bankenverband

Discussion paper

of the Association of German Banks on the use of distributed ledger technology (DLT) for securities transactions – legal considerations and proposals for reform

11 March 2019

This is a convenience translation only. In case of doubt, please see the original German version.

Bundesverband deutscher Banken e. V.
Burgstraße 28
10178 Berlin
Telefon: +49 30 1663-0
Telefax: +49 30 1663-1399
www.bankenverband.de
USt.-IdNr. DE201591882

Possible reforms to enable securities transactions to be carried out using distributed ledger technology (DLT)

The continuing development of new technologies will in future enable conventional (German) securities to be issued in forms other than certificates. Should these new technologies be used in securities issues, this may also lead to changes in the processes involved in the custody and settlement of securities, as well as in corporate actions and, possibly, securities trading. This, in turn, may make it necessary to adjust civil law and regulatory requirements at national and European level since the use of a new technology or procedure will change the business processes which formed the basis for the development of certain rules and regulations by lawmakers.

Any reform of supervisory or civil law should be guided by the **principle of technology neutrality**. The aim should be to create a harmonised regime and thus a level playing field for issuing securities where certificate-based issues can be on an equal footing with non-certificate-based securities issued using, for instance, a distributed ledger technology such as blockchain or a similar alternative. The legal classification of, and basic rules governing securities are laid down in **national** (civil) **law**. In any discussion about possible uses of DLT for securities transactions, national jurisdictions are therefore **in competition** with one another. This applies both to the legal systems of EU member states in relation to each other and to the legal systems of third countries.

This discussion paper will focus primarily on the issuance, custody and settlement of securities using distributed ledgers where claims on an issuer are established in closed or open networks, such as the internet, with subsequent decentralised storage of data related to the issue (and possibly the coding of contract components by means of so-called “smart contracts”).

The legal framework governing securities issues in distributed ledgers will be examined in this paper. The terms “DLT” and “blockchain” are used synonymously although blockchain is only one of several technical methods of creating and maintaining a distributed register.

Our analysis concentrates solely on distributed ledgers that operate in a restricted (or “permissioned”) network since the Association of German Banks considers this the only way to ensure transparent accountability for full compliance with the regulatory requirements governing securities (such as reporting, KYC identification or anti-money laundering (AML) requirements). Open, public (“permissionless”) networks are outside the scope of this paper.

A. Technical background

Starting point

The digitally distributed ledger

Distributed ledger technology (DLT) enables an authoritative record to be made of business processes even if the parties involved do not know each other but rely on mathematically verifiable information. This is made possible by networked computers reaching a consensus on the sequence in which transactions have been carried out and updated. Each computer in the network holds a copy of all entries relating to all transactions, so that the entire ledger is available on all networked computers. For this reason, the system is referred to as a "distributed ledger". Technically speaking, DLT thus enables the secure transmission not only of information, but also of assets. From a purely technical point of view, therefore, it would be possible to dispense with the intermediaries which have up to now played an essential role in securities transactions, for example, in order to ensure confidence in the system. DLT consequently opens up completely new possibilities for end-to-end digitisation of asset and trust-based business processes, thus making them more efficient.

Technology such as blockchain is commonly perceived to be closely linked to bitcoin, but this perception is already outdated because the technology has developed very dynamically. Bitcoin was merely the first (high-profile) application in 2009. There are now a number of other DLT strategies for a whole host of possible applications of the technology (ranging in the financial sector, for example, from trade financing to processing corporate actions and securities settlement in its entirety).

The various versions of DLT, the so-called frameworks (such as Corda and Hyperledger), can be used to construct an architecture tailored to the desired individual application. A higher transaction speed can be achieved by reducing the degree of distribution, for example. The expression "DLT" is therefore a generic term similar to "database", while "blockchain" represents a technical subcategory. Depending on the exact requirements, the concrete application should be configured in an architecture best suited to it. It is important to bear in mind that the diversity of possible solutions allows a very broad range of applications: use of the technology should not be reduced to a few popular niche areas.

