimination into a mathematical definition to ensure that discrimination can be verified with an algorithm and be prevented.

There are currently many approaches and research projects on this but a generally accepted standard has so far not been established. Ultimately, companies need to ensure that algorithms are designed in a way that legal requirements are taken into account. They have to prevent erroneous or prohibited conclusions to be drawn from their models using appropriate monitoring and transparency mechanisms.

# 4 Summary

BDAI has the potential to fundamentally change financial markets. New processes can result in key competitive advantages. Companies will therefore hardly be able to avoid having to develop a strategy on how to deal with BDAI. Many will certainly invest in BDAI readiness to ensure that they and their systems are BDAI-ready. But there may also be companies that will find their niche, providing products and services that are labelled as "guaranteed BDAI-free".

Neither supervisors nor regulators have yet found conclusive answers to all the questions raised due to BDAI. For this very reason, BaFin published its BDAI report in June 2018. It is now seeking an open dialogue with members of industry, the global regulatory community, academia and the press (see "Consultation" info box, page 25).

## Consultation

The report "Big data meets artificial intelligence – Challenges and implications for the supervision and regulation of financial services" is aimed at laying the foundations for in-depth discussions on big data and artificial intelligence. To this end, BaFin has invited a wide range of players, including companies and associations, other national and international supervisory authorities, representatives of academia and journalists, and consumers, to take part in the

consultation on its report. Further information can be found at [www.bafin.de](http://www.bafin.de).

The submitted responses will not be published individually but BaFin is planning to publish an anonymised and aggregated evaluation online.

The next issue of BaFinPerspectives will also cover the evaluation.

# III

The financial world is undergoing profound change because of the impact of Big Data Artificial Intelligence (BDAI). Established banks will hold their ground above all if they systematically work on their strengths, exploit their local presence and offer customers real value added.

# “This black-or-white debate is too superficial for me”

Interview with

**Prof Dr Stephan Paul,**  
Chair of Banking and Finance, Ruhr University  
Bochum



**Professor Paul, Bill Gates prophesied in 1994 that “banking is necessary, banks are not”. Do we have to admit in 2018 that he was right? Will his prediction come true in the next few years?**

With respect, but this black-or-white debate was and is too superficial for me. What we are experiencing are metamorphoses, the type of processes of change we have already observed in other industries. The end of books and newspapers was prophesied two decades ago, for example. Despite all the economic problems, they still exist, but they have changed under pressure from digitalisation. It's the same in the banking industry: banks have already adapted their internal and external processes to a considerable extent, but they still have a long way to go to remain sustainable. My forecast is therefore that banks will still exist in 25 years' time, but that they will look completely different than they do today.

**Which technology do you consider to be the decisive game-changer in banks' journey into the future?**

The analysis of very large data volumes using artificial intelligence – Big Data Artificial Intelligence, or BDAI – is certainly having the most serious impact. In the area of

investment advice, for example – the expansion of which many banks are now championing in light of depressed interest income – we can see that BDAI-based “robo-advice” can be a very effective and efficient solution for basic retail portfolio management requirements. Personal consulting is increasingly becoming the second-best alternative in this area, for both cost and quality reasons. BDAI will probably revolutionise banks' internal processes to an even greater extent: take the example of credit checks in the lending business.

**What about blockchain technology?**

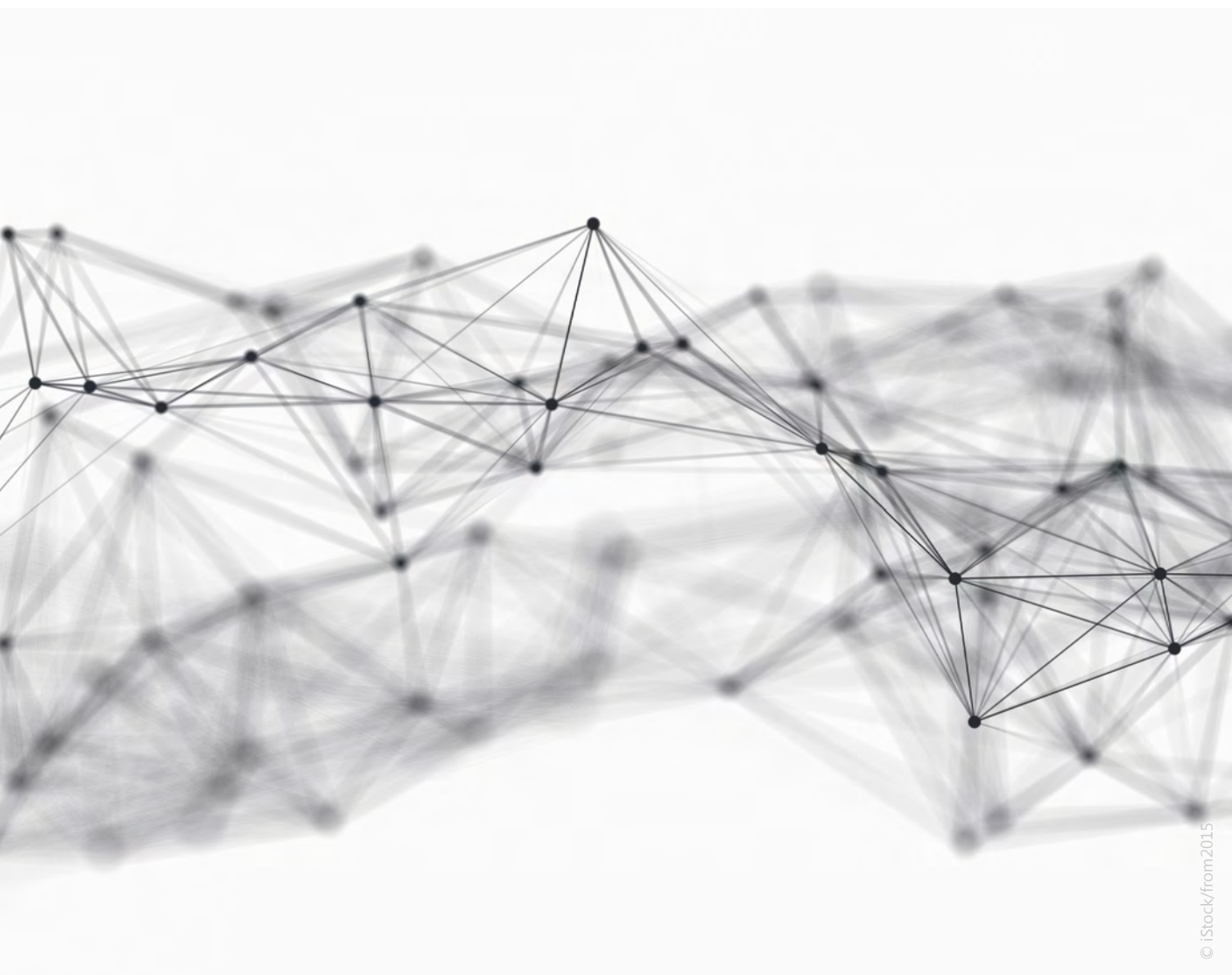
This is an area where we are seeing the first suppliers building their business model on this technology: effectively “Fintech 2.0”. Especially where security is concerned, this is undoubtedly a technology with future potential. But when I consider how much energy blockchains use and how time-consuming the transactions are, I think the current hype is overdone. By contrast, expertise in BDAI is already crucial today for stealing a competitive edge. And the banking industry must take care here not to fall behind the data giants from other sectors.

**Established banks and insurers are using agile methods in their own labs in an effort to copy fintechs and insurtechs. Do you think they will be able to make good the technology lead and stay in the market?**

These labs are popping up like mushrooms at the moment, but simply setting them up is not enough. What matters most is how the signals coming from these think tanks impact the existing organisation and change traditional corporate cultures. The lab can't be an isolated island. As many bridges to the mainland as possible must be built so that it can become the

organisation's innovation driver. Even then, not every bank will succeed in riding the peak of the digitalisation wave. That would also be too uneconomical. Instead, as is already evident today, there will be more and more alliances between banks and insurers on the one hand and fintechs/insurtechs on the other. The established players and the newcomers will enrich and change each other – in the sense of metamorphoses

**As a first step, the digitalisation of business models requires standardised data and processes.**



© iStock/from2015

**But this standardisation naturally also means sacrificing flexibility. How critical do you see this loss of flexibility for the market as a whole, and are approaches already emerging that could solve this problem?**

As far as basic requirements in both retail and corporate banking are concerned, standardisation is already well established, and digitalisation is actually accelerating this trend. This is a situation in which not every bank can still go its own way. However, similar product offerings based on similar IT and management systems, possibly sourced from only a handful of suppliers, run the risk of homogenisation, which ultimately also constitutes a systemic risk. But because this trend can no longer be reversed, it is all the more important for me to ask where the bank in question can still preserve its individuality in future and demonstrate expertise and relevance to its customers. This will be the only way to achieve sustainable competitive advantages.

**And where could that be?**

In the corporate banking business, it would clearly be in providing support and advice for customers to help them grow their business models in the digitalised world of Industry 4.0. We are experiencing the strongest process of upheaval in decades in almost all sectors of the economy. What this means for corporate finance, however, has not yet been properly thought through. If the practical formula “financing must fit the business model” applies, then the disruption of business models and innovative forms of organising and managing value chains mean that the challenges to corporate financial executives when it comes to raising liquidity are also facing radical change.

The intensification of cross-company alliances between value-adding partners, for example, raises the question of what the credit rating in the context of the bank rating should ideally be based on in future. What is happening is that traditional corporate finance is increasingly becoming project finance – uncoupled from the company as a whole. Individual loans are being transformed into value chain loans. This refers to larger investments that are increasingly being implemented in networks of multiple companies across different stages of the value chain, and whose success

depends on the quality of the partners involved. The success of the project, and hence the ability to repay the loan, is no longer the responsibility of a single actor, but of the network of actors – some of whom may have different credit ratings. Industry 4.0 is also leading to changes in collateral, which often still underpins loan agreements, at least for small and medium-sized enterprises: in the wake of digitalisation, corporate investments are focused less on traditional fixed assets and increasingly on intangible assets, in particular software and patents (intellectual property), as well as on support, maintenance and training costs. In many cases, these intangible assets are so company-specific that calculating lending values and limits can only rarely be based on the sort of generally accepted market prices that we know from commodities, vehicles or even real estate.

Advising clients in this process of transition is a tremendous opportunity for banks, but will require business client advisors to massively expand their skill sets.

**What about the retail banking business?**

The majority of Generation Z, i.e. tomorrow’s customers, self-critically admit that their general economic education is not sufficient to build up adequate retirement savings without help. Especially because empirical studies have shown that younger people, too, appreciate a personal contact person, this is a great opportunity for banks. The personalised retail sales network proves to be an important strength, making proximity to customers a factual and emotional experience. However, it also significantly increases requirements for expertise – in particular where investment advice is concerned. Banks will only be able to achieve competitive advantages over fintech companies if the advisors are also superior to progressively improved robo-advisors. The personal, local sales presence therefore has a future, albeit at fewer locations and with staff who are more highly qualified.

**Professor Paul, thank you for the interview!**

# III

Blockchain provides an additional logical layer on the internet for transporting assets. The learning curve is steep, but blockchain can make IT both more secure and massively more cost-effective.

# Distributed Ledger Technology: Blockchain as a Basis for Information Security

Authors

**Christian Flasshoff,**

Research assistant, Frankfurt School Blockchain  
Center, Frankfurt am Main

**Michael Mertens,**

Chair of the Executive Board, CryptoTec AG,  
Cologne

**Prof Dr Philipp Sandner,**

Head, Frankfurt School Blockchain Center,  
Frankfurt am Main

**Sebastian Stommel,**

Researcher, CryptoTec AG, Cologne

## 1 Introduction

Awareness of blockchain technology has been on the rise since the introduction of bitcoin in 2008. However, blockchain can do much more than managing a digital currency. The technology has the potential to challenge established business models fundamentally. Expectations for blockchain technology are already evident from the fact that the market capitalisation of the “cryptocurrencies” climbed to over 600 billion US dollars in 2017.<sup>1</sup> In the fourth quarter of 2017, funds invested in “initial coin offerings” (ICOs) exceeded traditional venture capital financing by a factor of 16.<sup>2</sup> An ICO is comparable to an IPO in which money is collected from investors, but is based on blockchain technology.

To enable an assessment of the realistic potential of blockchain technology, this article takes a closer look

at this technology compared with conventional IT systems and focuses in particular on the security of IT systems. Blockchain technology challenges many of the principles of traditional IT and solves many security issues in a fundamentally different way. Blockchain has the potential to significantly increase the security of IT systems, while at the same time massively reducing IT costs. Blockchain is not automatically the best solution to every problem. Besides, specific requirements must be considered during implementation to prevent risks. This article therefore also describes critical success factors for implementing blockchain projects. Involving cryptography experts early in the development process is essential to ensure that blockchain applications are as secure as possible. Blockchain not only transforms a company's IT department, but it can also impact the structure of the entire value chain. For this reason, the article also considers the potential for changing enterprise business processes from a holistic perspective.

---

1 Coindesk, Q4 2017 State of Blockchain, <https://www.coindesk.com/research/state-blockchain-q4-2017>, retrieved on 8 May 2018.

2 Coindesk, loc. cit. (footnote 1).



# 2 Advantages of blockchain technology

## 2.1 Immutable database

A blockchain is an immutable, continuously evolving database (“ledger”). This immutability is an advantage over conventional databases that is usually underestimated. At present, data are objects that are very easy to change. For example, it is not difficult to modify an entry in the main memory of a computer or a conventional database. In fact, IT systems are designed so that data can subsequently be changed easily. This function makes sense for many applications, but it also represents a severe security risk in conventional IT systems. Blockchain technology represents a paradigm shift because absolute data immutability enables entirely new approaches to designing IT systems. For example, it is no longer necessary to safeguard system security using dedicated infrastructure and firewalls. Instead, all data in the blockchain is already secured by cryptography and cannot be manipulated.

This data immutability allows for the implementation of entirely new business models because the data stored in the blockchain is resilient and trustworthy. As a result, payment transactions can be executed automatically using this data, for example, and the intermediary who confirms or guarantees the authenticity of the data becomes redundant. The data in a blockchain is so secure that even ownership rights and related details, such as those recorded in a land register, can be securely stored in the blockchain. Even democratic elections can be implemented by blockchain in a tamper-proof way. This preserves the secrecy of the ballot while ensuring that it is transparent to everybody that the elections were conducted properly.

## 2.2 Trustless systems

The principle until now has been that the longer data was held in the system, the more insecure it became because attackers could manipulate the data. The average time between a successful attack and detection of the attack is 180 days.<sup>3</sup> Blockchain turns this principle on its head: The longer data is stored in the blockchain, the more secure it becomes because the authenticity of data is verified by a growing number of participants in the network. For the security of some blockchain architectures, it is even irrelevant whether the identity of the participants is known or not. Previously, systems became increasingly insecure when they were accessed by unknown participants. In the case of blockchain, even unknown participants can interact with it and make the system more secure.

In connection with blockchain, the term “trustless system” means that the servers involved and their operators do not have to be trusted because the data in the blockchain verifiably cannot be manipulated. The blockchain itself creates trust in the system since the blockchain protocols automatically verify compliance by the participants with the blockchain rules. Process risk can thus be reduced as a blockchain automatically ensures that contracts are executed and payments are processed.

<sup>3</sup> Backofen, We need a comprehensive immunization of society against cyberattacks, <https://www.telekom.com/en/company/management-unplugged/details/eight-steps-to-cyber-immunity-for-enterprises-517446>, retrieved on 8 May 2018.

**Figure 1: Conventional database vs. blockchain ledger**





© iStock/From2015

## 2.3 Protection from data theft

Another advantage of blockchain technology over conventional databases is the protection it offers against the theft of massive data sets. There have often been headlines in the past about hacks of central databases with millions of stolen records, such as at Sony, Target, and Home Depot. Since a blockchain no longer requires credit card records, for example, but relies on end-to-end security, the data can no longer be stolen from servers. In particular, blockchain technology also offers the capability to store data in encrypted form. Additionally, direct payment functionalities and automatically executed contracts (“smart contracts”) can be implemented in blockchains using international consensus. Capabilities like this – and many more – go far beyond the functionality of conventional databases.

## 2.4 Transparency and verifiability

Another innovation that blockchain offers is the validation of stored data. Gathering information has become very easy in the internet era. Google’s value proposition is to make all data available in the world searchable in a single search engine window. However, it is often challenging to validate the data. Blockchain technology now allows the authenticity of all data in the blockchain to be verified, a quality that brings with it many potential applications. For example, customers can be assured that drugs have been developed based on actual clinical studies that cars have been designed based on valid emission studies, and that food has actually been produced in the region stated on the label. Validating data in the blockchain thus increases transparency for companies, customers and citizens.

# 3 Blockchain supports information security

Information security is a key objective of many companies. The Allianz Risk Barometer 2018 lists the risk of cyber attacks as the second most significant risk for companies in Germany.<sup>4</sup> Logistics service provider Maersk, for example, felt the impact of a cyber attack. An attack by the NotPetya trojan is estimated to have cost Maersk 200 to 300 million US dollars.<sup>5</sup> Besides increased IT security requirements, companies are at the same time also pursuing the goal of reducing costs for existing IT systems and improving interoperability. Blockchain can be a crucial technology here, helping companies to enhance information security and cut costs. Blockchains are considerably more resilient to common attacks on web applications<sup>6</sup>.

## 3.1 Separation of information and network security

What exactly makes blockchain applications so secure compared with conventional IT systems? To be able to answer this question, it is necessary to address the network security structure of conventional IT systems. Conventional IT systems feature a strict boundary between the outside and the inside. Only users inside the system can access the data and make changes in the system. To ensure security, access to the inside part is controlled at the operating system level. Depending on the required security level, the design of this access control may be more or less complex. Firewalls and

encrypted VPN<sup>7</sup> connections, for example, ensure that conventional IT systems are secure.

