English version
27 March 2019

Statement of the FinTech Council concerning the blockchain strategy of the German government in the context of public consultations

Preamble

Blockchain strategy of the German government. The German government is planning to develop a blockchain strategy. As part of these efforts, it is conducting a public consultation, partly by means of a detailed questionnaire. With this document, the FinTech Council[1] would like to make a statement on the German government's questionnaire regarding the planned blockchain strategy.[2] Further, it would like to comment on the position paper written by the Federal Ministry of Finance (BMF) and the Federal Ministry of Justice and Consumer Protection (BMJV) on the subject of the regulatory treatment of electronic securities and crypto tokens. The FinTech Council highly commends the German government for planning to develop a blockchain strategy.

Regulatory context as the primary focus of this statement. In this statement, the FinTech Council focuses primarily, but not exclusively, on aspects that have a regulatory context. A concrete implementation-related catalogue of measures forming part of the strategy is not the focus of this statement.

Representation of the euro on a blockchain system. In the context of forward-looking legislation, we would like to draw attention to the topic of euro-on-ledger in particular and cash-on-ledger in general, which covers topics such as official DLT-based currency in the form of e-money, commercial money or even central bank digital currency (CBDC). Various options are conceivable, but they give rise to different problems and systemic risks (see chapter on security of blockchain systems and chapter on the General Data Protection Regulation (GDPR)). Almost all the areas mentioned by the German government in the position paper (e.g. industry 4.0, IoT, energy, logistics and mobility) will not be successful without consideration of official currencies on a DLT basis.[3] Despite the importance of this topic, we will not make a comprehensive statement of this subject here, given that this topic is already being extensively analysed and partly implemented on a test basis in various places, e.g. central banks. It should also be noted that several companies in Europe have already tested euro-on-ledger with e-money licenses and have carried out pilot projects. The German government would be well advised to pay special attention to these projects, as any damage to confidence in the euro must be avoided. The

[1] Further information on the FinTech Council of the Federal Ministry of Finance can be found at the end of this document.
[2] In this document, the terms "blockchain" and "Distributed Ledger Technologies" (DLT) are used to describe all the different aspects of the technology, since a distinction is not appropriate for most of our statements.
[3] Of course, it is also possible to connect legacy systems via an interface.

demand for traditional currencies on DLT systems can also be met by an interface to existing banking systems. In any case, the issue of integrating the euro into or connecting it to blockchain systems should be taken into account and further investigated in the context of the German government's blockchain strategy due to its importance for German industry and the financial sector.

Summary of the main recommendations

Before aspects are explained in detail, the most important recommendations are summarised below:

- **Technology-neutral regulation:** An important part of the blockchain strategy is considered to be the technology-neutral regulation of blockchain technology. If possible, we recommend aiming for regulation that is separate from the technical implementation, in particular, separate from an exact specification of the blockchain technology used.
- **Focus of regulation on issuers and service providers:** The rules should primarily focus on service providers who interact with blockchain systems. They should be responsible for their offers and therefore be made liable for the offers and the risks associated with the technology used. Such service providers include issuers of securities, providers of custody solutions and service providers who connect the empirical real-world view with the conceptual world of tokens (e.g. connection of machines via IoT). The government should also tackle the fundamental problems for the enforcement of claims in blockchain systems.

- **Rapid regulation and rapid development of the blockchain strategy:** Due to the dynamic nature of blockchain technology and also the importance of the technology, the definition and implementation of the blockchain strategy, including any regulatory measures that may be necessary, should take place quickly.
- **European regulation:** Certain measures have to be implemented in Germany, but we want to emphasise the importance of regulation at a European level. In this respect, the blockchain strategy should target measures at this level. Some problems also require international regulation to avoid regulatory gaps or to close them if they exist. In addition, it is important to avoid a situation where, due to a lack of EU-wide regulation, “oases” for blockchain-based applications are created within the EU which could undermine the national laws of the other member states.
- **Dematerialised securities:** First steps towards the introduction of electronic securities have been taken with the position paper of the BMF and BMJV. This path should be pursued rapidly in order to dematerialise all types of securities. This applies not only to the document obligation but also to any written form requirements. Proper registration must be ensured, as is also currently required.
- **Aspects of data protection:** With regard to existing data protection rules, the blockchain strategy should plan to clarify the interpretation of the data protection rules in order to assess consistency with blockchain technology. Requiring operators to provide information is not compatible with a decentralised blockchain without an operator. Thanks to the public availability of the chain, however, the required information can easily be provided in a different way. It should also be clarified that so-called hashes and public keys are not personal data, because the original data cannot be reconstructed.
- **Importance of education:** Sustainable DLT innovations require interdisciplinary training in information technology, digitalisation, and programming. Related – previously niche – areas are also important (e.g. the interface between computer science and law, the interface between

computer science and engineering).Therefore, DLT education at universities, research institutes and in relevant companies should be promoted. This applies not only to education at universities but also to further training over the course of a person's working life.

- **Abstract definition of requirements for tokens:** In the future, tokens will appear in a wide variety of forms. This requires regulation that is as abstract as possible. Tokens will not only be used in the form of security tokens such as digital securities on blockchain systems. Tokens could also represent currencies such as the euro, or certain rights such as access to a rental car. Due to the expected range of areas of application, application-specific regulation would not be effective. We therefore recommend that the rules for the rights represented by a token be left as unchanged as possible and remain in the focus. This would automatically answer unresolved questions, for example regarding taxation. At the same time, general rules for tokens should be found that address general questions such as ownership, transfer, and misconduct (e.g. theft, fraud). These regulations can be made technology-neutral to ensure that they also cover other systems beyond blockchain.
- **Research field for Germany and the European Union:** The rapid technological development of blockchain-based systems is driven by industry. However, the question of what properties a blockchain would need in order to comply with regulation has not been pursued sufficiently. A research project in this field would have great potential to strengthen Germany and to highlight very precisely the problems and possible solutions between technology and regulation. When it comes to certain questions (e.g. quality parameters/security levels of blockchain systems, assessment of the reliability of blockchain systems), there is currently no reliable basis for decision-making. Such assessments are necessary in the context of formulating the requirements for the blockchain securities register of electronic bonds, for example. These research topics must be tackled rapidly. Therefore we advise that specific questions should be addressed in the context of focused analysis. These should be included in the blockchain strategy and support it in the coming years.