In the world of blockchains, however, this separation between the inside and the outside is almost entirely eliminated. A “public blockchain” is a public, redundantly stored database. The security of the data depends solely on possession of the relevant key and is safeguarded by cryptographic protocols. Security, therefore, does not need to be ensured by firewalls, so the blockchain decouples information security from network security. Essentially, it does not really matter if third parties have access to the blockchain (network security), as long as the data in the blockchain is protected by cryptography (information security). Of course, a blockchain does not necessarily have to be publicly accessible – it can also stay within a company (“private blockchain”). This blockchain approach enables enhanced data security while reducing security effort compared with conventional IT systems.

## 3.2 Security of blockchain standards

Blockchain technology is still in an early stage of development. For this reason, there are many different providers with different approaches. One criticism often levelled is that blockchain does not yet have adequate, consistent standards.<sup>8</sup> However, competitive advantages are rarely achieved by complying with rules, but rather by setting them. Companies such as Microsoft, Apple, Google and Facebook are among the most valuable companies in the world precisely because they have established their own standards and have not just waited for third-party standards. To gain a competitive edge in new technologies, it is often more important to be faster in the market than to offer the more perfect

---

4 Allianz Risk Barometer, Die 10 wichtigsten Geschäftsrisiken in Deutschland (The 10 most important business risks in Germany), [https://www.allianz.com/v\\_1516057200000/media/press/photo/risk-barometer-2018/Allianz\\_Risk\\_Barometer\\_2018\\_Top\\_10\\_Business\\_Risks\\_Germany.jpg](https://www.allianz.com/v_1516057200000/media/press/photo/risk-barometer-2018/Allianz_Risk_Barometer_2018_Top_10_Business_Risks_Germany.jpg), retrieved on 8 May 2018.

5 Scherschel, Heise Online – NotPetya: Maersk erwartet bis zu 300 Millionen Dollar Verlust (NotPetya: Maersk expects a loss of up to USD 300 million), <https://www.heise.de/newsticker/meldung/NotPetya-Maersk-erwartet-bis-zu-300-Millionen-Dollar-Verlust-3804688.html>, retrieved on 8 May 2018.

6 OWASP, Top 10 – 2017, The Ten Most Critical Web Application Security Risks, [https://www.owasp.org/index.php/Top\\_10-2017\\_Top\\_10](https://www.owasp.org/index.php/Top_10-2017_Top_10).

---

7 Virtual private network.

8 Hasso Plattner Institut, Bitcoin-Hype: HPI-Studie zum echten Innovationspotenzial der Blockchain (Bitcoin hype: HPI study of the true innovation potential of blockchain), <https://hpi.de/pressemitteilungen/2018/bitcoin-hype-hpi-studie-zum-echten-innovationspotenzial-der-blockchain.html>, retrieved on 8 May 2018.

technology. Especially with blockchain, however, security is indispensable. In particular, if hardly any existing technology is reused and everything is developed from scratch, blockchain developments often contain critical implementation errors. zCoin, for example, was the victim of a denial-of-spending attack. This exploited a mistake in the protocol and gave attackers access to coins that did not belong to them.<sup>9</sup> The DAO hack<sup>10</sup> is another a well-known case. That is why it is crucial for the project team to work together with cryptography experts when implementing blockchain projects. If possible, a formal proof of security should be developed to accompany implementation. This aspect is dealt with in more detail in section 5.1.

### 3.3 Communicable value added

Blockchain technology brings significant advantages to IT security. However, that does not mean that blockchain is automatically the best technology for each and every application. Before a company decides to implement a blockchain-based solution, it has to analyse the value added in great detail. If it does not, there is a risk that it will end up programming blockchain applications that offer no real advantages over other IT solutions. The principle of communicability is helpful here. It must be possible to communicate the added value to the customers or other stakeholders in an understandable manner. Blockchain applications that comply with this principle justify the investment and contribute to the success of the company. If this is not the case, blockchain may not be the best available technology.

---

<sup>9</sup> Schröder, Friedrich-Alexander-Universität Erlangen-Nuremberg – FAU-Forscher warnen vor „verbranntem Geld“ bei verschiedenen Kryptowährungen (FAU researchers warn against “burnt money” in various cryptocurrencies), <https://www.fau.de/2018/04/news/wissenschaft/angriff-auf-kryptowaehrung-entdeckt/>, retrieved on 8 May 2018.

<sup>10</sup> Biederbeck, WIRED – Der DAO-Hack: Ein Blockchain-Krimi aus Sachsen (The DAO hack: A blockchain crime thriller from Saxony), <https://www.wired.de/collection/business/wie-aus-dem-hack-des-blockchain-fonds-dao-ein-wirtschaftskrimi-wurde>, retrieved on 8 May 2018.

Some examples of actual value-added related to security thanks to blockchain technology are shown in the following:

- Payments in a peer-to-peer blockchain network are securely validated and immutable. The sort of recall that is allowed in a SEPA core direct debit mandate is not possible.
- Users can manage their own digital identity and themselves decide which provider should have access to which data if they maintain their user data using a blockchain. This allows users to benefit directly from the use of their data, for example by allowing it to be used for a clinical study.
- As soon as a smart contract has been digitally signed by both parties to the contract, the programming code guarantees the performance of the contract. These examples of value-added related to security can be communicated advantageously to customers and other stakeholders and are therefore good use cases for blockchain technology.

### 3.4 Cryptography

Cryptography is essential for the security of blockchain applications. The integrity of the data is protected by hashing (arithmetic operations). Digital signatures protect the authorship of entry and encryption protects access to information. This makes it possible to restrict access to and use of data, money, goods or other assets to defined participants. This requires cryptographic protocols with complex mathematical models. To explain how cryptography works in a blockchain, some processes are described in a simplified form in the following. The explanation uses the example of bitcoin, the widely used digital currency.

### 3.4.1 Secure identity

To participate in the bitcoin network, all users need an account in the bitcoin blockchain. To do this, the computer emulates 256 random coin tosses and remembers the result. There are  $1,157 \times 10^{77}$  different possibilities for the result, namely

115,792,089,237,316,195,423,570,985,008,687,907,853,  
269,984,665,640,564,039,457,584,007,913,129,639,935

This number of possibilities is so large that it could be used to assign a unique number to each atom in the universe. To generate this amount of possibilities, you could alternatively roll 100 dice at the same time. The enormous number of different possibilities of dice rolls is responsible for information security in the blockchain. It is impossible to guess the outcome of the dice roll and it would take millions of years to try it out using even the most powerful computers. The outcome of the dice roll must remain secret and later serves as a key to read the encrypted information. Hashing is used to create a public bitcoin address from the secret

dice roll, which is then stored in the blockchain. The encryption procedures are public and can, therefore, be audited. The security of the procedure is based on Kerckhoff's principle (1883), under which the security of cryptography is based on the secrecy of the key instead of the secrecy of the encryption algorithm. This principle is an important component of modern cryptography.

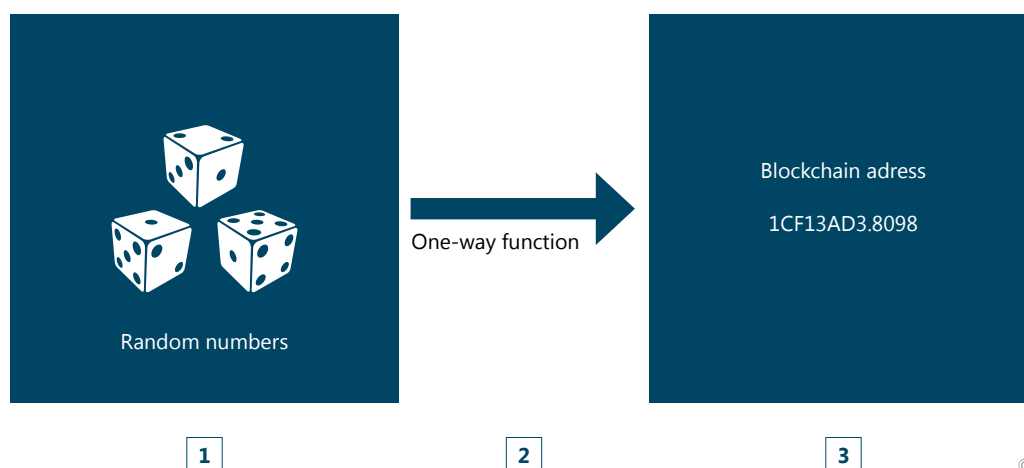
### 3.4.2 Transactions in the blockchain

The randomly assigned bitcoin address represents an account in the blockchain. This address can be used to receive bitcoins. Digital assets and other information can also be sent to other blockchain networks. For example, a randomly created blockchain address might look like this:

92024 57150 21345 42342 34121 34230 16215 64644  
54627 72316

Every participant who knows the address can send digital money or other assets to this address, in the same way as to a house address. And just like a house, only

Figure 2: Generating a blockchain account and address



© Cryptotec AG

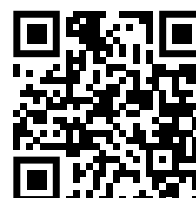
the owner of the blockchain address can use the money or decrypt the message. Decryption is done using a secret key (dice roll). It is not possible to extrapolate the underlying secret key from a public blockchain address. This is a one-way function of asymmetric cryptography. One-way functions are functions that can be easily calculated but cannot to all intents and purposes be inverted. For example, a blockchain address can be calculated from the dice roll, but not vice versa. One example of a one-way function from the physical world of a one-way function is when a glass is thrown onto the floor. The glass shatters into many small fragments and it does not require much effort to destroy the glass. However, an extreme effort is required to reassemble the fragments into the original glass.

### 3.4.3 Authenticating identities

However, blockchain addresses can be used for much more than account numbers in the bitcoin network. For example, industrial companies can assign individual blockchain addresses to specific products, goods and components, and identify them unambiguously in the production and distribution process. With the help of QR codes<sup>11</sup>, these addresses can be made machine-readable and registered in a blockchain. In addition, blockchain addresses can be assigned any attributes. For example, assigning the name of a company as an attribute makes it easier for other participants in the blockchain to identify the address. Knowledge of the outcome of the dice roll is necessary to assign an attribute. This makes it transparent that the attributes were only added by a participant who is also the owner of the address.

In a blockchain network, however, it is not absolutely essential to know the participants of the network. Even unknown and unconfirmed participants can participate in the blockchain without any loss of security. Whereas unknown participants in traditional IT systems pose a security risk, this is not a security or stability problem for public blockchains. This quality is an advantage of the blockchain because the barriers to adding new participants are lowered tremendously and users reach

**Figure 3: QR code for a blockchain address**



critical mass faster. Bitcoin is an excellent example of this because each participant can create their own account without having to register previously at a bank or administrative office. The participating identities can be authenticated at a later date if required. It is also possible to subsequently verify an unknown identity, thus allowing earlier actions to be retrospectively assigned to the confirmed participant. This advantage is also termed “key continuity”.

## 3.5 Identity management and key management

Blockchain identity management ensures that users of a blockchain do not need to know the long numbers or QR codes of a blockchain address by heart. The assigned attributes (for example company names) provide information about the identity of the participant and can be stored transparently in a database. Sending money to a blockchain address thus becomes as easy as sending an email. For blockchain applications with good identity management, there is no longer any need to enter the sort of complicated long account numbers that are required for SEPA credit transfers. A characteristic of good blockchain identity management is that several blockchain addresses can be assigned to a company or an individual. In practice, a variety of cryptographic methods are used for different blockchain applications, with the result that the blockchain addresses are not interchangeable. For example, blockchain solutions for a document repository use different cryptographic methods from blockchain solutions for P2P money transfers.

---

<sup>11</sup> Quick Response (see Figure 3).



The following example illustrates this scenario. A blog post author is normally paid for their work if it is published. However, the blog post is sent using a different blockchain than the agreed payment. Blockchain identity management is the interface between the two blockchains and ensures that the payment goes to the same person who wrote the post.

The function of the private key has already been explained. The secrecy of the key is important to ensure the security of the wallet (account) and the data.

Additionally, the user must not lose the key because this would mean that the digital wallet or the stored data would no longer be accessible to anybody at all. There is, therefore, a need for extensive backup and recovery solutions, both for individuals and for companies. Such solutions should, of course, be encrypted end-to-end. Otherwise, the blockchain security promise is irrelevant. In addition, the keys can also be divided and stored redundantly at trustees. Examples of such methods are *Shamir's Secret Sharing* or *multi-signature wallets*.

## 4 Blockchain in companies

### 4.1 Cash, information and goods flow

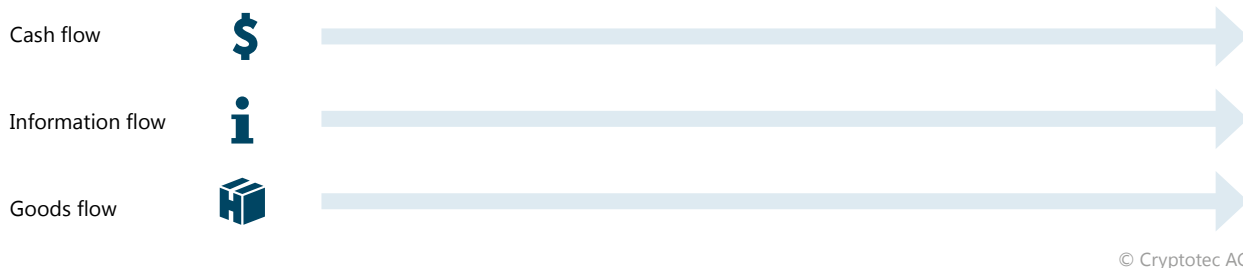
Blockchain also offers many advantages in enterprise applications, allowing the rapid, secure and cost-effective management of business processes. The technology allows for an automatic coordination of cash, information and goods flows. Any asset to which a value can be assigned can be managed in a blockchain. The owner of the asset can be identified unambiguously and reliably at all times. Furthermore, a blockchain can be used to transfer ownership and possession of an asset.

Such a transfer of assets in the blockchain is secure and cannot be reversed without the consent of the new owner. When an email is sent, only a copy is created and exchanged between the mail servers, whereas the assets are actually transferred in a blockchain. Physical goods can also be assigned a digital token, making it possible to track the goods. QR codes or RFID<sup>12</sup> chips can help amalgamate the physical good and the digital token.

---

<sup>12</sup> Radio frequency identification.

**Figure 4: The blockchain brings together the cash, information and goods flows**



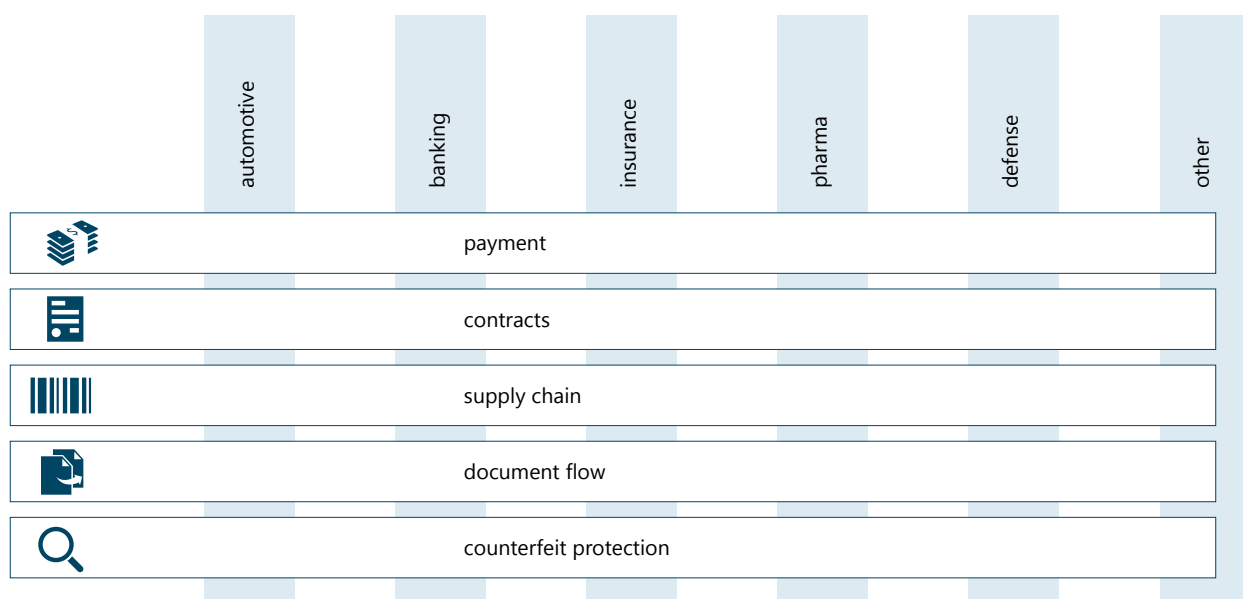
© Cryptotec AG

## 4.2 Accelerated process coordination

A blockchain can generate tremendous efficiency gains by modelling several processes, such as payments, contracts, supply chains, document exchange and protection against counterfeiting, in a single system. In such cases, the blockchain allows process steps to be optimally coordinated. For example, if an ordered item arrives at a company, documents can be automatically

checked, forgeries identified, the underlying contract executed and the money sent to the other party to the contract. Processes that previously ran separately can be performed automatically and in seconds thanks to the blockchain. The increased throughput speed harbours tremendous potential for cutting costs. Optimising processes through blockchain solutions can achieve savings of up to 99.9 percent and accelerate processes by a factor of 1,000. Horizontal coordination of the process chain can also be implemented on a cross-industry basis to simplify additional business processes.

**Figure 5: Horizontal coordination of the process chain**



© Cryptotec AG



## 4.3 Changing the value chain

Blockchain technology enables direct contact with all participants in a supply chain. For example, companies that are currently trapped in the middle of a supply chain have the opportunity to establish direct contact with customers. This allows manufacturers to sell a product or service directly to the end customer. However, this opportunity also poses a risk for established companies that previously had exclusive

market access and mediated between manufacturers and end customers. Blockchain technology attacks existing business models and strengthens the position of suppliers and manufacturers in the value chain. Moreover, blockchain enables companies to work together more efficiently and more quickly along the value chain. That is why being one of the winners in the future depends on understanding the value added of a blockchain.