Introduction

Relevance of the technology for policy-makers. By developing a comprehensive blockchain strategy, the German government wants to provide a firmly defined political agenda and a legal framework in order to promote Germany's innovative strength in this area and strengthen its future competitive position in the digital era. A driving factor is the – already remarkable – position of German companies (start-ups and established companies) in the blockchain sector. In addition, a first milestone is the realisation that blockchain technology is a key technology which could completely change the way in which companies operate and coordinate in the next 3 to 15 years.

Main fields of DLT application. Distributed ledger technologies (DLT) are mainly used in the areas of "finance and assets", what is known as the "machine economy", all registers (e.g. commercial register, land register, reporting system, and above all the identity of persons and objects) and data monetisation. Deployment in developing countries is also conceivable. The "machine economy" deals with the secure connection of billions of devices to the Internet and, in the future, to payment transactions. DLT, and crypto-assets in particular, can help to achieve financial inclusion goals in developing countries. This covers the provision of simple or complex financial services to two to three billion people who currently have no access, or only very limited access, to payment infrastructures or banking services.

Sustainability of legislation. We as the FinTech Council welcome this project and would like to offer structured assistance for efficient legislation in order to overcome future challenges associated with the direct application in the real economy of blockchain technology and other digital distributed systems for the maintenance of registries or for the recording of transactions (generally known as DLT). Blockchain technology is a specific subcategory of DLT. Our assessments refer to both technologies, blockchain in particular and DLT in general. Therefore, we will not explicitly differentiate between the two in the following statement.

Modular structure. The various possible applications create a demand for a legal framework that is as modular, comprehensive and flexible as possible. The enormous worldwide dynamism of the technology is characterised primarily by the open source character and the transparency of the crypto-assets' publicly accessible blockchain systems. Legislation must take advantage of existing developments but also release new innovative power, whilst at the same time counteracting the associated risks listed in this document. There are certain applications in the area of smart contracts and IT security that might be suitable for potential certification processes which go beyond legal regulation, but these applications are less suitable for other processes. Here, it is important to find an efficient cost-benefit ratio for the specific fields of application. The main focus should lie on abstract or generally valid rules for tokens.

Existing regulation as a foundation. From our perspective, it is crucial to redefine the relevant regulations universally for these digital, decentralised value exchange and contract processes and to either interpret existing regulations in a targeted way or supplement them. The aim is to promote the entire range of these technologies and to create a legal and organisational framework wherever the processes of a central party or intermediary – such as a bank, a stock exchange or a platform – can potentially be taken on by a DLT system. Intermediaries, however, will continue to fulfil important functions, e.g. as gateway providers, technology providers, contact persons for the government or parties responsible for compliance with regulatory measures, especially in the area of anti-money laundering.

Strengthening innovation through legal certainty. Overall, the intended regulation should primarily focus on being able to represent rights, claims and things in the "real world" by means of a DLT infrastructure – including the associated fields of application. Given this wide range of possible applications, profound legal questions arise in some areas which need to be clarified in order to rapidly provide legal certainty with regard to applications in industry. This legal certainty is crucial so that businesses (especially industrial companies, financial organisations and startups) and the public administration are able to rapidly develop and put into operation DLT-based systems and applications in Germany.

Need for a fundamental analysis. Bitcoin is now ten years old and illustrates the potential, the successes and the problems of new blockchain technologies and DLT. It is problematic for the existing legal and economic system that this technology eludes regulatory intervention by operating on a distributed, dynamic and transnational basis. The idea of using the rules technically coded into the system as an absolute reference point instead of a legal framework appears attractive at first glance but is highly problematic. Every logical system is incomplete, as has been demonstrated using formal proofs (e.g. Gödel's incompleteness theorem). This could also be true for DLT systems. The example of "The DAO" clearly shows that not all cases can be considered in advance and that errors exist in the system. However these systems do not provide for dealing with these cases or eliminating errors. In a way, the technical system resists a legal arrangement or correction and undermines the sovereignty of the legal system, in that users participate anonymously in a system without owner or operator. In this respect, this new technology disrupts the foundations of the existing economic and legal system.

Compatibility of IT and jurisdiction. The question is whether, in the course of technological progress, the further development of operator-less blockchain technology, can create the possibilities of intervening in the technology which is necessary for the legal system, or whether the conflict between the legal system and the technical systems remains unresolved. In any case, the question arises regarding which system can prevail over the other. Morally, human sovereignty over the technical system is to be demanded; in practical terms, it remains to be seen which allegiances will form and whether humans are ready to prefer technical malfunctions to human misjudgments. At present, many societies seem to be more inclined to put their faith in technology.

Risks and opportunities at the interface between business models and new technical implementation. Regulatory action in this area is necessary since regulated areas such as finance are affected, but the applications that use DLTs are not covered by the existing rules. Consumer protection rules must also be implemented accordingly with regard to DLT systems. Therefore, it must be ensured that business models on the blockchain meet regulatory requirements. It is necessary to consider the extent to which the corresponding regulatory requirements need to be modified for the new technology. In principle, the aim should be to ensure that regulation remains technology-neutral and does not need to be adapted to new technological developments. However, regulators should address risks that arise from the specific technical implementation – risks which are difficult to assess in advance.