# 5 Implementation of blockchain applications

## 5.1 Proof of security

The security of a blockchain application is decisive for its success or failure, so it is important not to make any mistakes during development that might endanger the security of the application at a later date. To better understand how to avoid such errors, it is helpful to visualise the process of developing a blockchain application. An idea for a blockchain can be outlined in three sentences. A concept can be defined in approximately 40 pages. The specifications need a further 150 pages. The actual implementation can then consist of three million lines of program code, corresponding to around 30,000 pages.

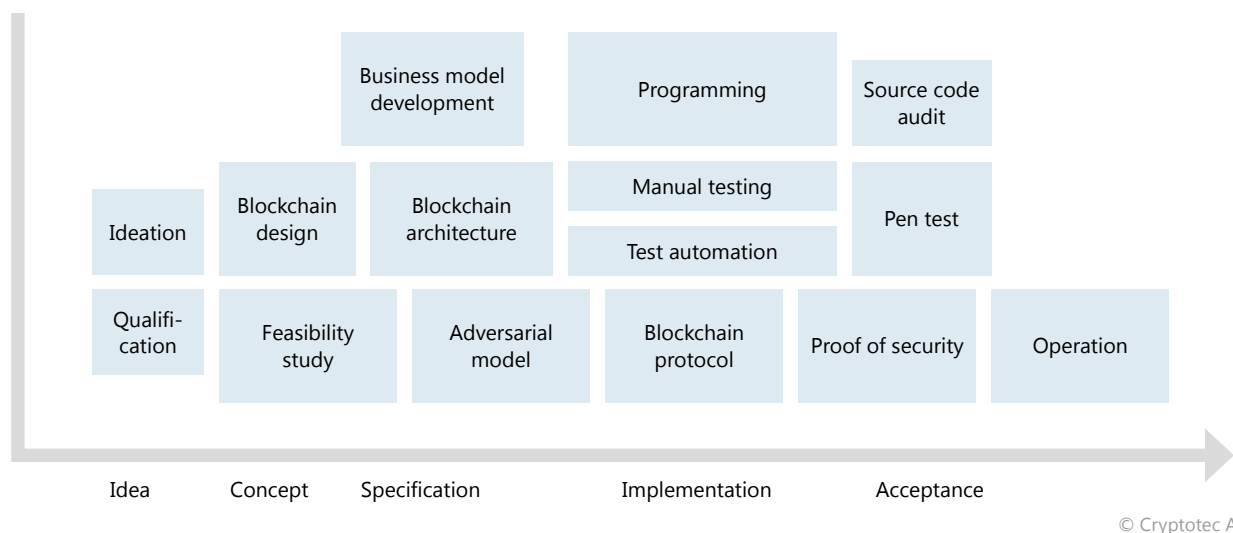
It is more or less impossible to check millions of lines of program code for security after the event and reveal conceptual errors. However, conceptual errors can have serious consequences for the blockchain, and in many cases cannot be rectified by a software update. It is therefore advisable to provide a formal proof of security

” The main advantage of blockchain technology is supposed to be that it’s more secure, but new technologies are generally hard for people to trust, and this paradox can’t really be avoided.“

Vitalik Buterin

at an early stage to ensure the correct statics, as it were, of the system. This proves mathematically that a system cannot be hacked by an existing computer. This abstract proof requires an adversarial model and protection objectives to be modelled. Such a positive proof of security requires only 20 pages and avoids subsequent

**Figure 6: Illustrative development process for blockchain projects**



high costs due to conceptual errors. The possibility of proofs of security has been known in computer science for years but is still only implemented rarely in practice. In accordance with a development process tailored to blockchain projects (see Figure 6, page XY), CryptoTec (editor’s note: where two of the authors of this article are employed), for example, provided proof of security to accompany the development of its internally developed blockchain document repository, guaranteeing document security, confidentiality and integrity.

## 5.2 Adversarial models and protection objectives

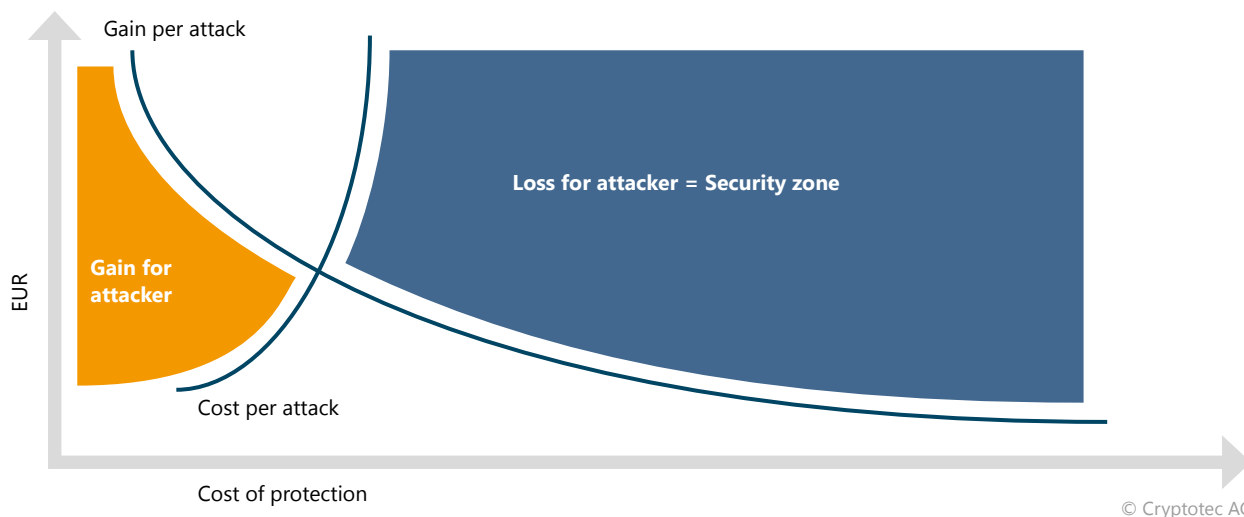
“If you don’t understand what you want to achieve, how can you possibly know when (or if) you have achieved it?”

Jonathan Katz

Adversarial models and protection objectives model possible scenarios and define the level of security required. An adversarial model defines the capabilities a potential attacker has and how an attacker can act. An attacker can be a professional hacker group or a user who circumvents payment. Developers must put themselves in the shoes of potential attackers to cover all possible attack scenarios. If one possibility is overlooked, it limits the security of the entire system. This takes a lot of time and experience with hacking attacks. In practice, internal employees at companies are often under time pressure and primarily know the perspective of their own company, not that of an attacker. In addition, the following principle applies in computer science: “A developer cannot test their own system.” Therefore, involving external experts is more or less mandatory when creating an adversarial model. By changing perspectives, potential new attack scenarios can be developed and the internal employees can focus on their core task of developing the system.

Protection objectives define the security level a system needs and the attacks that are to be prevented. There are two types of protection objectives:

**Figure 7: Profitability of attacks**



© Cryptotec AG

1. Every attack should be thwarted (100 percent protection).
2. Attacks that are economically advantageous for attackers should be thwarted.

100% protection is a difficult target to achieve as increasing the protection of a system becomes exponentially more expensive. In many cases, it is sufficient to make attacks by organised crime economically uninteresting. Figure 7 shows the gain per attack and the cost per attack as a function. The costs for the attacker increase exponentially as system protection increases. Once the cost of an attack is greater than the gain, the attack becomes uneconomic and unattractive for organised crime. It may, therefore, be sufficient to make a system secure enough that an attack is not profitable. The blockchain also increases the risk of an attacker being caught and prosecuted. In the past, hackers tried to remove possible traces on servers to avoid being identified. In blockchain applications, however, transactions cannot be retrospectively changed, but are transparently documented. The increased risk for attackers is an advantage of blockchain technology and can ultimately lead to lower costs for security measures.

## 5.3 User-friendliness

“Complexity is the worst enemy of security.”

Bruce Schneier

Bruce Schneier, American cryptography and computer security expert, succinctly summed up the connection between complexity and security in IT systems. An unnecessarily complicated design not only complicates usability but also creates more security gaps. An application should be as easy to use as possible and contain only the functions that are actually needed. User-friendly software does what the user expects it to do. Secure software does what the user expects it to do and nothing else. All other additional functions that the user does not need to increase the complexity of a system and at the same time impair security. This principle should be kept in mind especially when developing blockchain applications. In a highly networked world, products that are easy to use and difficult to hack are the most successful. Therefore, in addition to security, user-friendliness should also be an objective when developing new applications.



© iStock/From2015

## 5.4 Developing blockchain applications

“Bitcoin is not the kind of software where we can leave so many unresolved bugs that we need a tracker for them.”

Satoshi Nakamoto

It has already been mentioned that blockchain applications must be of high quality and may not contain any bugs. In many cases, bugs in the blockchain software cannot be reversed. For example, 500,000 Ethers, or about USD 375 million, of Parity Wallet users were frozen because the developers overlooked a serious bug in the code.<sup>13</sup> Quality management and auditing are very important when developing blockchain applications. It is therefore advisable to build on

blockchain modules that have already been developed and audited. Development costs can be reduced through collaboration with external blockchain experts, and security will be increased by proven solutions.

### 5.4.1 Defining requirements

When new blockchain applications are being developed, it is vital to define the requirements clearly in advance. This is the only way to select the best solution and prevent problems at a later stage. The Ethereum blockchain is a very popular platform for implementing new projects. However, that does not mean at all that it is the right platform for every project. For example, if you want to execute 1,000 transactions per second (TPS) in an industrial application, the Ethereum Network, which currently offers 20 TPS, cannot meet the application requirements.<sup>14</sup> The evaluation of requirements can be facilitated by an evaluation matrix for blockchain applications (see Table 1, page 46).

<sup>13</sup> Penke, Gründerszene – Parity-Millionen in Kryptowährung wohl für immer verloren (It looks like Parity millions in cryptocurrency are lost for good), <https://www.gruenderszene.de/fintech/parity-millionen-wallet-protokoll-999>, retrieved on 8 May 2018.

<sup>14</sup> AltcoinToday, Bitcoin and Ethereum vs Visa and Paypal – Transactions per second, <https://altointoday.com/bitcoin-ethereum-vs-visa-paypal-transactions-per-second/>, retrieved on 8 May 2018.



© iStock/From2015

**Table 1: Assessment matrix for blockchain applications**

Criterion	Qualification question
Speed	How many transactions can be validated per second?
Transaction size	How large can the data that are stored per transaction in the blockchain be?
Confidentiality	What confidentiality does the blockchain offer for information in the blockchain?
Availability	How high is the availability (in percent) of the application?
Verifiability	To what extent is it possible to verify that the data in the blockchain is correct?
Scalability	How easily can the blockchain be expanded by new functions?
Barrier to entry	Are users in the blockchain identified or can anonymous users also participate?
Payment	Can payments be processed using the blockchain?

## 5.4.2 Responsibility for blockchain development

“Blockchain is 80% business and 20% technology.”

William Mougayar

The enterprise-wide standardisation of processes is a major advantage of the blockchain. This often leads to the complete redesign of business processes, also known as “business process re-engineering”. It is not sufficient to transfer the existing processes to a blockchain. This only results in costs for the transition,

but no value added is created for the customer and no process optimisation is achieved. Competitive advantages can only be generated and the customer experience improved by completely redesigning business processes. The blockchain is, therefore, a topic that must be implemented by corporate management and the strategy department; individual departments lack the overview and decision-making authority for this. It would also be fatal to delegate the topic of blockchain to the IT department alone. The business share of blockchain developments is significantly larger than the actual programming since blockchain always includes security and economic incentives. An external perspective can also help analyse the company from a different perspective.

# 6 Summary

The blockchain is a crucial technology and can play a role in many sectors in the future. This technology has the potential to disrupt existing business models and replace them with more efficient models. Blockchain has several advantages compared with conventional IT systems. For example, data stored in a blockchain cannot subsequently be manipulated. Due to the separation of information and network security, third-party participants can also use the blockchain without posing a security risk. Information security is ensured through the use of cryptography. As a result, there is no need for the sort of complex protection mechanisms (VPNs or firewalls) that are necessary for conventional IT systems. Data can only be read by parties who know the secret key for opening the message. It is therefore also essential for the security of the data that the owner of the data keeps the key secret. The blockchain is by no means limited to the implementation of digital currency. Instead, the technology brings together the cash, information and goods flow in a single system.

This enables processes to be executed faster and more efficiently, which ultimately has a positive impact on the customer experience. Besides efficiency and new business models, blockchain solutions can enhance the security of IT systems. In practice, however, errors are often made when implementing blockchain applications. In many cases, such errors cannot be rectified by a simple update, but require additional development effort. For this reason, security should be ensured with the help of mathematical proof when blockchain solutions are implemented. In this context, all potential attack scenarios must be modelled and the required security level must be defined. Internal employees often do not have the experience and skills to develop bug-free blockchain solutions. The development of blockchain solutions should be managed by corporate management or the strategy department, as not only the IT department but all business units are affected by the changes brought about by blockchain technology.



© iStock/from2015

# I W

Digital ledger technologies such as blockchain promote the development of new, decentralised structures. Assessing them under the existing legal framework can shed light on numerous uncertainties.

# Blockchain Technology – Thoughts on Regulation

Authors

**Oliver Fußwinkel,**

Division for Innovations in Financial Technology  
Federal Financial Supervisory Authority (BaFin)

**Christoph Kreiterling,**

Division for Innovations in Financial Technology  
Federal Financial Supervisory Authority (BaFin)

## 1 Introduction

Take elements of game theory dating back to the 1920s and combine them with state-of-the-art encryption and network technology methods. This is how the Bitcoin network surfaced in January 2009.<sup>1</sup> Since then, the network has shown that the blockchain technology it is based on can work in a stable and reliable manner. So what does this have to do with BaFin? Its statutory duties include safeguarding the integrity and stability of the financial system and protecting consumers as a whole.<sup>2</sup> Blockchain technology is not a purely technological development, but also touches on aspects that are relevant from a supervisory perspective –

and even has potential implications for financial stability.<sup>3</sup> Before the matter can be explored in a supervisory law context, first a basic understanding of blockchain technology is necessary.

A blockchain is an immutable, public, append-only distributed digital ledger. “Public” means that the data can be accessed by anyone. Only certain participants can access private blockchains. “Immutable” means that it is virtually impossible to alter or delete data in a blockchain after it has been saved and encrypted. This means that it is only possible to add new data, as in

---

1 Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, <https://bitcoin.org/bitcoin.pdf>, retrieved on 10 July 2018.

2 See section 4 of the German Act Establishing the Federal Financial Supervisory Authority (*Finanzdienstleistungsaufsichtsgesetz – FinDAG*) and, for example, section 6 of the German Banking Act (*Kreditwesengesetz – KWG*).

---

3 Birch/Brown/Parulava, Special issue papers Towards ambient accountability in financial services: Shared ledgers, translucent transactions and the technological legacy of the great financial crisis, in: *Journal of Payments Strategy & Systems*, Vol. 10, No. 2, 2016, pages 118-131.





commercial bookkeeping, which does not allow entries in the book of prime entry to be deleted.<sup>4</sup> “Distributed” means that a public blockchain is not subject to the control of a single participant or organisation. Instead, the network (i.e. all participants as a whole) manages and safeguards the data, and each participant generally stores a full copy of all the data. The term “ledger” means that a blockchain can be used, as with Bitcoin, to not only manage and update units of account, but that the same fundamental method can also be used for many other types of digital records.<sup>5</sup>

The key components of a blockchain generally consist of a combination of cryptography, peer-to-peer network technology, consensus mechanisms, a ledger and a set of rules to define valid transactions.<sup>6</sup> This means that a blockchain is a distributed digital data structure that is, according to current knowledge, tamper-proof and can be used to store all kinds of valuable data.<sup>7</sup> One of the main characteristics of blockchains is that there is no need for a central authority that has to be trusted (as with cloud computing, for instance) and that each individual participant in a blockchain network has the ability to check and validate each individual transaction themselves from the moment the first transaction is recorded, as with Bitcoin, for example.<sup>8</sup> This means that a blockchain does not require any trust to be placed in an intermediary because it allows the participants themselves to create trust.

---

4 See sections 238 et seq. of the German Commercial Code (*Handelsgesetzbuch* – HGB) in conjunction with the application of the letter from the German Federal Ministry of Finance (BMF) dated 14 November 2014, ref. IV A 4 - S 0316/13/10003, Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD).

5 MIT Technology Review, *Explainer: What is a blockchain? Where it came from, what it does, and how you make one*, <https://www.technologyreview.com/s/610833/explainer-what-is-a-blockchain/>, retrieved on 10 July 2018.

---

6 Hileman/Rauchs: 2017 Global Blockchain Benchmarking Study.

7 Kreiterling/Mögelin, *Blockchain – ein Thema für die Finanzaufsicht?*, in: *Zeitschrift für das gesamte Kreditwesen*, no. 11/2017, page 528.

8 Greenspan, *Payment and exchange transactions in shared ledgers*, in: *Journal of Payments Strategy & Systems*, Vol. 10, No. 2, 2016, pages 172-180.

# 2 Emergence of decentralised ecosystems and the blockchain economy

One of the key questions relating to sustainable business activity is how to establish trust between strangers in order to allow transactions to be executed.<sup>9</sup> To date, this has been made possible by intermediaries such as banks and central securities depositories, although their role also pushes transaction costs up and thus makes the markets less efficient.<sup>10</sup> Blockchain technology can help to minimise the level of trust required and, as a result, lower the transaction costs incurred by the parties involved in the transaction, for instance by reducing reliance on intermediaries. To put this in perspective: problems resulting from abuse of trust, such as fraud, have a substantial negative impact on trade and commerce; the global damage caused by fraud, is estimated to amount to more than USD 4 trillion.<sup>11</sup>

By using blockchain technology, the level of trust required between transaction parties can be reduced by allowing the participants to verify actions taken within the network independently themselves (self-verifiability).<sup>12</sup> The “public network” this creates is designed as a deterrent to misconduct and to allow actions to be verified at any time and without the need for specific reasons. This means that blockchain technology could give rise to a new type of decentralised ecosystem: a blockchain economy. In decentralised ecosystems like these, agreed transactions would be executed, and largely enforced, autonomously based on rules such as those defined

in smart contracts.<sup>13</sup> Decentralised ecosystems would also manifest themselves in a new form of organisational design, based on governance rules specified in the blockchain.<sup>14</sup>

The emergence of decentralised ecosystems is affecting the traditional, established value chains within the financial services industry. Whereas in the past, these ecosystems aimed at the transfer of information, with the primary business advantage lying in the exploitation of information asymmetry<sup>15</sup>, the situation has already changed<sup>16</sup> due to the advent of fintech companies<sup>17</sup>. One of the effects caused by these innovative companies, which use technical solutions to specialise in individual parts of the value chain, is that they are making the uniform value chains in the financial services industry more fragmented.<sup>18</sup>

In decentralised ecosystems in the form of blockchain economies, each link in the value chains could potentially be affected to a much greater extent. The

---

9 Pearce/Warford, *World without end: economics, environment, and sustainable development*, 1st edition 1993.

10 Coase, *The nature of the firm*, in: *Economia*, Vol. 4, No. 16, 1937, pages 386-405.

11 Gee/Button, *The Financial Cost of Fraud 2017: the latest data from around the world*, <https://brand.crowe.co.uk/wp-content/uploads/sites/2/2017/02/crowe-the-financial-cost-of-fraud-2017.pdf>, retrieved on 10 July 2018.

12 Peters/Panayi, *Understanding Modern Banking Ledgers through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money*, in: *Tasca/Aste/Pelizzon/Perony, Banking Beyond Banks and Money*. *New Economic Windows*, 2016, pages 239-278.

---

13 Szabo, *The idea of smart contracts*, <http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html>, retrieved on 10 July 2018. While in a democratic state based on the rule of law, the courts remain the last enforcement mechanism under procedural law, the rules contractually agreed between the parties would actually result largely in automated, decentralised enforcement in a blockchain economy.

14 Beck/Müller-Bloch/King, *Governance in the Blockchain Economy: A Framework and Research Agenda*, [https://www.researchgate.net/publication/323689461\\_Governance\\_in\\_the\\_Blockchain\\_Economy\\_A\\_Framework\\_and\\_Research\\_Agenda](https://www.researchgate.net/publication/323689461_Governance_in_the_Blockchain_Economy_A_Framework_and_Research_Agenda), retrieved on 10 July 2018.

15 Healy/Krishna/Palepu, *Information asymmetry, corporate disclosure, and the capital markets: A review of the empirical disclosure literature*, in: *Journal of accounting and economics* 31.1-3, 2001, pages 405-440.

16 Alt/Ehrenberg, *Fintech – Umbruch der Finanzbranche durch IT*, in: *Wirtschaftsinformatik & Management* 03/2016, pages 8-17.

17 There is no generally valid definition of the term “fintech companies” as yet. As a combination of the words financial services and technology, the term generally refers to young companies that use technology-based systems to offer specialised, and particularly customer-centric, financial services.

18 Chiu, *Fintech and Disruptive Business Models in Financial Products, Intermediation and Markets-Policy Implications for Financial Regulators*, in: *Journal of Technology Law and Policy*, Vol. 21 (1), 2016, pages 55-112.

battle for the customer interface<sup>19</sup>, which is resulting, among other things, in the formation of platform economies, would also be influenced by the blockchain economy. Ultimately, there would be no need to trust a platform operator that could end up generating higher transaction costs in the long run as an intermediary. A blockchain economy has its own infrastructure platform that is created and controlled by its participants.<sup>20</sup> Consequently, the blockchain network does not just occupy the customer interface directly and control it on a decentralised basis, it involves the parties in the transaction process much more than any solution developed before. In these decentralised ecosystems, blockchain-based technology and processes can transfer not just information, but value.<sup>21</sup>

Such a major change in the technological infrastructure of the financial services industry would not only affect the systems used ("Which technology should be used?") and business processes, organisation and governance in place ("How and with whom should objectives be achieved?"). The potential that blockchain technology offers, could also have a significant effect on the strategy ("What should be done?") pursued by companies in the financial services industry. Consequently, blockchain technology could potentially have an impact on strategy, processes and systems.<sup>22</sup> Looking at blockchain technology only with a view to cutting costs could mean overlooking the earnings potential that it offers.

Questions relating to strategy, processes and systems in connection with the blockchain economy are important, but details critical to its success are also decisive. It is still questionable whether existing requirements, such as the European General Data Protection Regulation (GDPR)<sup>23</sup> and its "Right to be forgotten"<sup>24</sup>, could also be implemented in full via blockchain technology using the procedures that are currently known.

Additionally, the security and protection offered by current blockchain solutions is based on only one level. The defence in depth approach of ISO Security Standard 27033<sup>25</sup>, however, consists of multiple levels to ensure the maximum possible degree of data security and protection. For instance, the "perimeter" protection level offers the highest level of security and protection. In contrast, the lowest level of protection is the "data" level. All data stored in current blockchains (on-chain data) is at the data level. This raises the question as to what extent a blockchain solution could satisfy the protection needs of entities supervised by BaFin in the context of their respective information risk management.

---

19 Goodwin, The battle is for the customer interface, <https://techcrunch.com/2015/03/03/in-the-age-of-disintermediation-the-battle-is-all-for-the-customer-interface/>, retrieved on 10 July 2018.

20 Underwood, Blockchain beyond bitcoin, in: Communications of the ACM, Vol 59, No. 1, 2016, pages 15-17.

21 Church, MIT Management School, Blockchain, explained, An MIT expert on why distributed ledgers and cryptocurrencies have the potential to affect every industry, <http://mitsloan.mit.edu/newsroom/articles/blockchain-explained/>, retrieved on 10 July 2018.

22 Österle/Blessing, Business Engineering Modell. In: Österle/Winter, Business Engineering: Auf dem Weg zum Unternehmen des Informationszeitalters, 2nd edition 2003, pages 65-85.

---

23 Regulation (EU) No 2016/679, OJ L 119/1.

24 Art. 17 of the General Data Protection Regulation (GDPR).

25 See ISO/IEC 27033-2:2012(en) Information technology - Security techniques - Network security - Part 2: Guidelines for the design and implementation of network security, <http://www.iso.org/standard/51581.html>, retrieved on 4 July 2018.

# 3 Basic approach adopted by BaFin

Blockchain technology offers significant innovative capacity across a whole range of sectors, as well as the potential to influence the financial industry in many ways, such as in payment transactions, securities trading, asset management and banking. It is not yet possible to reach a definitive conclusion on the nature and scope of these effects. However, one aspect that stands out is the diminishing role played by intermediaries in a blockchain economy, as mentioned above. At present, BaFin mainly supervises companies with an intermediary function, such as credit institutions. Nevertheless, even in a future blockchain economy, it would still have to be possible to achieve the overarching objectives of ensuring the integrity and stability of the financial system, and

collective consumer protection. Technological teething troubles should sound a note of caution and help to curb the widespread indiscriminate enthusiasm for innovation that currently prevails, without blinding us to the potential offered.

When dealing with crypto tokens and with innovative financial technologies in general, BaFin is always guided by the principle of technological neutrality, true to the motto "same business, same risk, same regulation". This also allows it to continue to uphold the principles of proportionality and equal treatment based on the rule of law.



# 4 ICOs and crypto tokens: risks and supervisory classification

Manifestations of the blockchain economy can already be found in the financial market today and have supervisory law implications. In addition to the digital reproduction of what were previously paper-based processes and products, such as the launch of a bond via blockchain technology<sup>26</sup> and foreign trade financing using letters of credit<sup>27</sup>, new constructs of a disruptive nature are also emerging. These include the raising of capital using initial coin offerings (ICOs)<sup>28</sup>, a concept that has been growing in popularity considerably since around 2017 and which is to be analysed in greater detail in this document due to its current significance for investors and issuers. Another aspect of fundamental importance, not only in the context of ICOs, is supervisory classification of the various options available for representing value digitally in a blockchain using crypto tokens<sup>29</sup>. The section below therefore begins with a general supervisory assessment of various sub-groups of crypto tokens, before moving on to address the particular features and risks associated with their issue in the context of an ICO.

## 4.1 Crypto tokens

Crypto tokens can have different functions and characteristics. Some tokens are an integral component of a certain blockchain, such as Bitcoin for the Bitcoin blockchain and Ether for Ethereum. In addition, smart contracts can be used to create various function-based tokens, e.g. with Ethereum. These tokens are then created and managed within an existing blockchain

infrastructure (in this case, Ethereum). As smart contracts are freely programmable in principle, meaning that the corresponding tokens can differ from each other considerably, a case-by-case assessment is the only way of reliably categorising each token under supervisory law.

Critics of this approach, who understandably want to see straightforward solutions, fail to recognise the diverse ways in which tokens can be designed and their wide range of technical properties. They also do not fully take into account that programmers and distribution teams are free to use the terms that they choose to describe their creations; there might well be a thousand different terms for similar, and even essentially identical tokens. Meanwhile, the same term can be used to refer to a large number of different tokens. The critics also fail to recognise that the blanket assignment of different tokens to certain supervisory categories would, in a large number of cases, produce results that are not justified given the circumstances, and could potentially restrict the scope for innovation. They also ignore the fact that regulatory requirements in the form of vague general definitions that everyone has to adhere to effectively result in standardisation that at least limits the potential for innovation. Requirements like these are also extremely unlikely to take account of the basic legal principles governing regulatory and supervisory activities, namely the principle that administrative authorities are bound by law, the principle of proportionality and the principle of equal treatment.<sup>30</sup>

---

26 Daimler press release, Daimler and LBBW successfully utilize blockchain technology for launch of corporate Schuldschein, <https://media.daimler.com/marsMediaSite/en/instance/ko.xhtml?oid=22744703>, retrieved on 3 July 2018.

27 Zim press release, ZIM's Groundbreaking Blockchain-Based Bill of Lading, <http://www.zim.com/news/press-releases/zims-groundbreaking-blockchain-based-bill-of-lading>, retrieved on 3 July 2018.

28 Often also, and more accurately, referred to as "token generating events" or "token sales".

29 We used the term "crypto tokens" for the purpose of this article because it is unbiased and precise. The term is neutral and, unlike other terms such as "cryptocurrencies", "crypto assets" or "virtual currencies", does not imply any characteristics that crypto tokens do not necessarily have.

---

30 Regarding the principle of proportionality, see also Grzesick, in: Maunz/Dürig, Grundgesetz-Kommentar, 82nd supplement 2018, Article 20 marginal note 107.



© iStock/From2015

In general, crypto tokens can be understood as the digital representation of an intrinsic or market-assigned value using distributed ledger technology (DLT)<sup>31</sup>. This definition based on value emphasises, in particular, the currently prevalent use of crypto tokens as an investment object, without specifying in advance whether the token in question embodies a claim or obligation of an entity or triggers other payment flows in favour of the holder by virtue of its function.

The term “virtual currency” used in Article 1(2)(d) of the 5th Money Laundering Directive, which is designed to cover all potential uses of virtual currencies, will also prove significant: “digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or

legal persons as a means of exchange and which can be transferred, stored and traded electronically”.<sup>32</sup>

Crypto tokens are not unregulated per se, but rather fall under the existing financial market regulation - depending on the specific structure used in the case in question. This means that they are not regulated as a general category, but rather specifically and in a technology-neutral manner, based on substantive facts (and not on marketing considerations) that are subject to legal interpretation, meaning that they can also include new situations.

As a result, it is the specific individual case that determines the supervisory assessment of a business model based on crypto tokens. Based on the experience gained from evaluating business models in connection with crypto tokens to date, the main regulations that prove relevant for the purposes of the evaluation are those set out in the German Banking Act (*Kreditwesengesetz – KWG*), the German Securities Trading Act (*Wertpapierhandelsgesetz – WpHG*), the German Securities Prospectus Act (*Wertpapierprospektgesetz – WpPG*), and the German

---

31 The Bank for International Settlements (BIS) describes distributed ledger technology as follows: “DLT refers to the processes and related technologies that enable nodes in a network (or arrangement) to securely propose, validate and record state changes (or updates) to a synchronised ledger that is distributed across the network’s nodes,” BIS, Distributed ledger technology in payment, clearing and settlement, <http://www.bis.org/cpmi/publ/d157.htm>, retrieved on 3 July 2018.

---

32 Directive (EU) 2018/843, OJ L 156/43.



Capital Investment Act (*Vermögensanlangengesetz* – VermAnlG). Numerous other elements of financial market regulation also come into play, such as, in particular, the German Money Laundering Act (*Geldwäschegesetz* – GwG), the German Payment Services Supervision Act (*Zahlungsdiensteaufsichtsgesetz* – ZAG), the German Investment Code (*Kapitalanlagegesetzbuch* – KAGB), but also directly applicable secondary European law such as the EU Market Abuse Regulation (MAR).<sup>33</sup>

Clarity regarding the supervisory classification of a specific project involving crypto tokens can be achieved – after reading the preliminary information available at [www.bafin.de](http://www.bafin.de) – by obtaining an information letter from BaFin. Such information letters, as a form of simple

sovereign action, are not regulatory in nature as a matter of principle (section 24 of the German Administrative Procedure Act (*Verwaltungsverfahrensgesetz* – VwVfG)).

In addition, the supervisory laws give BaFin the power, in case of doubt, to make a binding declaratory decision – subject to a fee<sup>34</sup> – as to whether a company is subject to supervision under the Banking Act, the German Insurance Supervision Act (*Versicherungsaufsichtsgesetz* – VAG), the Investment Code or the Payment Services Supervision Act.<sup>35</sup> In practice, such individual declaratory

---

<sup>33</sup> Regulation (EU) No 596/2014, OJ L 173/1.

---

<sup>34</sup> Section 14 et seq. of the FinDAG in conjunction with section 2 (1) and Appendix 1 no. 1.1.8.1. of the Regulation on the Imposition of Fees and Allocation of Costs Pursuant to the FinDAG (FinDAGKostVO); the fee amounts to €10,000.00.

<sup>35</sup> See section 4 of the KWG, section 4 of the VAG, section 5 (3) of the KAGB and section 4 (4) of the ZAG.

decision only arises in special cases, as all four relevant acts generally allow, and normally require, BaFin to intervene by issuing a cessation and/or a winding up order if business operations are found to be unauthorised (applying the German enforcement doctrine of *intendiertes Ermessen*). In the opposite case, a negative statement regarding a potential authorisation requirement for a business project only makes sense as a non-regulatory form of information, as BaFin cannot decide that an entity is not subject to an authorisation requirement unless it has assessed this entity's entire business. In both cases, BaFin's contact form provides company founders with a straightforward digital channel for making initial contact with BaFin free of charge.<sup>36</sup>

Setting aside the legally relevant constituent statutory elements and their interpretation by BaFin/in the court decisions of the highest administrative courts, crypto tokens can – for the purpose of a simplified overview – be divided into three broad categories<sup>37</sup>:

- Payment tokens (like Bitcoin): these are generally used exclusively, or among other things, as a personal means of payment and they tend not to have any intrinsic value. They have no other function, or only limited functions, beyond this.
- Securities tokens (equity and other investment tokens): users have membership rights or contractual claims involving assets, as with equities and debt instruments.
- Utility tokens (app tokens, usage or consumption tokens): can only be used in the issuer's network to purchase goods or services. Very complex legal structures generally apply to utility tokens.

#### 4.1.1 Payment tokens and “virtual currencies”

Payment tokens like Bitcoin, Ether and Ripple's XRP are not currencies in the narrower sense of the term, which correspond to the constitutional framework for

a country's monetary system.<sup>38</sup> This means that, from a legal perspective, only legal tender and current account holdings linked to legal tender held at government-approved credit institutions, the latter also referred to in a derogatory sense as fiat money, would qualify as currencies. In economic terms, however, a currency serves as a means of payment, as a store of value and as a unit of account. These properties are directly related to each other. Crypto tokens such as Bitcoin do not, per definitionem, have any of these economic characteristics to a sufficient degree. Moreover, crypto tokens do not resemble currencies or conventional investments either in their performance or in terms of their characteristics. This means that they do not constitute currencies in economic terms, but are to be regarded more as a speculative object.<sup>39</sup>

BaFin has already assessed Bitcoins and similar “virtual currencies” from a supervisory perspective by including them in the guidance notice “Information on the Payment Services Supervision Act (ZAG)” (*Hinweise zu dem Gesetz über die Beaufsichtigung von Zahlungsdiensten*) dated 22 December 2011. The guidance notice has since been amended as part of the implementation of the Second Payment Services Directive. But even in its prior version, the guidance notice contained information that still applies today:

“The term “e-money” is a [...] legal term which, typologically speaking, only covers certain aspects of the economic phenomenon of electronic money. Regardless of whether computer network, server-based or card-based electronic units of value serve as means of payment in economic reality, e-money only exists, in particular, where it is issued in return for payment of a cash amount. [...] This means that units of value designated as means of payment that are created in barter clubs, private barter circles or other payment

36 [https://www.bafin.de/SiteGlobals/Forms/Kontakt/Fintech\\_Integrator.html](https://www.bafin.de/SiteGlobals/Forms/Kontakt/Fintech_Integrator.html).

37 It is possible, and not unusual, to see hybrid forms of tokens.

38 See section 14 (1) sentence 2 of the Deutsche Bundesbank Act (*Gesetz über die Deutsche Bundesbank*), Regulation (EC) No 974/98, Article 10 of 1 January 2002.

39 Thiele/Diehl, Kryptowährung Bitcoin: Währungswettbewerb oder Spekulationsobjekt: Welche Konsequenzen sind für das aktuelle Geldsystem zu erwarten?, in: ifo Schnelldienst 70, no. 22, 2017, pages 3-20.



systems in return for real economy services, goods deliveries or services, or that, like Bitcoins, are created in computer networks without any consideration being provided in return, cannot be classified as e-money, even if they serve the same economic function as e-money and, from a money creation perspective, have the actual potential of privately generated means of payment (see also the government's reasoning regarding section 1a (3), Bundestag printed paper no. 17/3023, page 40). [...] the removal of network money business (section 1 (1) sentence 2 no. 12 of the KWG) in the version of the 6th KWG amendment excluded the aspect of private money creation."