Definition of key terms

Different types of blockchain systems and DLTs. Developing a vision regarding the general topic of blockchain is complex because there are many types of blockchains and DLTs: public blockchain systems, private blockchain systems, or hybrid systems (federated blockchain systems), with or without tokens, etc. Assessing or even finding new rules is therefore difficult and sometimes even impossible, since scalability, applicability, transaction costs, security, etc. depend on which characteristics of a blockchain system are being discussed.

Relationship between blockchain and DLT. In our statement, we consider the full scope of DLT protocols and their applications, of which blockchain is, strictly speaking, a subset. Accordingly, one definition of blockchain/DLT would be:

> *“a protocol for synchronising a decentralised database consisting of a set of distributed ledgers, wherein the changes 1) are replicated and not changeable, 2) are secured by cryptography, and 3) can be automated (by smart contracts)."*

Differentiation between public and private blockchain systems. The discussion about blockchain ranges from the functionality and application of public blockchains like Ethereum – open, widely used, but with important scaling problems that have to be solved – to private DLT protocols (e.g. Hyperledger or R3 Corda). The latter are not fully decentralised but are currently highly scalable. In addition to these examples of general blockchain protocols for which different applications can be programmed, there are many special blockchain protocols that can be created for a specific company, application, or industry.

Altogether we can observe two very different areas in which blockchain or DLT is used with completely different dynamics:

- **Public blockchain systems**: These are completely decentralised technologies and often involve a crypto token which is intrinsic to the system. They are often financed by an initial coin offering (ICO). These systems are the basis for the development of open (B2C) applications, often by startups, who may follow very disruptive approaches (e.g. disintermediation of certain sectors).

- **Private blockchain systems**: These are primarily DLT protocols for enterprise applications (or in the context of public administration) with specific permission options, most of which do not require crypto tokens. These are the basis for novel use cases in companies, which are more frequently implemented by or via established companies – individually or in consortia.

It is important to avoid a situation in which the discussion concentrates mainly on the former variant, which may subjectively be perceived as more "current" even though the latter will lead to market-oriented applications in many different sectors.

Token economy

Abstract definition of tokens. "Token" is a term that is often used but not clearly defined in connection with blockchain applications, especially platform-based use cases. In particular, this is because the use of the term token in the context of "real world" digital use cases and in connection with purely blockchain-based use cases could be perceived as very different at first sight. We will examine these two facets of the term token separately below in order to develop a congruent approach. With these two concepts, we first of all distinguish between use cases implemented purely on the blockchain (e.g. payment transactions based on crypto assets) and use cases implemented on the blockchain for digitising existing rights, things or claims (e.g. euro payment transactions on the blockchain).

Digital mapping of any rights through tokens. We would like to refer to a very clear definition of the term token in the context of the first draft of a law[4] which is expected to enter into force in Liechtenstein in a few months. In general, tokens do not represent a sole right in a digital context according to the definition, but should rather be understood as a platform-based shell or container. This may embody "claims or membership rights in respect of a person, property rights or other absolute or relative rights."[5] An example is the right of ownership of a (physical) object of value or a security. Other examples range from traditional currencies (e.g. euros, US dollars) to token-based intellectual property licensing rights and tokens for real assets (e.g. machines, cars, etc.). Within this framework, the specific rights included in tokens, for example, capital market rights, can then be applied. Third parties interacting with the tokens (e.g. in the context of secure custody, trade, valuation or linking of identities to persons/companies/objects) should, in turn, be subject to additional separate service-related rules in order to ensure jurisdiction at all levels. We will continue this line of argument throughout this text.

[4] The document "Government Consultation Report and the Draft Act on Transaction Systems Based on Trustworthy Technologies (Blockchain Act)" is available at https://www.llv.li/files/srk/vnb-blockchain-gesetz.pdf (German version).
[5] See note 9, p. 87.

Token economy: tokens in “real world” use cases

Enormous economic potential. A central value proposition of the blockchain is to make real goods and assets of all kinds legally storable in a digital form and tradable or transferable between any parties, potentially by eliminating the current intermediaries. According to prevailing opinion, the construct of the (digital) token seems to be a suitable means of achieving this goal. The token represents the real value or object or intangible right in the digital world on the blockchain. In the following, we will use the term “value” for all kinds of values, objects and intangible rights, e.g. real estate, automobiles, shares, license rights. The owner of the token nevertheless has all rights and duties which would result from the possession of the corresponding value in the real (not digital) world. To guarantee this, it is of utmost importance to ensure the legal certainty of the transformation of the “real” value into a token. This process is also called tokenisation. The resulting implementation is referred to as the token economy.

A proven concept in a new form. The concept of the token is not a new approach. However, tokenisation on the basis of the blockchain promises to open up new economic possibilities and realise potential efficiencies. A good example of this is money (i.e. the euro) on the blockchain (see below).

Advantages of tokenisation. Among the advantages that are gained due to the tokenisation of real values are:

- Traceability of value transfer from owner to owner;
- Simplifying value transfer and potentially reducing associated costs;
- Increasing the liquidity of tradable assets by making them easier to divide, e.g. the almost arbitrary divisibility of tokens could make it easier to sell small shares in real estate;
- The possibility of merging physically separated markets and thus increasing transparency, as well as possibly creating new products.

Categorisation of legally problematic areas: In our opinion, the legal and regulatory issues that must be addressed in connection with tokens, tokenisation and the transfer of tokens can be divided into two categories:

- **Token container:** the essence of the token without consideration of the underlying value;
- **Token content:** the value, content, right or thing represented by the token on the blockchain.