This means that BaFin not only established the general non-applicability of the provisions governing e-money, as defined in section 1 (2) sentence 3 of the ZAG, to the majority of the virtual currencies known at that time<sup>40</sup>. It also proved that the removal of network money business by the Fourth Financial Market Promotion Act<sup>41</sup> of 1 July 2002 was a conscious decision made by the legislator to abolish the former concept of network money business, which was still considered banking business under section 1 (1) of the KWG in the 6th KWG amendment (entry into force on 1 January 1998), as part of the implementation of the First E-Money Directive. This definition of network money business included the "creation and management of payment units in computer networks", which not only covers the subsequent e-money within the meaning of the EU E-Money Directives, but also would have included any other kind of virtual units of account which, like Bitcoin, are created without any consideration provided in return and are designed to act as a sort of secondary form of private money alongside legal tender.

The reasons cited by the legislator at that time for the creation of the concept of network money in 1997 appear almost visionary with regard to later developments: "Network money is saved by the user

on the PC's hard drive and is used once or several times to execute remote payments by way of a dialogue between the computers involved, with state-of-the-art cryptographic processes designed to protect against forgery or falsification. The payments are generally executed anonymously, as with cash."<sup>42</sup>

With the removal of this concept, which reads as if it had been tailored to reflect the virtual currencies that emerged on the basis of blockchain only years later, it was clarified that the creation and certainly the mere use of virtual currencies as a substitute for cash or book money did not constitute activities subject to authorisation requirements per se. This means that virtual currencies can be used to settle payment obligations between the users involved. Similarly, the mining of these tokens does not constitute an activity subject to authorisation requirements, because the miner does not issue or place the tokens itself, at least not in a system similar to Bitcoin.

Another provision set out in the 6th KWG Amendment was, however, deliberately maintained, namely the classification of units of account as financial instruments (only) within the meaning of the German Banking Act (KWG) pursuant to section 1 (11) sentence 2 no. 7 of the KWG. This meant that the authorisation requirements for transactions involving financial instruments could still be used to address gaps with regard to virtual currencies, in particular also with regard to anti-money laundering measures, while avoiding any conflict between the former network money business, as a form of banking business, and the harmonised regulation of the e-money business.

In 2011, BaFin classified Bitcoins and similar payment tokens as financial instruments in the form of units of account pursuant to section 1 (11) sentence 1 of the KWG. These are units comparable to foreign currencies

---

40 At that time, section 1a (3) of the ZAG (old version). Assessment on a case-by-case basis, however, is always decisive.

41 Fourth Financial Market Promotion Act, Federal Law Gazette (BGBl.) I 2002, page 2010.

---

42 Draft bill on the implementation of EC directives aimed at harmonising banking and securities supervisory provisions of 6 April 1997 (*Regierungsentwurf zur Umsetzung von EG-Richtlinien zur Harmonisierung bank- und wertpapieraufsichtlicher Vorschriften vom 6.4.1997*) (6th KWG Amendment), Bundestag document 13/7142, page 64.

and not of legal tender. They include value units having the function of private means of payment in barter transactions, as well as any other substitute currency used by virtue of private-law agreements as a means of payment in multilateral settlement accounts. This makes a central issuing party obsolete.<sup>43</sup> On the other hand, admissibility under monetary law, as referred to above, is irrelevant for the purposes of assessment as a unit of account and, as a result, as a financial instrument within the meaning of the German Banking Act.<sup>44</sup>

---

<sup>43</sup> See BaFinJournal January 2014, page 26 et seq.

<sup>44</sup> BaFin guidance notice, Information on financial instruments pursuant to section 1 (11) sentences 1 to 3 of the KWG (equities, investments, debt instruments, other rights, units in investment funds, money market instruments, foreign exchange, units of account and emissions certificates) (*Hinweise zu Finanzinstrumenten nach § 1 Abs. 11 Sätze 1 bis 3 KWG (Aktien, Vermögensanlagen, Schuldtitel, sonstige Rechte, Anteile an Investmentvermögen, Geldmarktinstrumente, Devisen, Rechnungseinheiten und Emissionszertifikate)*), [www.bafin.de/dok/7852552](http://www.bafin.de/dok/7852552), retrieved on 10 July 2018.

This means that, if the scenario involves other circumstances aside from use as means of payment or the mining of payment tokens, an authorisation requirement may be triggered – especially if a market is created on which these tokens are traded. The commercial re-conversion of Bitcoin into euros is subject to an authorisation requirement pursuant to section 32 (1) of the KWG as a matter of principle. This service is to be classified as a principal broking service (section 1 (1) sentence 2 no. 4 of the KWG) if the service provider takes the Bitcoins on commission in order to sell them to a third party on the market for the customer's account. In cases involving action taken in the name and for account of another party (*offene Stellvertretung*), which are unlikely to be practically relevant, the service would have to be classified as contract broking pursuant to section 1 (1a) sentence 2 no. 2 of the KWG. If the provisions governing the transaction are set out in a purchase agreement between the service provider and the customer, the transaction is to be classified as proprietary trading pursuant to section 1 (1a) sentence 2 no. 4 of the KWG. This often includes providers that





offer the direct conversion of common currencies into payment tokens as exchange traders, virtual bureaux de change or by BTC ATMs.

If payment tokens are not directly re-converted between the parties to the reconversion but include involving a third party (such as an Internet platform that functions as a conversion authority for virtual money into legal tender), this might also be subject to an authorisation requirement under section 10 (1) of the ZAG due to the provision of payment services. If, on behalf of the acquirer, the third party transfers the real equivalent value of the virtual currency to the conversion recipient via the third party's own account, the third party is conducting money remittance business (section 1 (1) sentence 2 no. 6, first alternative of the ZAG). If it acts on behalf of the payment recipient, it may, under certain circumstances, be conducting acquiring business within the meaning of section 1 (1) sentence 2 no. 5, second alternative of the ZAG. A combination of the two types of business is conceivable if the payment service provider acts on behalf of both parties to the

conversion (often the case with Internet platforms). The specific contractual agreements between the participating parties – as is always the case in assessing the authorisation requirement – are deciding factors. It may be difficult to delimit the types of business in some cases, particularly where business terms have not been set out in accordance with legal standards.<sup>45</sup>

Authorisation requirements pursuant to the German Banking Act then lead to classification as obliged entities pursuant to section 2 of the GwG which must meet, in particular, general due diligence requirements (section 10 of the GwG) and recording and retention obligations (section 8 of the GwG) and well as comply with internal safeguards (section 6 of the GwG) and report suspicious cases to the Financial Intelligence Unit (FIU) (section 43 of the GwG).

---

<sup>45</sup> See BaFinJournal January 2014, page 26 et seq., and [www.bafin.de/dok/8054452](http://www.bafin.de/dok/8054452).

## 4.1.2 Securities tokens

A large number of newer generation crypto tokens, particularly those issued in initial coin offerings (ICOs)/ token generating events (TGEs) represent an intrinsic asset for the owner of the associated private key (equity and investment tokens). This should not be a surprise as the option of digital transfer of assets without intermediaries is a core feature of a blockchain economy.

These may be regarded as securities within the meaning of section 2 (1) of the WpHG depending on the legal position that these tokens convey. Contrary to what the German word for securities, "*Wertpapiere*", suggests, the legal definition makes it clear that securities do not need to be on paper. It suffices if transactions can be documented in such a way on the basis of distributed ledger or blockchain technology that the rights embodied in the token can be clearly attributed to an address (not necessarily a name):

"Securities within the meaning of the German Securities Trading Act, whether or not represented by a certificate, are all categories of transferable securities with the exception of instruments of payment which are by their nature negotiable on the financial markets, in particular, shares in companies, other investments equivalent to shares in German or foreign legal persons, partnerships and other enterprises as well as depositary receipts representing shares, debt securities, [...]".

This definition transposes the term of securities pursuant to Article 4 (1) no. 44 of the Markets in Financial Instruments Directive (MiFID II)<sup>46</sup> into national law. On this basis, the following criteria must all be met for a token to be regarded as a security pursuant to section 2 (1) of the WpHG:

- transferability of the token
- negotiability of the token on the financial markets by its nature
- embodiment of membership participation rights or contractual rights in the token
- token not classified as a pure instrument of payment

For this document it is sufficient to continue with a description of the main aspects as, in its advisory letter dated 20 February 2018<sup>47</sup>, BaFin already informed the public in detail of these requirements:

In technical terms, token transferability e.g. requires that the token can be transferred to other users. In so doing, the token must be transferable "according to its type", i.e. its essential legal substance or technical nature must remain unchanged when transferred to a third party. Restrictions on the number of possible transfers and transfer only by certain privileged users are aspects that may disqualify generic transfer as a security.

A generic standardisation is decisive in token negotiability. If tokens embody specific rights that differ in each case, they may be transferable, but their negotiability, on the other hand, is not established. It must be possible to determine the type and quantity of tokens in transactions, i.e. they must be fungible. The tokens' capability of being held in custody is, in contrast, not a statutory requirement for their negotiability. Furthermore, negotiability must be given on financial markets. The possibility of negotiation is sufficient; actual negotiation is not required. As a rule, crypto token trading platforms organised on a centralised or decentralised basis are to be regarded as financial markets to this end.

The token must embody share-like membership rights or other property rights of a contractual nature that are sufficiently comparable to the examples of transferable securities listed in section 2 (1) of the WpHG, in particular bonds or debt instruments. It must be

---

46 Directive (EU) 2014/65, OJ L 173/349.

---

47 BaFin, Initial Coin Offerings: Advisory letter on the classification of tokens as financial instruments, [www.bafin.de/dok/10690958](http://www.bafin.de/dok/10690958), retrieved on 10 July 2018.

ensured, on a case-by-case basis, particularly with regard to the frequently hybrid nature of many tokens flagged as utility tokens, that the instrument in question is a financial instrument rather than an instrument largely attributable to the real economy. A predominant link to the real economy can be questionable, particularly in the case of tokens with which none of the goods or services promised can yet be purchased as they have yet to be developed. In such cases, whether or not the functionality promised in the token itself and associated materials such as whitepapers can be realised depends, among other things, on the efforts of the issuer. The token thereby primarily serves funding purposes, which may be an argument for regarding a certain token as a financial instrument, if the token also embodies rights comparable to securities. Again, it is the assessment of the individual case that is decisive.

The embodiment of membership rights is particularly deemed to be the case if the token conveys a form of participation in an enterprise organised as an association, showing a similarity to a share.<sup>48</sup> Constructions similar to depositary receipts that only confer the right to exercise membership rights may embody membership rights as well.

Embodiment of property rights is deemed to exist if the legal positions linked to the token are similar to a debt instrument, in that there are e.g. contractual claims against the token issuer or a third party. However, for this to be the case, it is necessary that, as a rule, the contractual claim be linked to the token and be only transferable along with it.

The token may not be classified as a pure instrument of payment. Instruments of payment include in particular means of payment such as cash, book money and electronic money, as well as other instruments intended to initiate a payment process.<sup>49</sup> If a token does not meet the requirements of an instrument of payment, it is excluded, as a purely electronic means of payment, from

the definition of securities in the WpHG. In such cases, the above-mentioned classification as a unit of account in accordance with section 1 (11) sentence 1 no. 7 of the KWG applies.

A token that is to be classified as a security also falls under the scope of the capital market law requirements for securities. Potential prospectus obligations pursuant to section 3 (1) of the German Securities Prospectus Act (*Wertpapierprospektgesetz – WpPG*) or Article 3 (1) of the Prospectus Regulation<sup>50</sup> in the case of a public offer, applicability of the organisation requirements and rules of conduct<sup>51</sup> as well as the possibility of product intervention pursuant to the WpHG<sup>52</sup> are of note here. Furthermore, the regulations on trading obligations and market supervision pursuant to the MiFIR<sup>53</sup> would have to be observed, as would the regulations prohibiting market manipulation and insider trading, and on ad hoc obligations for issuers and obligations for financial analyses pursuant to the market abuse regulation (MAR), if the additional requirements under Article 2 of the MAR have been met; that is, if the securities are traded, in particular, on a regulated market, or in a multilateral or organised trading system. This would be the case, if a crypto currency exchange e.g. were admitted as a multilateral trading facility (MTF) or an organised trading facility (OTF) within the scope of the regulation. Not least, business transacted in securities that is of a commercial nature or scale, which requires commercially organised business operations is subject to authorisation requirements of the German Banking Act and thus also fall under the definition of an obliged entity in accordance with section 2 of the GwG.

### 4.1.3 Utility tokens

With respect to pure utility tokens (app tokens, product use tokens, consumption tokens), the focus is on the sole use for purchasing real-economy goods or services

---

48 Roth, in: Hirte/Möllers, *Kölner Kommentar zum WpHG*, second edition 2014, section 2 marginal note 48.

49 BaFin, Guidance notice on financial instruments, loc. cit. (footnote 47).

---

50 Regulation (EU) No 2017/1129, OJ L 168/12.

51 For the rules of conduct and other references, see BaFinJournal May 2018, page 18 *et seq.*

52 [www.bafin.de/dok/10334186](http://www.bafin.de/dok/10334186).

53 Regulation (EU) No 600/2014, OJ L 173/84.



© iStock/From2015

and not on a financial consideration. Utility tokens are not e-money if there is no third-party acceptance or they are only issued in exchange for other payment tokens (such as Bitcoin or Ether). With respect to pure usage tokens, there is also much to suggest that their issue does not induce any authorisation requirements under the Banking Act, the Payment Services Supervision Act or the Investment Code. Moreover, the possibility of classifying such tokens as a financial instruments pursuant to the Banking Act is also often ruled out, meaning that any trade-based services performed exclusively with these tokens on the secondary market do not require authorisation.

In contrast to virtual currencies, pure product use tokens are not designed as means of payment and thus do not qualify as units of account either; as a general rule, they also do not fall under the concept of other financial instruments pursuant to section 1 (11) of the KWG. However, because of the many hybrid forms, tokens that display elements of both product use tokens and of a virtual currency or securities tokens often require a more in-depth assessment.

If the issuer's offer describes the supposed utility token as also functioning as a means of payment, the token may well be considered to be a unit of account and thus a financial instrument pursuant to the Banking Act. From a supervisory point of view, the utility token category includes tokens that cannot be allocated to the payment token or securities token categories, which give rise to obligations under supervisory law.

#### 4.1.4 Initial Coin Offerings

ICOs are to be distinguished from initial public offerings (IPOs) both economically as well as organisationally<sup>54</sup>. ICOs are also referred to, in some cases, as token generating events (TGEs). Tokens are sold or auctioned in an ICO. The main idea of ICOs is to raise funds from third parties for an idea or a business model. ICOs frequently include a white paper, intended to give an overview of the planned project, but it is often not equal to the

---

<sup>54</sup> Conley, Blockchain and the Economics of Crypto-tokens and Initial Coin Offerings, <http://www.accessecon.com/Pubs/VUECON/VUECON-17-00008.pdf>, retrieved on 10 July 2018.

structure, comparability and informational significance of prospectuses pursuant to the Securities Prospectus Act. Further contact with the issuers is then frequently made using a variety of online channels such as the website, Telegram and Slack. In terms of technology, many ICOs use smart contracts from Ethereum, the second largest blockchain after Bitcoin in terms of market capitalisation. The tokens auctioned or sold in the ICO are managed via the smart contracts.

Economically, there are significant differences between raising capital by means of conventional equity- or debt-based funding instruments and an ideal type of ICO that includes the elements of the blockchain economy explained in this document. Crypto tokens can directly represent the value of decentralised networks determined by means of contributions by third parties, whereas conventional equity investments initially represent the value of the initiating company and only indirectly the value of the decentralised network initiated (but not necessarily operated) by it. From a certain point on, networks organised on a decentralised basis depend on the efforts of the participating community and less on those of the initiator.<sup>55</sup> ICOs also give private investors access to investment opportunities similar to venture capital in that they are more liquid but also involve greater risk. At the end of the day, ICOs can use smart contracts to optimise transaction costs. This can be accomplished by means of automated, non-discretionary, decentralised and easy cross-border settlement of contractual agreements. The disintermediation impact of blockchain technology – as the basis of ICOs – further reduces the concentration effects in intermediary-based platform economies and creates competitive pressure on these established intermediaries.<sup>56</sup>

In supervisory terms, a distinction is to be made between the initial token issue, i.e. the actual ICO, and

subsequent trading with tokens on the secondary market. The supervisory classification of the token has an impact on potential obligations at issuance (e.g. prospectus obligation) as well as potential obligations for third parties participating in the issue and in secondary market trading. The authorisation requirements explained above have to be pointed out in particular, especially for secondary market business, such as operating crypto exchanges, or business at the interface to real money. One example here is the operation of exchange machines, because operating businesses like this in Germany without prior authorisation is also a criminal offence. In contrast, for the self-issuance of an ICO, the legal nature of the tokens issued is not decisive as supervisory law grants a broad issuer privilege; real economy companies issuing their own financing instruments do not normally require authorisation requirement under the Banking Act.

ICOs are to be distinguished from another frequent manifestation, the airdrop. In an airdrop, a blockchain project distributes free tokens. Those who want to receive free tokens in an airdrop normally have to hold tokens in the relevant blockchain project. However, likes or retweets are often also demanded in exchange for distribution of airdrop tokens. In general, airdrop tokens are not distinguishable from regular tokens and can be freely traded. The aim of airdrops is to increase awareness, trading volume and in the long term the value of the related crypto token.

In BaFin's opinion, ICOs are highly speculative investments. Investors should expect high volatility and consider the possibility of a total loss of their investment, particularly in early experimental projects. When investors buy tokens in an ICO, the issuers are not usually located in Germany. In such cases, German consumer protection and protection of personal data do not apply. White paper documentation is generally insufficient and confusing and does not meet the same standard of information as that of prospectuses drawn up in accordance with the Securities Prospectus Act. The ability to assess ICO risks requires an in-depth, particularly technical, understanding of the subject matter. ICOs are often held in the non-regulated area of the financial sector and take advantage of jurisdictions

---

<sup>55</sup> This requires, however, that the network already be operational and that it is not only a promise by the issuer.

<sup>56</sup> Klöhn/Parhofer/Resas, Initial Coin Offerings (ICOs) – Markt, Ökonomik und Regulierung, in: Zeitschrift für Bankrecht und Bankwirtschaft 2018, 89 et seq., 93 et seq. and further references

with more lax regulation. Moreover, the structure of ICOs makes them highly vulnerable to abuse and fraud.<sup>57</sup>

In order to address this risk situation, BaFin published a consumer warning<sup>58</sup> and an accompanying article in BaFinJournal<sup>59</sup> on 9 November 2017. Moreover, reports on losses in the context of ICOs also increased and there were strong indications of the market overheating. Warnings were even to be heard from the crypto scene itself. BaFin was also aware of findings on technical deficiencies of individual ICO concepts.

The primary or main risks directly related<sup>60</sup> to crypto tokens comprise in particular 1) market liquidity and volatility risks, 2) counterparty and project risks as well as 3) technical and operational risks (including cybersecurity risks). These main risks relate to specific features of crypto tokens and their current use as well as to known microfinancial risks in connection with market liquidity, volatility, leverage, etc.<sup>61</sup>

- Market liquidity and volatility risks: in respect of crypto tokens, it should be noted in particular that illiquid or flat market structures impair the ability to sell or purchase crypto tokens without impacting the price. The high volatility of market prices also raises doubt that crypto tokens are suitable for private investors or can be used for payment and settlement. Trading volume, prices, price volatility, number of users, bid/ask spreads, price spreads between exchanges and the costs of concluding transactions provide information on specific risks.
- Counterparty and project risks: The project risk of crypto tokens generated in ICOs and the projects

financed with them could impact the positions of the crypto token owners (investors), as, in many projects, the value and stability of the crypto tokens largely depends on the project team behind the crypto tokens or the ICO. The project underlying an ICO e.g. might not be realised, which would ultimately make the crypto tokens worthless. This risk class is relevant, particularly in the context of ICOs, as the total size of the ICO market is currently still small compared to the overall crypto token market. There is, moreover, a counterparty risk for crypto token owners that arises from crypto token brokers, crypto trading platforms, wallet providers and other intermediaries.

- Technical and operational risks (including cybersecurity risks): blockchain technology will be able to offer a number of advantages in the future. However, crypto tokens – especially those that are part of decentralised projects and that consequently work with governance structures of limited effectiveness – also carry technical and operational risks. These include vulnerability to theft and fraud. Cyberattacks, transaction finality, poor scalability and long delays may also pose operational risks. Such risks, particularly the disproportionately high dependency on functioning IT infrastructures, also exist for service providers and crypto token trading platforms.

The above analysis demonstrates that, depending on their structure in the respective case, not all tokens are subject to capital market regulation in a manner that addresses these risks as it does those of conventional capital market instruments. For this reason, indicators and transmission channels of these risks into the financial system must be monitored, in the interests of both private and institutional investors, but also in terms of financial stability and integrity.<sup>62</sup>

---

57 Marktwächter Finance section press release, Neue Kryptowährungen sind hochriskante Geldanlagen, <http://ssl.marktwaechter.de/pressemeldung/neue-kryptowaehrungen-sind-hochriskante-geldanlagen>, retrieved on 3 July 2018.

58 [www.bafin.de/dok/10185906](http://www.bafin.de/dok/10185906).

59 See BaFinJournal November 2017, page 15.

60 Of no further note here are the indirect risks of leverage that arise from using crypto tokens as an underlying for derivatives or from purchasing crypto tokens via debt financing such as loans.

61 For risks that arise specifically from the situation in an ICO, please see the detailed explanation in Klöhn/Parhofer/Resas loc. cit. (footnote 62), page 95 *et seq.*

---

62 FSB, FSB report sets out framework to monitor crypto-asset markets, retrieved on 27 July 2018.



# 5 Conclusion

The crypto token market as a whole shows high innovation speed, strong information asymmetries and gaps in data availability. This means that national supervisory authorities such as BaFin, as well as European supervisory authorities and international standard setters, must continue to work intensively in this area and keep abreast of developments.

At the time of writing, more than 1,600 crypto tokens are currently traded on marketplaces, with the lion's share of the transaction volume in only five of these crypto tokens. Crypto token prices have significantly declined since the end of 2017, which has resulted in a considerable decline in market capitalisation. Prices at the end of June 2018 were just under one third of the high recorded in January 2018. At the same time, however, there has been a considerable increase in the number and volume of ICOs. Extrapolating the first

half-year figures for the whole of 2018 yields an ICO volume almost six times higher than in 2017 (USD 3.9 billion), and extrapolating the first half-year figures to the whole year 2018 for the number of ICOs results in nearly five times as many ICOs for 2018 than occurred in 2017 (210 ICOs). Worldwide, 489 ICOs raised more than USD 11 billion in the first half of 2018 alone.<sup>63</sup> Crypto token markets are still small in relation to the global financial system and thus do not yet adversely impact financial stability.<sup>64</sup>

Given the growth rate, one can indeed speak of hype about ICOs and the crypto tokens they create.

---

<sup>63</sup> CoinSchedule, Cryptocurrency ICO Stats 2018, <http://www.coinschedule.com/stats.html>, retrieved on 25 June 2018.

<sup>64</sup> FSB, loc. cit. (footnote 62).

However, it is to be expected that the crypto token and ICO phenomena as such will continue even after a cooling-off of the current frenzy, as, in addition to the advantages described above, ICOs may in the foreseeable future become an important source of funding, particularly in the early-stage financing of young businesses.<sup>65</sup>

Moreover, connections to the traditional financial sector have been limited thus far. Despite the launch of crypto token futures, the volume of financial institutions' trading and positions still remain small compared to their investments in markets for other asset classes.

The crypto token area continues to experience rapid development in qualitative terms as well. Some market participants e.g. have signalled an interest in the launch of crypto token exchange traded funds (ETFs) that have the potential of quickly elevating crypto token risk for private clients by lowering the technological barriers for directly holding crypto tokens.

Despite the numerous questions that remain, the more attention academics, politicians, international standard setters and supervisory authorities pay to this topic, the more legal security it will bring to the market. Moreover, the stated positive effects of individual manifestations such as ICOs should not be underestimated in spite of all the risks.

The low significance of this market for financial stability attributed at this time can thus not be seen as a final conclusion.<sup>66</sup> With respect to regulatory and supervisory assessment of all aspects of the blockchain economy, it is not an unregulated Wild West scenario, particularly in Germany – but there is no fully established supervisory and regulatory landscape either.

Risk-adequate and technology-neutral regulation comes at a price: introducing new business models will become more time-consuming as a result. Individual investor interest in achieving a return on investment as quickly and easily as possible, and issuer interest in raising funds from third parties to use for its own commercial purposes<sup>67</sup> must, for BaFin, however, always be reconciled with the overarching goal in the interest of the general public of maintaining a financial market that displays integrity and inspires confidence. This enables sustainable, well-conceived and therefore trustworthy financial innovations to prevail and, ultimately, for each to pay off. Despite the undisputed difficulties from clarifying supervisory issues prior to the market launch of a business model, this fundamental regulatory concept has proved successful in principle over the past few decades, also for financial innovations of the past. Individual case detail aside, the strategic consideration of the manifold applications of blockchain technology, such as tokens, also ensures that unnecessary or obsolete regulatory constraints can be addressed from the perspective of all public and private interests.

Further progress in this area can be expected to be achieved through the strengthening of legal certainty by means of continued market information and a targeted, internationally coordinated analysis of potential regulatory deficits.

---

65 Weitnauer, Initial Coin Offerings, rechtliche Rahmenbedingungen und regulatorische Grenzen, in: Bank- und Kapitalmarktrecht 6/2018, page 231 et seq.; 236; Zickgraf, Initial Coin Offerings – Ein Fall für das Kapitalmarktrecht?, in: Die Aktiengesellschaft 2018, page 293 et seq., 307.

66 See Financial Stability Committee, Fifth report to the German Bundestag, June 2018, page 42.

---

67 No case has yet come to light of an ICO in which the initiators' interest in making a profit has not played a role. Particularly in the context of blockchain technology, this fact is often turned around in marketing-oriented statements addressed to policy makers and investors to explain that investing in an ICO serves a greater good such as the establishment of decentralised platforms without intermediaries. It is indeed a feature of the blockchain economy that it does not need any intermediaries or centralised control of the platform to earn a profit, if you merely retain enough of the tokens initially created for free, with the expectation of a later increase in value.

# W

In a globalised financial world in which more and more people pay digitally, transfer money and make their investments online, IT governance and information security now have the same significance for supervisors as ensuring that companies have adequate capital and liquidity. It was therefore a logical step for BaFin to expand on its requirements in this area.

# Digitalisation and Information Security in the Financial and Insurance Sectors as a Focus of Regulatory Requirements

Author

**Dr Jens Gampe,**

Division for Policy Issues relating to IT  
Supervision and Inspections, Federal Financial  
Supervisory Authority (BaFin)

## 1 Introduction

In the financial world, information technology (IT) is now no longer merely an secondary requirement for generating income: it has become – and this also makes it vulnerable – the core infrastructure both for all banking processes and for all non-banking processes. BaFin President Felix Hufeld made precisely this point at the BaFin conference “IT Supervision in the Banking Sector” on 16 March 2017.<sup>1</sup> IT security is also a socially relevant issue.

Both aspects – IT as the basis for economic activity along all value chains in the financial sector and the reminder that no sustainable and socially acceptable business is possible without information security<sup>2</sup> – were the critical factors in BaFin’s decision to develop the ‘Supervisory Requirements for IT in Financial

Institutions’ (*Bankaufsichtliche Anforderungen an die IT – BAIT*) together with the Deutsche Bundesbank and in consultation with representatives of the credit institutions and their associations. BaFin published the BAIT<sup>3</sup> on 6 November 2017. The ‘Supervisory Requirements for IT in the Insurance Sector’ (*Versicherungsaufsichtliche Anforderungen an die IT – VAIT*<sup>4</sup>), which were published by BaFin on 2 July 2018, establish similar requirements for the insurance industry.

The BAIT and the VAIT are principle-based and proportionally designed rulebooks whose purpose is to expand on and make more transparent BaFin’s previously more generally formulated requirements addressing IT.

---

1 [www.bafin.de/dok/9045758](http://www.bafin.de/dok/9045758).

2 DTCC & Oliver Wyman, Large-scale cyber-attacks on the financial system – A case for better coordinated response and recovery strategies, <http://www.oliverwyman.com/our-expertise/insights/2018/mar/large-scale-cyber-attacks-on-the-financial-system.html>.

---

3 Circular 10/2017 (BA) – Supervisory Requirements for IT in Financial Institutions (BAIT).

4 Circular 10/2018 (VA) – Supervisory Requirements for IT in the Insurance Sector (VAIT).

## 2 Changing IT requirements in the financial sector

At banks, the value chain has always essentially been focused on processing information, so digitalisation is nothing new for the institutions. In the past, however, the digitalisation of banking transactions mainly happened inside institutions and for a long time out of sight for most customers – despite its importance, especially for payment transactions.

The first online banking offerings (e.g. BTX<sup>5</sup>) for customers already appeared more than 30 years ago. But it is only in the past 10 to 15 years that cashless payments – including as part of the increasingly popular online banking services – and online brokerage have become established in the retail banking business. Competitive direct banks and the first app-based fully digitalised institutions have ushered in the next technical evolutionary stage in customer interaction.

But digitalisation in banking also means supporting and automating business and IT processes with the help of relevant data and suitable IT systems (hardware and software components) – across all customer channels, the entire information chain in the enterprise and across defined interfaces with third parties.<sup>6</sup> It is particularly important in this context for business processes, which in many cases also extend across several business units, to be intelligently networked. Nor should the increasingly in-depth interaction with companies that provide – to a greater or lesser extent – external IT services for the institutions be forgotten.

Supervisory monitoring and inspection practice reveals that many banks still have problems finding technically rational solutions for linking together multiple – or heterogeneous – digitalised business processes. However, this is crucial for digitalisation, which is supposed to provide targeted support for the business. It is not enough just to digitalise individual processes or introduce digital business models in some areas only.

Technological progress demands a much stronger focus on innovation and permanent adaptation to dynamically changing customer behaviour.<sup>7</sup>

In addition to the ubiquitous and growing information and cybersecurity risks, digitalisation also entails strategic risks for banks and their IT service providers because it changes the value chains in the financial services sector.<sup>8</sup> Various trends are now emerging in the digitalisation of the banking sector.<sup>9</sup>

Some of these technological developments (and enhancements) are outlined in the following:

### **Digitalisation initiatives at the customer interface**

Although online banking offerings were developed at an early stage in traditional branch-based banks, they were mostly implemented with at most lukewarm support because the primary focus was on customer footfall in the branches. The quality of digital services has certainly increased considerably in the meantime, but in many cases they are still poorly coordinated with the traditional branch business, even though most customers now expect to be offered services across all distribution channels.<sup>10</sup>

Direct banks, fintechs<sup>11</sup> and crowdfunding platforms, which often only offer a specific slice of the banking

---

5 Abbreviation for a German videotex service.

6 Röseler, Banking wird sich ganz radikal ändern, Treiber des Wandels ist die Digitalisierung (Banking will see radical change and the driver of change is digitalisation), in: Zeitschrift für das gesamte Kreditwesen, no. 7/2018, page 25 et seq.

---

7 COREtransform: White Paper – Primat des Technologischen – Regulatorik im Spannungsfeld zwischen Gestalten und Verwalten (White Paper – Primacy of technology – The tension between designing and managing regulatory activities), <https://transform.core.se/de/about/insights/knowledge-work/white-paper/>.

8 BaFin, Big Data meets artificial intelligence – Challenges and implications for the supervision and regulation of financial services), pages 7 et seq. and 62 et seq., [www.bafin.de/dok/11250046](http://www.bafin.de/dok/11250046).

9 Deutsche Bank Research, Fintech reloaded – Traditional banks as digital ecosystems, [http://www.dbresearch.de/PROD/RPS\\_EN-PROD/PROD0000000000451937/Fintech\\_reloaded\\_%E2%80%933\\_Traditional\\_banks\\_as\\_digital\\_ec.PDF](http://www.dbresearch.de/PROD/RPS_EN-PROD/PROD0000000000451937/Fintech_reloaded_%E2%80%933_Traditional_banks_as_digital_ec.PDF).

10 Stollarz, Digitalisierung in der Finanzbranche ist kein Selbstzweck (Digitalisation in the financial sector is not an end in itself), in: Börsen-Zeitung online, 28 April 2018, page B5.

11 There is currently no generally accepted definition of the term „fintech“. As a combination of the words *financial services* and *technology*, fintechs are generally understood to be start-ups that offer specialised and particularly customer-centric financial services based on technology-driven systems.



business, have been rushing into this gap for several years now. The increasing popularity of these innovative providers has massively ramped up competitive and investment pressure on established players in the banking sector.<sup>12</sup> If they want to hold their ground in this environment, they must do more than just invest in technology – for example in implementing mobile apps and omnichannel platforms. Rather, the banks must also quickly adapt their operational structures and governance mechanisms to the new developments.

### **Process digitalisation**

The growing maturity of digital technologies is seeing the emergence of new possibilities to further automate processes that are currently only partially

automated – for instance in the lending business (e.g. “credit factory”) and everything to do with account opening (e.g. the “VideoIdent” online identity verification solution).

However, established banks will only be able to compete with new digital competitors in the online business if they also more heavily automate adjacent back-end processes and hence significantly improve their cost structures. Nor is it enough just to develop new solutions for process digitalisation. Those solutions must be integrated swiftly and effectively into the value and process chains – inside the institution and across institutions.

A further factor is that in many places, they have to deal with outdated and/or overly complex IT systems. Many institutions also have significant deficits in their IT governance, as supervisors have established. In many cases, governance-related requirements are not

---

<sup>12</sup> Deutsche Bank Research, Start-ups beflügeln Märkte mit digitalen Technologien (Start-ups inspire markets with digital technologies) (Fintech #7), [https://www.dbresearch.de/PROD/RPS\\_DE-PROD/PROD000000000447700/Start-ups\\_beff%C3%BCgeln\\_M%C3%A4rkte\\_mit\\_digitalen\\_Technolog.PDF](https://www.dbresearch.de/PROD/RPS_DE-PROD/PROD000000000447700/Start-ups_beff%C3%BCgeln_M%C3%A4rkte_mit_digitalen_Technolog.PDF), retrieved on 11 May 2018.

effectively implemented and their operationalisation is not adequately monitored.<sup>13</sup>

### **New dynamics in IT projects**

What customers expect from banks when it comes to the use of modern technologies also applies increasingly to the IT project organization and the software development process implemented in this connection at the institutions and their IT service providers: they must be fast, lean and adaptable at short notice – in short: agile.

More than 35 per cent of banks now say that they use Scrum to organise their IT development projects, while about 30 per cent rely on Kanban.<sup>14</sup> Both of these agile software development approaches offer an opportunity to significantly change software components in the development process. For example, an operational basic version of an application can already be available at most in a few weeks, rather than months.

Despite all the buzz about innovative software development, however, it pays to remember that a crucial condition for secure IT operation is that – in addition to suitable, functional hardware – there is also a need for software that has been developed, as far as possible, in such a way that security measures augment the conventional software development process. As a general rule, this is the only way to ensure that sufficient attention is paid to security, regardless of whether an agile or another approach is chosen for development.<sup>15</sup> A condition for this, however, is that security is integrated as an explicit requirement in the development process (“security by design”), and that holistic security

measures are incorporated, implemented, tested and approved by the relevant functions, starting with initialisation and before the system goes live.