Examples of token container and token content. This model can perhaps best be represented by the metaphor of a freight container, complementing the description of a token economy given above. The token container corresponds to the container itself and the content of a container corresponds to the real value so that a loaded container corresponds in this analogy to the token introduced here. Handling a loaded container involves on the one hand the rules and processes for the container and on the other hand the rules and processes for the cargo it contains. For example, while transporting a container, we should take into consideration the dimensions of the container, transport processes and loading processes. In the standardised loading documents, for example, the acceptance of the load by the respective carrier is also confirmed. In addition, there are “content-dependent” rules, e.g. the import regulations that apply to the respective loaded container.

Elements of an efficient token regulation. Following this model, the consistent introduction of tokens that is most compatible with current laws, regulations and processes, and which is hence the basis of a

digital token economy could take the following form, being composed of two key elements:

- **General rules for all types of tokens:** Rules that are linked to the nature of the token as a container; hence rules that apply to tokens of all types,e.g. regulations, laws, control requirements. This concerns, for example, the generation of tokens (shells), the tokenisation of real values as well as the reverse process (digital representations are deleted and the administration of the rights for a value is again carried out purely in the non-digital world), the transfer of tokens between entities on the blockchain as well as administration/storage of the tokens.

- **Existing laws and regulations**: Capital market laws and regulations (but also laws and regulations in other legal areas) should be applied to tokens according to their nature, i.e. depending on the value underlying the token (container load), to the greatest extent possible and in an unchanged form. However, where necessary, adjustments should be made to allow for the appropriate digitisation of the value and to transfer the essential elements of the law to the digital world. For example the custody of tokens where the "container content" represents securities, is conducted in accordance with the Securities Deposit Act.

First milestones for electronic securities. In our view, the key-issues paper[6] recently published by the Federal Ministry of Finance and the Federal Ministry of Justice and Consumer Protection is compatible with this model. It discusses how electronic securities (bearer bonds) can be produced and circulated in accordance with existing laws. Decisive changes to the corresponding laws (e.g. "[...] the current rule whereby securities must be represented by physical certificates will no longer apply across the board [...]") will be made as well as suggestions as to how essential aspects of today's regulatory framework, e.g. investor protection, should be implemented in the digital world in order to meet the corresponding requirements. The above-mentioned position paper also contains proposals for the implementation of consumer protection for digital debt securities. These implementation proposals are therefore based on the current consumer protection guidelines for the financial instruments mentioned in the paper.

Tokens and consumer protection. Since the token is theoretically accessible to everyone, at least when offering tokens on blockchains without access restrictions, and the sale would thus correspond to a type of issue, it would be worth considering whether, and which, generally applicable consumer protection rules should exist for tokens in the case of an implementation in accordance with the token model described above. In combination with the specific rules and regulations for electronic debt securities, this would ensure the level of consumer protection aspired to in the above-mentioned position paper. Liechtenstein's Blockchain Act, which was mentioned earlier, sets this out on p. 68: "[...] token issuers are obliged to publish basic information about the tokens and inform potential buyers about the tokens [...]".

Separation between tokens and underlying blockchain infrastructure: As noted in the introductory remarks to this chapter, the value proposition of blockchain includes, in particular, the legal security of tokenisation and its reversal, the rights, and obligations evidenced by the token itself, as well as all token-related processes. This also shows the limits of the separation between the token and the token management system. The token itself cannot ensure its own stability. If the blockchain storing the token is compromised or even deleted, the token is also affected. Likewise, double spending of the token can only be prevented by the surrounding system. Thus the digital token has completely different character-

[6] See "Key-issues paper on the regulatory treatment of electronic securities and crypto tokens – Allowing for digital innovation, ensuring investor protection" of 7 March 2019 (Federal Ministry of Finance, Federal Ministry of Justice and Consumer Protection).

istics compared with a paper certificate. In particular, the security of the token depends on the design of the consensus algorithm of the respective blockchain system. As far as we know, metrics for assessing dynamic safety do not yet exist (cf. the chapter “Security and reliability of blockchain systems”).

Life cycle of a token. In order to enshrine the token economy in law in a legally secure manner, it seems necessary to clearly define the terms “token” and “possession of a token” and to regulate the processes and information obligations relating to the life cycle of a token accordingly. A good starting point can be found in the Liechtenstein bill. In this regard, we currently regard it as necessary to enshrine the following points in law:

- “The token as a legal element to embody rights of all kinds” (citation from the Liechtenstein bill);
- The mandatory basic information for each token;
- Proof of exclusive ownership and transfer of ownership. In current practice, cryptographic private-public key-based infrastructures are usually used for this purpose.

We currently see a need to regulate the following processes throughout the token lifecycle:

- The **creation or tokenisation** – technical creation of the token, linking to the respective basic information as well as linking to the rights embodied by the token;
- The **issuance** – public issuance/provision of the tokens;
- The **transfer** – direct transfer between users of a blockchain (peer-to-peer transfer), direct transfer between users through dedicated service providers, operation of markets for tokens of all kinds; and
- The **custody** – processes and IT applications for the custody of tokens or corresponding private keys (usually outside the blockchain) and custody services.

The importance of the right contained in a token. On the basis of the container model, the treatment of a specific token or a token class results from the laws and regulations to be created in the implementation phase, and from the owner’s rights contained in the token. In case of doubt, the contained right will determine how the token is dealt with.

Token economy: tokens in use cases that are entirely blockchain-based

Representation of exclusively digital rights. Following the use cases in which tokens are used to digitally represent rights in the “real” or physical world, we now turn to a possible treatment of tokens that exclusively bear digital rights. Strictly speaking, one would still have to distinguish between native tokens (ITC class TTS41 according to the International Token Classification, ITC[7]), e.g. ether as a

[7] The classification system “International Token Classification” (ITC) was introduced by the International Token Standardisation Association (ITSA), which is based in Berlin. The associated founding members are, among others, the Bundesverband deutscher Banken (BdB) and the Bundesverband Investment und Asset Management (BVI).

native token of the Ethereum blockchain, and purely digital tokens (ITC class TTS42), e.g. securitisations of rights that are defined only on the blockchain, e.g. the shares of an investment fund that invests only in crypto-assets.

Tokens with direct reference to the respective infrastructure. Native tokens (ITC class TTS41) are part of the respective blockchain infrastructure and in our opinion enjoy a special position on the respective blockchain, since their generation and direct forwarding between users of the respective blockchain is closely linked to the respective blockchain protocol. Basic information about these native tokens is generally derived from the respective system parameters or from the protocol.

Equivalence to tokens with direct reference to the real world. In the case of tokens that represent purely digital rights but are not native tokens as defined above (ITC class TTS42), we consider in principle the same requirements to exist as described above in the section “Tokens in ‘real’ world use cases”. These tokens are generated, possibly on the basis of rules, and then made accessible to the users of the blockchain. A transfer from user to user (i.e. peer-to-peer) takes place, as with the tokens described above in “real” world use cases, on the basis of the protocol of the respective blockchain.

Equal treatment of tokens (token container). Due to the fact described above, we are of the opinion that all tokens have to be fundamentally treated the same. However, different technical requirements in terms of implementation should be taken into account by having sufficiently abstract regulation.

Tokens have a variety of appearances

Tokens as heterogeneous constructs. Among other things, the German government argues in its blockchain strategy questionnaire that there is no danger to financial market stability from the amount of crypto assets in circulation today but that, for example, money-laundering obligations must be adapted immediately. We welcome this point and would like to emphasise it. The money-laundering problem must be solved urgently, otherwise the level playing field with the established players will be distorted, and they will have to bear massive costs as a result. If crypto assets are brought into line with local laws, this could lead to the development of worldwide carrier platforms for tokens (e.g. Ethereum).

Enormous variety of different token types. The range of projects (mostly startups) that have been financed by tokens so far, as well as the spectrum of further application possibilities for token ecosystems as carrier platforms for rights, will become increasingly differentiated. Well over US$19 billion in investment capital was raised in 2017 and in the first half of 2018 via ICOs. However, almost half of those investments have since lost some or all of their value. Typically, the utility tokens that have been issued to date grant the purchaser a right to future services or claims to products. Fraudulent emissions also hit the headlines as part of the major ICO wave in 2017 and 2018. We would like to take the existing uncertainties regarding the type and design of tokens as an opportunity to draw attention in the following section to a special form of tokens: security tokens. This could also be viewed in the context of a corresponding regulation of electronic money. Ultimately, none of the areas mentioned by the German government (industry 4.0, IoT, energy, logistics and mobility) can

avoid having a reference to official currencies based on DLT. This issue is therefore of particular importance.

Security tokens

Security tokens as a future "shell" for securities. As part of the description of the ecosystem surrounding the token economy and the tokenisation of valuables, so-called "security tokens" are mentioned in the German government's questionnaire. Security token offerings (STOs) have emerged from ICOs and form the basis for the mapping of securities in the future. Based on the current application possibilities and characteristics of the token types, we assume that, in addition to "pegged payment tokens" (ITC class EEP21P), e.g. in the form of euro-on-ledger, security tokens (ITC class EEP23) in particular will dominate the market in the next 5-10 years. This field should therefore be given special weight in the legislative process. A key outcome of security tokens will be a significant reduction in setup costs for placing securities on the capital market.

Notation of security tokens on carrier platforms. The main distinguishing feature between utility tokens (ITC class EEP22) and security tokens is the fact that a legally recognised capital market construct is represented by a token within the framework of security tokens. Crypto assets such as Ethereum or EOS can become an efficient carrier platform for securities. On the basis of these, security tokens are then "installed" through the use of smart contracts, for example, which can represent securities in a legally compliant manner (in particular with regard to money-laundering guidelines) – even if the underlying carrier platform is a cryptocurrency such as Ethereum. The central advantages of DLTs are also apparent in the field of security tokens. Security tokens can be transferred freely (also internationally), enable lower setup costs, generate only low transaction costs, can basically be programmed arbitrarily, and improve the power of disposal over the tokens to the extent that, for example, they can be decoupled from a stock exchange to a digital terminal device. In addition, token transactions are tamper-proof and automated to a high degree through the integration of smart contracts. Conversely, this shows a hidden problem, namely incomplete regulation. A regulated company, such as a bank, could not issue legally compliant tokens because the block-chains could not be aligned with the basic IT (BAIT) requirements. The risks from IT implementation must be included in the technical requirements of the regulator in order to create a level playing field.

Abstract instead of specific regulation. In February 2018, BaFin issued a letter of advice on the regulatory classification of the tokens and crypto currencies relevant for ICOs. In the course of this analysis, we recommend consideration of the specific properties of STOs, but we also point out that no explicit classification of tokens is required for efficient and objectively based legislation. The right represented by a token is of crucial importance (e.g. various securities laws) when specific basic token regulations are enacted that concern "digital handling", i.e. ownership, possession, theft, etc. In this case the token would be a container for other rights with existing rules. Based on this the container itself has to be regulated on an abstract and general basis. Since tokens can be used very flexibly, the application types for tokens will increasingly reach areas that are still unknown to us today. Against this background, a regulation based on specific token types is not effective (as explained above), as it would be inflexible, fragmented and would conflict with other specific regulations. Instead, the container model proposed in Liechtenstein should be analysed in order to regulate the connection of the "real world" to digital infrastructures in a generally valid and abstract

way.

European Union as the desired level for regulation. National initiatives should not replicate the kind of regulatory fragmentation in Europe that characterises the traditional financial system. With the capital markets union, the EU has launched a comprehensive initiative aiming at strengthening the European single market and, above all, the cross-border allocation of capital. This ambitious project has only achieved limited success so far due to the strongly diverging national legal regimes and the national market structures that are based on these. In the area of crypto assets, no market structures demarcated by national borders have yet been established that could disrupt the allocation of capital in the single market.