### **Say goodbye to your own data centre – Is the cloud “as a service” a solution?**

More than 50 per cent of the companies surveyed in the financial sector say they are already working on streamlining their data centres and consolidating their IT infrastructure.<sup>16</sup> This is also being made possible by the increased use of external cloud services, to which applications, platforms as well as security solutions, for example, are being redeployed. Especially with “as a service” concepts<sup>17</sup>, companies can both standardise and accelerate their IT architecture.<sup>18</sup> However, redeploying the processing of what may include highly sensitive data to the cloud also involves a considerable security risk, both to the security of the cloud’s (i.e. the cloud operator’s) IT systems and to the security of the data to be processed or stored in the cloud (i.e. the cloud user’s data).<sup>19</sup>

---

13 See Chapter 6.4., Governance – II.2. BAIT

14 IT Finanzmagazin, 70 Prozent der Banken und Versicherer entwickeln mit agilen IT-Methoden wie Scrum oder Kanban (70 per cent of banks and insurers use agile IT methodologies such as Scrum or Kanban), <https://www.it-finanzmagazin.de/70-prozent-der-banken-und-versicherer-entwickeln-mit-agilen-it-methoden-wie-scrum-oder-kanban-35438>, retrieved on 11 May 2018.

15 Schild, Heise Online – Sichere Softwareentwicklung nach dem „Security by Design“-Prinzip (Secure software development using the “security by design” principle), <https://www.heise.de/developer/artikel/Sichere-Softwareentwicklung-nach-dem-Security-by-Design-Prinzip-403663.html>, retrieved on 11 May 2018.

---

16 Bain & Company, Mehr Tempo, weniger Altlasten: IT-Architektur im digitalen Zeitalter (More speed, fewer legacies: IT architecture in the digital age), <http://www.bain.de/en/publikationen/articles/it-architektur-im-digitalen-zeitalter.aspx>.

17 Alongside Software as a Service (SaaS) and Platform as a Service (PaaS), Infrastructure as a Service (IaaS) is one of the three service models in cloud computing. The service generally includes the provision of data centre infrastructure by a cloud provider. The resources are accessed through private or public networks. Examples of components of the infrastructure provided under IaaS include servers, computing and network capacity, communication devices such as routers, switches or firewalls, storage space as well as data backup and archiving systems.

18 IT Finanzmagazin, Studie zur IT-Architektur: Banken & Versicherer haben wachsende technologische Defizite (IT Architecture Study: Banks & insurers have growing technology deficits), <https://www.it-finanzmagazin.de/bain-studie-zur-it-architektur-banken-versicherer-haben-wachsende-technologische-defizite-45983>, retrieved on 11 May 2018.

19 com! Professional, Sicherheit in der Cloud funktioniert anders (Security in the Cloud works differently), <https://com-magazin.de/praxis/cloud/sicherheit-in-cloud-funktioniert-1469946.html>, retrieved on 11 May 2018.

# 3 Fundamental international supervisory requirements for IT

Financial market supervisors already addressed the requirements for IT infrastructure at an early stage, focusing initially on governance requirements in particular. In its 2010 report<sup>20</sup>, the Senior Supervisors Group, which reports to the Financial Stability Board (FSB) and represents the supervisory authorities of the ten countries that supervise the world's largest banks, emphasised the importance of strong IT governance and defined what is a core requirement from BaFin's point of view: the IT strategy must be a pivotal part of the business strategy. In this respect, BaFin expects the necessary requirements for digital transformation to be based on business policy principles and anchored strategically, since the IT architecture can only be strategically enhanced using a holistic, enterprise-wide approach.

Many IT regulatory requirements have arisen in the recent past, among other things because banks' internal processes running on their technical systems were or are not (yet) sufficiently integrated and automated. Examples of these include data aggregation and reporting processes that are relevant for managing a bank (key requirements here are to be found in BCBS 239<sup>21</sup>, which were implemented in the latest revision of the German Minimum Requirements for Risk Management (*Mindestanforderungen an das Risikomanagement* – MaRisk)).

Industry and supervisors are also increasingly becoming aware of another aspect in the wake of digitalisation, namely information security and cybersecurity<sup>22</sup> (see info box "Definition of information security and cybersecurity").

## Definition of

### Information security and cybersecurity

- Information security includes greater protection of information, in and with IT, but also without and beyond IT.<sup>23</sup>
- Cybersecurity deals with all aspects of security in information and communication technology. The scope of classical IT security is expanded to include the entire cyberspace, which covers all information technology relating to the Internet and comparable networks and includes communication based on them, applications, processes and processed information.<sup>24</sup>

20 Senior Supervisory Group, Observations on Developments in Risk Appetite Frameworks and IT Infrastructure, <https://www.newyorkfed.org/medialibrary/media/newsevents/news/banking/2010/an101223.pdf>, retrieved on 11 May 2018.

21 Basel Committee on Banking Supervision, Principles for effective risk data aggregation and risk reporting.

22 Steffens, Hacker-Jagd im Cyberspace – Grundlagen und Grenzen der Suche nach den Tätern (Hunting hackers in cyberspace – Principles and limitations of the search for the culprits) in: c't 14/2017, page 122.

23 See BSI Standard 200-2, page 12.

24 BSI, [https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/cyber-sicherheit\\_node.html](https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/cyber-sicherheit_node.html), retrieved on 30 July 2018.



Beyond the realm of information security, cybersecurity also has a political dimension because in many cases it proves to be extremely difficult to identify the real attackers after a cyberattack so that effective measures can then be taken against them.<sup>25</sup>

Because of the overriding importance of cybersecurity for the financial sector, the G7 Cyber Expert Group presented a report on the fundamental elements for effective assessment of cybersecurity in the sector, which

was adopted by the G7 finance ministers and central bank governors on 12 October 2017.<sup>26</sup> BaFin is currently examining the extent to which the BAIT need to be adapted or expanded in order to meet the requirements of the G7 report, such as requirements for contingency management<sup>27</sup> and corresponding exercises.

---

25 Geiß, Völkerrecht im „Cyberwar“ (International law in “Cyberwar”), <http://www.ipg-journal.de/schwerpunkt-des-monats/neue-high-tech-kriege/artikel/detail/voelkerrecht-im-cyberwar-859/>, retrieved on 11 May 2018.

---

26 See Federal Ministry of Finance: [https://www.bundesfinanzministerium.de/Content/EN/Standardartikel/Topics/Financial\\_markets/Articles/2017-10-27-Cyber-Security-download.pdf?\\_\\_blob=publicationFile&v=2](https://www.bundesfinanzministerium.de/Content/EN/Standardartikel/Topics/Financial_markets/Articles/2017-10-27-Cyber-Security-download.pdf?__blob=publicationFile&v=2).

27 Lawrence, Cybersimulation: Der Teufel, den man kennt (Cybersimulation: The devil you know), in: Herbert Frommes Versicherungsmonitor, <https://versicherungsmonitor.de/2018/05/03/cybersimulation-der-teufel-den-man-kennt/>, retrieved on 11 May 2018.



# 4 IT-related regulation by the EBA

Because digitalisation is not a national issue, it is essential to develop a Europe-wide common understanding and consistent regulatory requirements on the topic. The European Banking Authority (EBA), in which BaFin is also represented at various levels, is responsible for harmonising supervisory practice in the European Union (EU).

The EBA published guidelines on the SREP (Supervisory Review and Evaluation Process) on 7 July 2014.<sup>28</sup> The SREP includes an assessment of key indicators, the business model, governance and capital and liquidity risks. The EBA defined the term “IT risk” for the first time in its SREP Guidelines (see info box “Definition of IT risk”).

## Definition of

### IT risk

According to the EBA SREP Guidelines [GL/2014/13], information and communication technology (ICT) risk means “[...] the current or prospective risk of losses due to the inappropriateness or failure of the hardware and software of technical infrastructures, which can compromise the availability, integrity, accessibility and security of such infrastructures and of data.”<sup>29</sup>

In order to validate and assess IT risk within the SREP even more precisely, the EBA issued additional guidelines<sup>30</sup> to supplement and further specify the assessment of ICT risk on 11 May 2017. In addition to the general SREP, it has developed an ICT SREP for significant institutions (SIs) and one for less significant institutions (LSIs).

Paragraph 5 of the May 2017 ICT SREP Guidelines aims to ensure the convergence of supervisory practices in the assessment of ICT risk under the SREP. The Guidelines contain assessment criteria that the competent authorities should apply to the supervisory assessment of institutions’ ICT governance and strategy and to the supervisory assessment of their ICT risk exposures and controls.

In addition, the supervisory authorities must assess whether the institution’s general governance and internal control framework duly cover the ICT systems and related risks and if the management body adequately addresses and manages these aspects, as ICT is integral to the proper functioning of an institution. In particular, the supervisory authorities must assess

- whether the institution has an ICT strategy that is adequately governed and in line with the institution’s business strategy,
- whether the institution’s internal governance arrangements are adequate in relation to the institution’s ICT systems,
- and whether the institution’s risk management and internal control framework adequately safeguards the institution’s ICT systems.

On the basis of Title 5 of the July 2014 EBA SREP Guidelines, supervisors should also assess whether the institution has an appropriate and transparent corporate structure that is “fit for purpose”, and has implemented appropriate governance arrangements. With regard to the ICT systems and in line with the EBA Guidelines on Internal Governance<sup>31</sup>, they should assess whether the institution has a robust and transparent organisational structure that clearly defines responsibilities for ICT. This also applies to the management body and its committees. They must also assess whether key persons

<sup>28</sup> EBA Guidelines EBA/GL/2014/13.

<sup>29</sup> EBA Guidelines EBA/GL/2014/13, loc. cit., page 17.

<sup>30</sup> EBA Guidelines EBA/GL/2017/05. The abbreviation “ICT” stands for information and communication technology.

<sup>31</sup> EBA Guidelines EBA/GL/44.

responsible for ICT, such as the Chief Information Officer (CIO) and the Chief Operating Officer (COO), have adequate direct or indirect access to the management body. This aims to ensure that the management body also knows and addresses the risks associated with ICT.

As the importance of IT outsourcing for business performance continues to grow, but also in light of the associated security risks, the Guidelines require the supervisory authorities to assess whether the institution's ICT outsourcing policy and strategy considers the impact of ICT outsourcing on the institution's business and business model.



© iStock/from2015

# 5 Supervisory requirements for the IT of institutions with a German banking licence

In Germany, too, IT supervision has increasingly moved into the focus of supervisory activities. As far back as 2012, BaFin established an “IT infrastructure of banks” division. In early 2018, it established the “IT Supervision/ Payment Transactions/Cybersecurity” group, with which that division was merged. Among other things, this group is responsible for policy issues relating to cybersecurity, supervision of payment and electronic money institutions, IT-related inspections and policy issues relating to IT supervision. Since then, IT supervision has been implemented on a cross-sectoral basis, and is described in the following using the example of the German Banking Act (*Kreditwesengesetz* – KWG):

The general principle for the supervision of institutions in section 6 (2) of the KWG reads: “BaFin shall counteract undesirable developments in the lending and financial services sector which may endanger the safety of the assets entrusted to the institutions, impair the proper conduct of banking business or provision of financial services or entail major disadvantages for the economy as a whole.”

BaFin interprets this as meaning that the “assets entrusted to the institutions” today are generally data that are processed and stored in IT systems. Impairment of the proper conduct of banking business or provision of financial services can therefore always be assumed if, as a minimum,

- the availability of IT systems is inadequate, i.e. if the IT systems are not operational as intended and data is not processed correctly,
- data integrity cannot be fully guaranteed, i.e. if the correctness of the data (data integrity) and/or the correct functioning of the IT system (system integrity) cannot be assured, or
- confidentiality cannot be assured, i.e. if the data to be protected can be manipulated without authorisation and without being detected.

BaFin’s general responsibilities under section 6 of the German Banking Act are specified in greater detail in section 25a (1) (see info box).

In the BAIT, BaFin has specified its understanding of a proper business organisation as it affects IT.

## Information

### Section 25a (1) of the German Banking Act (KWG)

This section sets out that “an institution shall have in place a proper business organisation which ensures compliance with the legal provisions to be observed by the institution as well as business requirements. The management board is responsible for ensuring the institution’s proper business organisation; it shall take the necessary measures to formulate the applicable internal guidelines except where such decisions are taken by the supervisory

body. A proper business organisation shall comprise, in particular, appropriate and effective risk management, [...]; risk management shall comprise, in particular, [...]

4. adequate staffing and technical and organisational resources;
5. the definition of an adequate contingency plan, especially for IT systems, [...] .”

# 6 Interpretation of supervisory requirements by the BAIT

## General comments

Like the MaRisk<sup>32</sup>, which were revised at the end of October 2017, the BAIT represent an interpretation of the legal requirements of section 25a (1) sentence 3 nos. 4 and 5 of the KWG. As the institutions are increasingly making use of IT services provided by third parties, for example because they are outsourcing IT services, the BAIT also include section 25b of the KWG in this interpretation. Among other things, this governs the treatment of outsourced activities and processes. The relationship between the BAIT and the general banking supervisory requirements for risk management is ensured by references to specific paragraphs in the MaRisk.

In the first version now available, the BAIT address in particular issues where BaFin identified material deficiencies in its inspections in recent years. Examples of such issues include IT strategy and governance, information security, access management and application development, as well as the procurement of IT services from third parties by means of IT outsourcing or the external procurement of IT services.

The BAIT are designed in particular to help the management of institutions and – indirectly through outsourcing agreements – IT service providers ensure a proper business organisation, including in terms of the organisational and operational structure of IT and the use of IT systems. However, the principle-based requirements of the BAIT should not be seen as an exhaustive list of requirements. In this respect, in accordance with AT 7.2 of the MaRisk the institutions and their IT service providers are still required to base their implementation of the BAIT requirements on generally established standards and to implement them effectively.

Additionally, an essential characteristic of the BAIT is that the principle of dual proportionality applies without restriction.

## Heightening IT risk awareness

A critical objective of the BAIT is to heighten IT risk awareness in the institutions and in particular at management levels. The relevant term “IT risk” was already defined above<sup>33</sup>. The need to create risk transparency and to address IT risk at all levels of the institution runs through all eight topic modules of the BAIT and is an integral part of the requirements in the individual paragraphs.

### IT strategy – II. 1. of the BAIT

In terms of IT strategy, the focus is on the requirement for management to deal regularly with the strategic implications of the various aspects of IT for the business strategy. In addition to the institution’s organisational and operational structure of IT, this also includes handling end-user computing (EUC) in the organisational units, strategic statements on the external procurement of IT services (outsourcing of IT services or external procurement of IT services) und basic requirements for contingency management, for example.

The management board must define the IT strategy in a cyclical process and resolve and publish it internally in the institution after discussing it with the supervisory board. The measures defined in the strategy for achieving the strategic objectives also establish clarity about the importance of IT for conduct of banking business. In addition, BaFin also expects strategic statements in particular about IT risk awareness, as well as references to compliance with the information security requirements in the institution and with regard to third parties.

### Governance – II. 2. of the BAIT

IT governance is the structure used to manage and monitor the operation and further development of IT systems, including the related IT processes on the basis of the IT strategy. The management board is responsible for the effective implementation of the IT governance arrangements within the institution and with regard to third parties. It is also responsible for ensuring that in particular information risk and information

---

<sup>32</sup> Circular 09/2017 (BA) – Minimum Requirements for Risk Management (MaRisk).

---

<sup>33</sup> See page 75.



© iStock/from2015

security management, IT operations and application development are appropriately staffed. In BaFin's view, this is particularly important because it enables the risk of the qualitative or quantitative understaffing of these areas to be identified at an early stage and rectified as soon as possible.

#### **Information risk management – II. 3. of the BAIT**

As part of information risk management, the institution must identify the level of protection required for relevant data or information. Target measures must be defined on this basis and compared with the actual measures that have been effectively implemented. The resulting transparency of the risk situation, the derivation of risk-reducing measures and the monitoring of their effective implementation, as well as the management board's awareness of the identified residual risk, constitutes the central requirement for heightening IT risk awareness in the institution and with regard to IT service providers.

To ensure that relevant IT-related risks can be adequately managed in addition to IT risk, BaFin expects the institutions to have an up-to-date overview of

the components of the defined information domain<sup>34</sup>, as well as their dependencies and interfaces. The institution should be guided in this respect in particular by internal operating needs, business activities and the risk situation. To be able to discharge its management responsibilities, the management board must be informed regularly, but at least once a quarter, above all about the results of the risk analysis and any changes in the risk situation.

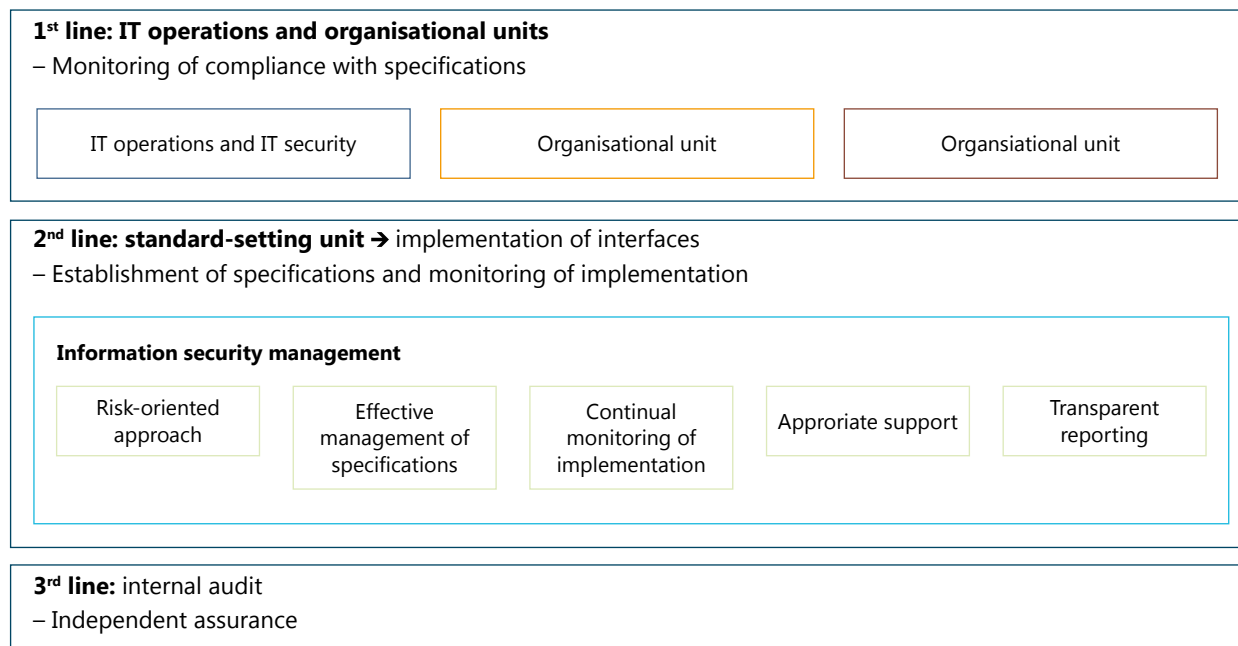
#### **Information security management – II. 4. of the BAIT**

Information security management makes provisions for information security, defines corresponding processes and manages their implementation. BaFin considers information security to be part of the second line of defence in the three-lines-of-defence model (see figure 1 "Three-lines-of-defence model", page 80); it both monitors and supports the operational first line of defence.