Priority for European initiatives. Where national initiatives cannot be avoided, they should be aimed at the creation of a single European market. A new technology can also be an opportunity to initiate overdue regulatory reforms that are blocked by national special interests.

Digital mapping of securities. A reorientation of securities regulations should fully exploit the specific advantages of digital technologies. Digital mapping of securities, especially in conjunction with blockchain technology, allows real-time representations of a company's shareholder structure. This offers unprecedented opportunities for transparency initiatives of all kinds. Moreover, such real-time transparency can enable more efficient forms of corporate governance and help to avoid manipulation and the need for investor compensation.

Blockchain technology and the General Data Protection Regulation (GDPR)

Open questions due to the irreversibility of blockchain transactions. Under the current requirements of the General Data Protection Regulation (GDPR) and the national Federal Data Protection Act, data protection law and blockchain technology are not compatible, at least in most cases. One of the basic properties of the blockchain is that it is unchangeable and "plaintext" (i.e. publicly visible transaction data that may be pseudonymous). On one hand, full compliance with the rights of data subjects under the GDPR is normally unlikely to be possible in the case of public chains. Depending on whether the data is collected directly from the data subjects or not, the information listed in Article 13 or Article 14 of the GDPR must be communicated to the data subjects. This is likely to pose considerable practical challenges, including simply communicating the names and contact details of the controller as defined in the GDPR, apart from anything else. Normally, a public blockchain is set up on a purely decentralised basis, i.e. it has no controller.

Difficulty with disclosure of data sets. In particular, the GDPR grants data subjects rights with respect to disclosure, amendment, deletion, correction, restriction of processing, data transferability and, if applicable, objecting to the processing of their data. It is not yet clear how these rights will be safeguarded in view of the immutability and permanent storage of the data stored in the blockchain. In the context of the usual blockchain applications, it is simply not possible, for example, to satisfy the rights of data subjects with respect to deletion and correction. Adjustments of the blockchain are possible, but these contradict the original approach, because they require central units besides the blockchain and/or further assumptions have to be made about the trustworthiness of the partners. Currently, discussions are being held on approaches that involve storing transaction hash values instead of transaction data, using the keys (i.e. the personal nature of the data record) only as

references to other keys, so that their connection can be deleted, or forming time slices from the blockchain. All these methods strongly change the characteristics of the blockchain but can probably only be used constructively in very special cases. This is the case, for example, when an entity is sufficiently trusted to carry out eliminations centrally or distributed on a limited basis but is not trusted enough to carry out transactions centrally.

Waiver of rights not possible. It is impossible to contractually waive the rights of the data subjects. This is legally not possible, because a waiver of the data protection rights is simply invalid under the given rules.

Clarification of the operator question. Detailed further analyses seem necessary in this respect in order to be able to map the requirements of the GDPR in blockchains. In addition, the GDPR would have to be adapted in such a way that it also takes into account systems without an operator (or with an operator that cannot be recorded), as is the case with public blockchains. This has not yet been the case in the previous legislative process with regard to data protection matters.

Smart contracts and legal contracts

Smart contracts for the automation of legal obligations. A further development stage within the token economy are so-called “smart contracts”. Smart contracts are computer programs for the automated execution of contractual or legal obligations. In addition to contractual conditions, these include the automatic transfer of tokens in accordance with the contract. This enables permanent control and exhibits large potential for automation. The German government argues that the use of smart contracts can optimise applications in various areas by reducing costs and transaction times, e.g. in the energy sector.

The difference between smart contracts and contracts in the legal sense. First of all, the distinction between a smart contract and a contract in the legal sense is essential: a contract in the legal sense is a legal commitment of the parties to declarations of intent expressed by them. When interpreting the content of the declarations of intent and thus the contract, all circumstances of the individual case are taken into account. The legal obligation manifests itself in the official enforcement of the corresponding details of the contract. A smart contract is not a contract in the legal sense; at best, it can accurately represent a legal contract. After all, a smart contract is inevitably limited to the corresponding computer code. An overall assessment of all circumstances of the individual case to determine the “correct” consequences is unimaginable, even taking into account all currently realistic artificial intelligence (AI) solutions.

Trustworthy smart contracts in a technological process. Smart contracts are of greatest importance when it comes to contract execution: So-called “if-then conditions” in a contract can be automated, leading to a guaranteed execution. Smart contracts were therefore correctly defined in the 1990s as digital versions of a vending machine. Similar to a traditional (functional and unmanipulated) vending machine, a smart contract addresses the counterparty risk, in this case, the buyer’s ability and willingness to pay. Trust is replaced by a technical process. However, the result of this technical process is not necessarily “legally correct”. The German government should analyse this topic separately.

Smart contracts' ability to function as legal offers and acceptance. Despite the focus on contract execution and the fact that a distinction has to be made between legal contracts and smart contracts, the use of smart contracts can create legal liabilities and contracts. The use of a smart contract may constitute an offer, depending on the form in which it is used in individual cases; the payment into a smart contract may constitute acceptance. The conclusion of a legal contract conclusion is not limited to a certain form and can take place in principle in any language, including a programming language like Solidity, for example.

Consumer protection is the top priority. The use of programming languages to define contractual obligations gives rise to problems, however: Important information can be lost during the preparation of contracts. In addition, the corresponding smart contracts are often more difficult to read than standard contracts after they have been created. In this case, issuers and service providers should be responsible for the smart contracts that are issued.

Unlawful interference with another party's possessions and the state monopoly on the use of force. In any case, it must be ensured that smart contracts are not used to enforce consequences against consumers and other contracting parties who are typically in a weaker negotiating position, such as tenants, travelers or patients, that would otherwise be clearly prohibited. In particular, the prohibition on unlawful interference with another party's possessions (*verbotene Eigenmacht*) must be observed so that the state monopoly on the use of force remains unaffected. In individual cases, differentiating between recognised prepaid models and disruption of ownership could prove challenging.

Conflict between law enforcement and decentralised blockchain systems. Similarly, the decentralised and transnational nature of public blockchain systems creates a problem when a court orders that the text of a contract must be interpreted differently than how a machine would interpret it. Such a change is not provided for and, in case of doubt, requires a fundamental change in the underlying blockchain, as happened with "The DAO". It is likely to be difficult to enforce this in all jurisdictions due to the multiple interdependencies in DLT systems. Issuers and service providers are also liable for errors caused by the technology used.

Formal requirements as a limitation of the use of smart contracts. The general possibility of concluding contracts in any language and in any manner does not mean that all contracts can be legally concluded in this way. Some businesses require a specific form. This applies, for example, to the transfer of real estate or company shares as well as to the granting of certain powers of attorney. In some cases, there are mandatory requirements for the physical representation of assets. This applies, for example, to securities. In this respect, the law currently limits the use of smart contracts. The German government's initiative on the regulatory treatment of electronic securities is a first important step towards reducing legal barriers to innovation and should be used as an incentive to carry out an evaluation regarding the question of in which areas the relevant formal requirements should be replaced by technology-neutral supervisory law.

Complexity of smart contracts. The conditions to which a disbursement or another sequence is linked can be extended at will. These enhancements can make the contracts highly granular and lead to corresponding consequences with a high degree of accuracy. It is absolutely not possible for smart contracts to replace jurisdiction. A subsequent correction of the results must always remain possible. This is only possible on public blockchain systems if programmers of public blockchain systems or the authors of smart contracts have anticipated this and prepared the program code accordingly. Issuers and service providers should be liable for the program code (e.g. smart contracts, custody solutions) they place on the market.

Security and reliability of blockchain systems

Stability of blockchain systems based on game theory. Even in the case of private blockchains, the system reliability requirements (for example, BAIT compliance for banks) can still be imposed on the operator or operators, this is not the case with public blockchains. Although tough integrity and reliability are the goal of blockchain infrastructure, it needs to be acknowledged that integrity and reliability are mainly ensured on the basis of game theory. This means that its operational reliability is dynamic in nature and is the stochastic result of given probabilities (e.g. concerning the finality of transactions). That is why Satoshi Nakamoto started Bitcoin as an experiment. If the computing power is distributed unfavorably in the open system, the blockchain can be compromised (e.g., 51% attack on Bitcoin Gold). If no operator is interested in running a public blockchain any longer, it will effectively cease to exist. Today, approximately 1,000 blockchain systems have become inactive, following highly euphoric beginnings in many cases.

Conflict between uncontrolled reliability and regulated economic sectors. The reliability of a public blockchain is therefore subject to dynamic changes and cannot be controlled. This is likely to be contrary to most applications in regulated economic sectors (e.g. investor protection). Here, research is still needed before the result of the experiment (namely applicability) can be evaluated in all aspects. The issuers and service providers must be held accountable in this context too.

Requirements for IT security. For the secure operation of a DLT, it must be ensured that the private keys are securely stored in one (digital) location. They must, on the one hand, be protected against data loss and, on the other hand, be protected against misuse by means of encryption. When clarifying the application architecture, it must be taken into account that many DLTs, especially blockchains, currently do not provide adequate security with a view to quantum computers. Accordingly, there is a real risk that DLTs could be attacked by third parties in the medium term and that all data could be decrypted.

General regulation of tokens

Cross-border processes. The use of DLT must be regulated at an international level since the rights represented by tokens are not necessarily tied to physical ownership within geographical borders. For example, associations of states such as the European Union could form a single authority responsible for the classification and monitoring of tokens. As an international network, these organisations could then constitute a worldwide expert body to carry out the economic use and political regulation of tokens without geographical restrictions. An international consensus for the regulation of DLT would not only promote innovation in this area but could also be a valuable starting point for a general political dialogue. For Germany and all other countries of the European Union, we believe that the EU offers an optimal starting point for formulating efficient regulation. Irrespective of the above, the rights embodied in a token can be designed and implemented at the respective national level, as it is currently the case with the interaction of European Union legislation and national

legislation. However, this perspective implies that the German government should focus mainly on the area of cross-border token transfers.

Tokens as a point of contact for regulation. In addition, the essential characteristics relating to the lawful possession of a token and the respective relationship between the token and the law applicable in the particular situation should be defined in legislation. The digital transfer of tokens should be another focus of the legal framework. A transfer of tokens between possible blockchain/DLT systems should also be considered. Regulations and procedures with regard to undesirable criminal activities should also be addressed. A good starting point for this is, for example, the application of anti-money-laundering and anti-terrorist financing regulations in the context of tokens, which the German government has already called for. Legislation at the token level and not with respect to a specific blockchain/DLT is also proving to be advantageous in other countries, since all possible applications can be captured in broad-based abstract legislation and comprehensively represented in legal terms. Consequently, the state should also regulate the service providers who interact with tokens (e.g. in terms of trading, generation, custody) through appropriate licensing and registration, and set requirements for the appropriate blockchain/DLT infrastructure to be used. In this case, certification in separate areas is presumably not required.

Further relevant aspects

Central Europe is among the leaders in the area of blockchain. Within Europe, a successful development of the DLT landscape can be observed in particular in the Baltic states, Germany, Austria, Switzerland, and Liechtenstein. In addition to the legal design of possible regulations, education represents a second decisive factor in terms of a successful future with DLTs.