---

<sup>34</sup> An information domain includes, for example, business-relevant information, business processes, IT systems as well as network and building infrastructures.

**Figure 1: Three-Lines-of-Defence model**



© Source: own data, based on the three-lines-of-defence model, BIS Occasional Paper No. 11, 2015, Bank for International Settlements (BIS)

The management board is responsible for agreeing and publishing an information security policy within the institution that reflects the identified risk situation. The protection requirements defined as part of information risk management are to be specified in greater detail in information security guidelines.

BaFin believes that the information security officer (ISO)<sup>35</sup> or – at larger institutions – the information security management system (ISMS)<sup>36</sup> is primarily responsible for implementing, complying with and overseeing the institution’s provisions for information security, both internally and in respect of third parties, on the basis of the supervisory requirements and the relevant standards. For this reason, the information security officer function must be independent in terms of organisation and process so that information security can be evaluated and – if necessary – information

security incidents can be processed without conflicts of interest. The ISO reports to the management board regularly (at least once a quarter) and on an ad hoc basis.

Particularly in view of the increasing cyber risk, BaFin expects appropriate staff and financial resources to be available for this function in terms of both quantity and quality – as can be inferred from section 25a of the KWG in conjunction with AT 7.1 of the MaRisk and the relevant standards (BSI Standard 200-2, p. 40 et seq., ISO/IEC 27001: 2013, 4.4). Of course, BaFin also observes the principle of proportionality and has elaborated special exemption options in particular for small institutions.

**User access management – II. 5. of the BAIT**

Rights to access precisely defined parts of IT systems are necessary for certain tasks to be performed. They are also a central element for creating IT security. The user access rights concept must therefore be documented in writing as part of user access management. The organisational units must be involved

35 See BSI Standard 200-2, page 40 et seq.  
 36 See ISO/IEC 27001: 2013, 4.4.

in the development of the concept. The user access rights concept must apply the need-to-know principle, meaning that access rights are only approved and set up if they are needed to perform a concrete task. This also applies to the recertification process, which reviews whether access rights granted are still required. If this is no longer the case, the access rights must be effectively removed.<sup>37</sup>

### **IT projects and application development – II. 6. of the BAIT**

The management and monitoring of IT projects must in particular take account of risks in relation to duration, use of resources and quality. The management board must ensure that a general overview is prepared of IT project risks and risks resulting from the interdependencies between different projects.

Precautions must already be taken in the course of application development to ensure the confidentiality, integrity, availability and authenticity of the data to be processed in that program. The objective of these requirements is to reduce the risk that the application is unintentionally modified or deliberately manipulated. Attention is drawn again at this point to the remarks on integrating the relevant security measures in the sense of security by design.<sup>38</sup>

In addition, from BaFin's perspective it always makes sense to categorise end-user computing (EUC) applications that the organisational units develop or operate into risk classes and to evaluate this classification regularly. BaFin also expects each institution to document all EUC applications in a central register, especially applications that are important for banking processes, risk management and monitoring or accounting.

### **IT operations – II. 7. of the BAIT**

IT operations primarily fulfil the requirements resulting from the implementation of the business strategy and from the IT-supported business processes, and in doing so also manage the portfolio of IT systems appropriately. Furthermore, IT operations should also take up technical innovations according to the requirements of the organisational units and – if appropriate in project form – transfer them to IT production.

The corresponding processes for changing IT systems must be designed and implemented depending on their nature, scale, complexity and riskiness (proportionality). This also applies to newly procured or replaced IT systems as well as to security-related subsequent improvements (security patches). As part of product lifecycle management, the risks stemming from outdated IT systems must also be monitored. However, this is only possible if all components of the IT systems, including inventory data and the interdependencies of the managed objects, are managed appropriately.

---

<sup>37</sup> See BSI, *IT-Grundschutz: M 2.8* Assignment of access rights.

<sup>38</sup> See page 72.





Medium-sized and large institutions should generally use a configuration management database (CMDB), small ones at least an inventory register. The information collected must be updated regularly and on an ad hoc basis.

In the event of unscheduled deviations from standard operations, suitable criteria for informing the management board in advance of possible causes of this disturbance, the contingency measures to be taken to maintain or restore business operations, and the rectification of the deficiencies must be documented in writing. As part of contingency management<sup>39</sup> in accordance with AT 7.3 of the MaRisk, documented contingency tests must be carried out and evaluated regularly at the institution and, if necessary, together with significant IT service providers, and any weaknesses and deficiencies identified must be rectified.

#### **Outsourcing and other external procurement of IT services – II. 8. of the BAIT**

If an institution uses IT services, the same generally applies as for the use of services: the institution must verify whether this involves outsourcing within the meaning of section 25b of the KWG. If this is the case, it must meet the requirements of section 25b of the KWG and AT 9 of the MaRisk, and the institution must perform an advance risk analysis. The risks from other external procurement of IT services, the definition of which can also be found in AT 9 of the MaRisk, must also be assessed in advance. This is the only way the institution can determine its complete risk situation and identify concentration risks in externally procured IT services. BaFin also expects the measures derived from the relevant risk analysis to be incorporated into the design of the individual contracts with external service providers. In the case of significant outsourcing of IT services, the requirements of AT 9 number 7 of the MaRisk must be complied with; this also applies of course to cloud computing.<sup>40</sup>

#### **Implementation of the BAIT**

The BAIT entered into force with their publication on 6 November 2017. BaFin did not provide for an implementation period or transitional periods because the BAIT do not impose any new requirements on the institutions and their service providers. The relevant requirements of the German Audit Report Regulation (PrüfbV) including the BAIT will be taken into account for the first time in the audit of the 2018 annual financial statements. Since the beginning of 2018, inspections under section 44 of the KWG with an IT focus have also been based on the BAIT.

#### **Possible revisions to the BAIT**

The modular design of the BAIT gives BaFin the necessary flexibility for future revisions or additions. BaFin has already announced on several occasions that the topic of "IT contingency management including test and recovery procedures" is to be integrated into the BAIT.

It is also currently examining whether the BAIT need to be adapted to the "G7 Fundamental Elements of Cybersecurity"<sup>41</sup> and the "Guidelines on the security measures for operational and security risks of payment services under Directive (EU) 2015/2366 (PSD2)".<sup>42</sup>

In close cooperation with the Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik* – BSI), BaFin is also considering a special module on critical infrastructures (KRITIS) to supplement the BAIT. This special module will apply exclusively to those banks and IT service providers that are operators of critical infrastructures in the financial and insurance sector within the meaning of section 2 (10) of the German BSI Act. It will formulate the necessary requirements that these operators of critical infrastructures must fulfil in order to comply with the relevant requirements of section 8a (3) of the BSI Act.

---

<sup>39</sup> See *BSI-Grundschrift* 100-4 or ISO 22301:2012.

<sup>40</sup> See BaFinJournal April 2018, page 29 *et seq.*

---

<sup>41</sup> See Chapter 3.

<sup>42</sup> EBA Guidelines EBA/GL/2017/17; Payment Services Directive 2.

# 7 Digitalisation of the insurance industry

## Digitalisation as one of the key strategic topics in the insurance industry

As well as optimising internal enterprise processes and increasing efficiency, digitalisation in the insurance sector is primarily concerned with improving contact with customers.<sup>43</sup> In recent years, insurance companies have already streamlined and automated many of their business processes – internally and in distribution. The internal automation ratio can be significantly increased in particular by automating manual process steps in the direction of application, contract and claim processing that is as fully digital as possible. Costs can also be reduced through economies of scale. Many standardisable processes such as contract portfolio management and claims management are already highly automated.<sup>44</sup>

Another focus of digitalisation in the insurance industry is on the design of customer interfaces. The digital transformation of insurers can only succeed if customer

loyalty and customer satisfaction can as a minimum be maintained or, better still, significantly increased. To achieve this, it is essential to provide customers with measurable value added – in the best case, an optimal customer experience from customers' point of view.<sup>45</sup>

## New challenges in insurance distribution – cyber insurance

Various studies show that cyber threats have been recently moving further to the fore both internationally<sup>46</sup> and on the risk agenda of German companies. The current Allianz Risk Barometer published by Allianz Global Corporate & Speciality SE (AGCS) shows that cyberattacks are now in second place of the most feared corporate risks.<sup>47</sup>

---

43 Versicherungsforen Leipzig, Digitalisierung der Customer Journey bei Versicherungen in der DACH-Region (Digitalisation of the customer journey at insurers in the DACH region), <https://www.liferay.com/documents/10182/171894549/Digitalisierung%20der%20Customer%20Journey%20bei%20Versicherungen%20in%20der%20DACH-Region>, retrieved on 11 May 2018.

44 Bain & Company, Digitalisierung der Versicherungswirtschaft: Die 18-Milliarden-Chance (Digitalization of the insurance industry: The multi-billion opportunity), page 21, [http://www.bain.de/Images/161202\\_Bain-Google-Studie\\_Digitalisierung\\_der\\_Versicherungswirtschaft.pdf](http://www.bain.de/Images/161202_Bain-Google-Studie_Digitalisierung_der_Versicherungswirtschaft.pdf), retrieved on 11 May 2018.

---

45 IT Finanzmagazin, Whitepaper der Versicherungsforen Leipzig & NICE: Kunden und Digitalisierung treiben die Assekuranz (White paper of the Leipzig insurance forums & NICE: Customers and digitalisation are driving the insurance industry), <https://www.it-finanzmagazin.de/whitepaper-der-versicherungsforen-leipzig-nice-kunden-und-digitalisierung-treiben-die-assekuranz-31078>, retrieved on 11 May 2018.

46 datensicherheit.de: Cyber-Sicherheitsvorfälle: Neuer KASPERSKY-Bericht über Folgekosten liegt vor (Cyber security incidents: New KASPERSKY report on follow-up costs now available), <https://www.datensicherheit.de/aktuelles/cyber-sicherheitsvorfaelle-neuer-kaspersky-bericht-ueber-folgekosten-liegt-vor-25899>, retrieved on 11 May 2018.

47 Allianz Risk Barometer 2018, [https://www.allianzdeutschland.de/allianz-risk-barometer-2018/id\\_79713564/index](https://www.allianzdeutschland.de/allianz-risk-barometer-2018/id_79713564/index), retrieved on 11 May 2018.



The German insurance industry has also responded to this situation by developing a cyber insurance product that takes various forms.<sup>48</sup> The German Insurance Association (*Gesamtverband der deutschen Versicherungswirtschaft e.V. – GDV*) has published – non-binding – general insurance policy conditions (“AVB Cyber”) that impose extremely far-reaching requirements on applicants wishing to insure this risk.<sup>49</sup>

### **Supervisory Requirements for IT in the Insurance Sector (VAIT)**

It should come as no surprise that BaFin also expects the industry that can insure cyber risks to comply with and effectively implement the basic requirements for IT governance, IT risk and information security management, application development and the operation of IT systems. In mid-March of 2018, BaFin issued the draft Circular on Supervisory Requirements for IT in the Insurance Sector (VAIT)<sup>50</sup> for consultation. On 2 July 2018, it published the VAIT.

In the same way as the BAIT for the banking sector, the VAIT will constitute the central element of IT supervision for all insurance companies and *Pensionsfonds* (companies) referred to in numbers 2 and 3 of the preliminary remarks on the VAIT.<sup>51</sup>

The Circular contains guidance on interpreting the provisions of the German Insurance Supervision Act (*Versicherungsaufsichtsgesetz – VAG*) governing business organisation, to the extent that they relate to companies’ technical and organisational resources (see info box “Interpretation of the VAG by the VAIT”).

48 VersicherungsJournal.de, Signal Iduna bringt Cyber-Schutzschild auf den Markt (Signal Iduna launches cyber shield product on the market), <https://www.versicherungsjournal.de/versicherungen-und-finanzen/signal-iduna-bringt-cyber-schutzschild-auf-den-markt-131904.php>, retrieved on 11 May 2018.

49 GDV: AVB Cyber, relevant here: A 1-16 (and specifically A 1-16.2 a), <https://www.gdv.de/resource/blob/6100/d4c013232e8b0a5722b7655b8c0cc207/01-allgemeine-versicherungsbedingungen-fuer-die-cyberisiko-versicherung--avb-cyber--data.pdf>, retrieved on 11 May 2018.

50 [www.bafin.de/dok/10622504](http://www.bafin.de/dok/10622504).

51 See BaFinJournal April 2018, page 24 *et seq.*

## **Interpretation of the VAG by the BAIT**

The VAIT interpret sections 23, 26 and 32 of the VAG, for example.

The VAIT thus specify what BaFin understands to be the appropriate design of IT systems (hardware and software components) and the associated IT processes, with particular regard to information security requirements. As many companies now obtain IT services from third parties in the form of outsourcing or other service relationships, the relevant requirements are also formulated in the VAIT.

The VAIT aim to make transparent what BaFin requires of companies and their IT service providers. This is designed to help them ensure a proper and effective business organisation, including with regard to IT. However, as the VAIT do not cover all the requirements, and the granularity and scope of the requirements are not exhaustive, all companies are obliged to apply generally established IT standards and take into account state-of-the-art technology, above and beyond the detailed specifications contained in the VAIT.

The principle of proportionality also plays a significant role in the implementation of the requirements of the VAIT for business organisation and hence also in the design of structures, IT systems or enterprise processes. The requirements must therefore be met in a way that takes account of the nature, extent and complexity of the risks associated with the company’s activities.

The need to create risk transparency and to deal with IT risk at all levels of the company and its IT service providers also runs through all topics covered by the VAIT.

# 8 Summary

Digitalisation has already triggered considerable, and in some cases far-reaching, change in the financial and insurance industries and will continue to do so. Many customers want to be able to interact with banks and insurers anywhere, anytime. The expectations they have of companies in terms of the security and integrity of their data are correspondingly high. This is leading to intense competition between established providers and innovative new competitors.

Banks and insurers possess two raw materials that are needed in a digital world – trust and data. The increasing deployment of Big Data (BD) and Artificial Intelligence (AI) that is currently also observable in the financial market poses huge challenges to both industry and the regulators, as well as – and in particular – customers. Despite all the necessary pressure for change, companies would be well advised for economic considerations alone to think hard about the extent to which they really want to leverage the full potential of the new technologies, for example when monetising personal data with the help of BDAI applications. Otherwise, they run the risk in some cases that reputational damage could outweigh the benefits.

BaFin's primary mission is to safeguard the proper functioning, stability and integrity of the financial system. It discharges this mission, for example, by imposing supervisory requirements on the business organisation of companies that require permission to operate on the financial market. It goes without saying that digital change is also not leaving the supervisory authorities unscathed. They must regularly assess what new legal and technical requirements the wave of innovation currently being experienced by society and industry is placing on regulation and supervision. No one can give a conclusive answer at the moment, but this makes it all the more important to continuously confront such issues and to ensure a constant exchange between authorities, business and researchers.

It will necessarily be a task for society as a whole to strike a balance between the returns expected by companies, the necessary monitoring of compliance with governance and cybersecurity requirements by supervisors, and the informational self-determination of consumers, and to ensure this in the long term.



# Imprint

## **Publisher**

Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)  
Federal Financial Supervisory Authority (Bundesanstalt  
für Finanzdienstleistungsaufsicht – BaFin)  
Communications (Directorate K)  
Graurheindorfer Straße 108 | 53117 Bonn  
Marie-Curie-Straße 24 – 28 | 60439 Frankfurt am Main  
[www.bafin.de](http://www.bafin.de)

## **Editing and layout**

BaFin, Speeches and Publications

Editing: Ursula Mayer-Wanders (Head of Division)

Tel.: +49 (0)228 4108-2978

Jens Valentin

Tel.: +49 (0)228 4108-2363

Layout: Susanne Geminn

Tel.: +49 (0)228 4108-3091

E-mail: [perspektiven@bafin.de](mailto:perspektiven@bafin.de)

## **Designkonzept**

[werksfarbe.com](http://werksfarbe.com) | konzept + design

Humboldtstraße 18, 60318 Frankfurt

[www.werksfarbe.com](http://www.werksfarbe.com)

Bonn and Frankfurt am Main | 1 August 2018

ISSN 2625-5952

## **Access**

BaFinPerspectives is published twice a year on the BaFin website in German and English. The German edition is published under the title “BaFinPerspektiven”. If you sign up to the BaFin-Newsletter, you will be informed by e-mail when a new edition is published. The BaFin-Newsletter can be found at: [www.bafin.de](http://www.bafin.de) » [Newsletter](#)

## **Disclaimer**

Please note that great care has been taken in compiling all of the information contained herein. However, BaFin accepts no liability for the completeness and accuracy of this information.

The articles and interviews in BaFinPerspectives are subject to copyright. Reprinting and distribution is only permitted with BaFin’s written consent, which may also be issued by e-mail.

## **Printed by**

Druckerei Silber Druck oHG

Am Waldstrauch 1

34266 Niestetal