High importance for education. Future-proof and scalable DLT innovations require solid education in information technology, digital technology, and programming. Therefore, we recommend providing comprehensive support, including the development of a strategy, in the area of education with regard to DLTs in particular, but also digital technology in general; this could be restricted to the relevant occupational fields, but be open to all age groups. Related areas, which until now have only been of niche significance, are also important in this context (e.g. interface between computer science and law, interface between computer science and engineering).

Importance of the private sector for the operation of DLT systems. Due to the highly dynamic nature of the market, we do not consider it appropriate for a government or the European Union to position itself as the sole operator of a DLT infrastructure. The regulation of service providers is enormously important since the market will ultimately define sustainable concepts through supply and demand. Therefore, control is only possible indirectly via legislation. It could also be advantageous for state authorities to operate computing nodes in DLT systems, e.g. to enable real-time analysis and to automate reporting to the authorities.

Differentiation between DLT systems and databases. In contrast to expert opinions cited by the German government, blockchain systems do not aim to replace conventional database systems in any way. Instead, DLT systems will complement the current database systems. In principle, the German government should clarify this in the definition of terms used in its questionnaire and in the blockchain

strategy based on the questionnaire.

Electricity consumption of public blockchain systems. An essential feature of some crypto assets, which has been the subject of criticism, is the enormous power consumption caused by the proof-of-work (PoW) consensus algorithm. Although this cannot be changed in the short term, it only affects crypto assets and tokens issued, and applications implemented, on public blockchains with a PoW consensus algorithm, and hence does not affect all approaches by far. The German government should make it clear in its questionnaire that DLT and blockchain systems can fundamentally be operated with low power consumption, e.g. if consensus algorithms such as proof-of-stake (PoS) or proof-of-authority (PoA), which is relevant for critical infrastructure, are used.

Possibility of direct government intervention in DLT protocols and smart contracts. With regard to the intended regulation, we would also like to raise concerns that the legal framework does not necessarily have to be formulated from an external perspective in all aspects. It is conceivable that the state will in future implement its regulations (e.g. in the area of taxation) directly in the protocols of blockchain systems. This option should not be dogmatically excluded; on the contrary, for reasons relating to a level playing field, this could even be implemented in the protocols as a mandatory requirement, given that banks are also required to remit capital gains tax (now even on a transnational basis due to FATCA).

Elections as application of blockchain technology. Government processes, such as elections (e.g. federal elections, state elections, local elections) and resolutions can also be tokenised and mapped. In addition to public elections, this also applies to votes in companies (e.g. general meetings, corporate actions), associations or other entities seeking consensus. It is hardly possible to manipulate votes through the use of the technology, which practically rules out electoral fraud. Appropriate technical DLT protocols could enable the media, public initiatives and other voters to follow decision-making processes in close detail. In addition, election results could be calculated accurately and on an ad-hoc basis, while at the same time reducing administrative and organisational costs enormously. Therefore, the German government should examine this complex scenario in the context of its blockchain strategy. With regard to anonymous elections there are, however, already concepts worth considering that do not involve blockchain.

Conclusion

Technology-neutral regulation. There should be no “Lex Blockchain”, as the position paper already states. The laws should set out requirements in a technology-neutral way. The obstacle for technical progress (also for blockchain) is mostly that the technologies of “paper, signature, and identity card” are assumed to be mandatory for the requirements of possession, declaration of intent and identification. Especially for blockchain, the requirements for reliability of the system and for possibilities for the regulator to intervene must be defined in a technology-neutral way.

Taking account of dynamic change. It is clear how immature blockchain technology is at present, but it is also clear how rapidly development is currently taking place. At the current time, there is no longer a single definitive blockchain or blockchain technology. The blanket term covers quite different operator models (public versus private) and quite different concepts (from proof-of-

work consensus blockchains, to “blockchain inspired” tools such as R3 Corda or similar, to newer distributed ledger technologies, e.g. based on directed acyclic graphs). Since a legally binding definition of blockchain is not possible given ongoing developments, regulation or legislation should always be neutral with regard to all technologies that can be used in a particular application context.

New research projects and sufficient budget. In our opinion, it would therefore be extremely advantageous to initiate research projects in Germany or the EU in which, among other things, analysis is carried out regarding how a blockchain that complies with existing regulations can be designed. This is not yet the focus of technical developments. While banks invest more than half of their IT budgets in regulatory adaptations, probably little has been invested in this context with regard to blockchain. In the course of the project, it would also be possible to see where the technology can adapt to the regulatory requirements and where, conversely, the regulatory requirements have to be adapted to the new technology because the requirements are formulated too specifically. Relevant specific questions would also address, for example, the quality parameters and safety levels of blockchain systems or an assessment of the reliability of blockchain systems. The studies currently being carried out on blockchain technology by the Federal Office for Information Security are also worthy of note in this context.

Enormous potential with significant risk. The entire technical ecosystem around DLT and blockchain is characterised by a high degree of modularity and flexibility with regard to tokenisation. Therefore, it is difficult to estimate all possible effects on the basis of today’s knowledge. Nevertheless, legislation that is efficient, future-oriented, and (by necessity) cross-border can lead to a significant strengthening of innovative capacity. The digital mapping of rights and identities, combined with modular legislation, can find numerous positive applications in various areas of the economy. However, it must be borne in mind that the digital systems do not simply digitise documents; instead, they have completely different characteristics: identical copies cause difficulties, public blockchains in particular are decentralised, transnational infrastructures elude judicial access, coded contracts are interpreted differently by machines than humans intended, corrections are barely possible (even if a court order exists), and data protection can only be achieved by workarounds that call into question the original intention behind the system. Ten years have passed since the appearance of Bitcoin, the first application of blockchain technology. An intensive assessment by legislators is overdue in order to determine the potential of the technology. At the same time, the implementation requires enormous care and the possibility of correction, since the technology is fundamentally different from the existing system of national statutory regulations.

Berlin, 27 March 2019