Although public networks lend themselves to a number of different applications, our discussion paper focuses on restricted or private networks which can only be accessed by a limited number of participants (meeting a defined set of criteria). In view of the existing regulatory framework, we believe these networks are best suited to the digitisation or tokenisation of securities. A true public network, as we see it, is one in which anyone who has access to the software can participate without the need for registration or identity verification. For processes involving the transfer of securities or payments, at least a parallel register for verifying the identity of the

parties would be required in order to ensure compliance with legal requirements (e.g. for preventing money laundering and terrorist financing). We consider the maintenance of parallel registers less secure than an integrated system, however. On top of that, there would be a lack of clarity concerning the responsibilities of those involved.

I. DLT – origin and mode of operation

Origin of DLT

"Blockchain" became known as the technology behind the cryptocurrency bitcoin. But although bitcoin pioneered the use of DLT, the potential of the new technology goes far beyond this one application. If you compare blockchain as a basic technology with the internet, for example, email was the first application of the internet. And though this application is still highly relevant, considerably more applications exist today and more still are conceivable in the future.
The catchy name "blockchain" is made up of two components:

1. The **bundling together** of transactions into **blocks**. The intention is to enable transactions, owing to this bundling, to be verified more effectively.
2. The **linear** arrangement of transactions in a **chain**. This makes it easy to trace the chronology of the transactions. With the help of this chronology, it is possible to analyse whether the transactions are valid and reach a clear conclusion. This prevents situations where, for example, an asset is first transferred to one party and then transferred again in error to another party. Only the party last recorded as receiving the asset is in a position to forward it on.

Historical example: bitcoin

Bitcoin has both attributes of blockchain: transactions are bundled in 1MB-sized packets of data into blocks and then verified by means of a mathematical problem. The difficulty of the problem is continuously adjusted in such a way that a problem can only be solved by a computer once every 10 minutes. As competition for the verification of a block increases, the amount of the computing power required rises, as does the amount of electricity consumed, though this applies only to the so-called "proof of work (PoW)" consensus algorithm used here for bitcoin. There are two aspects to the reward:

1. A fixed number of new bitcoins are issued (currently 12.5) for solving the problem. The amount of new bitcoins issued per block is halved step by step at certain points in time (the next time will be in 2020). The process of acquiring new bitcoins by verifying a new block (solving a mathematical problem) is called "mining", the verifying nodes are known as "miners".
2. If a user wants a transaction to be prioritised and processed more quickly, they can attach a transaction fee (bitcoins that have already been issued). Owing to the rule that a new block can only be created every 10 minutes, approximately seven transactions per second are possible. The number of desired transactions is already generating a backlog.

Miners therefore give priority when including transactions in their next block to those which will pay a transaction fee.

The reason why such considerable effort is necessary when mining bitcoin is that the algorithm selected for reaching a consensus requires virtually no confidence in institutions or third parties, but only in cryptography, i.e. the technology behind the mathematical problem and the public/private key methods used.

Bitcoin was originally conceived as an alternative currency and therefore also a means of payment, even for small amounts. Given the high transaction costs, however, this seems unrealistic. Since the speed of transactions is constant, transaction fees fluctuate greatly depending on the transaction volume. In 2018, for example, the average cost per transaction fluctuated between around USD 0.05 and USD 8.52. Unless the bitcoin network changes its underlying rules, bitcoin is likely to remain unattractive as a widespread means of payment, although some niche uses certainly exist, such as in the area of international payments.

From blockchain to distributed ledger technologies (DLTs)

Further alternative architectures have evolved which, strictly speaking, can no longer be called blockchain.

1. **No blocks, but linear chains**: the efficiency of the block concept depends on the amount of effort needed to verify a transaction. If a verification method is selected which is not time-consuming and costly, individual transactions can also be verified efficiently without having to bundle them into blocks. This architecture was used, for example, when building Corda, the open source platform of the financial consortium/start-up R3.
2. **Blocks, but no chain**: this combination is almost non-existent, since technologies with non-linear chains (directed acyclic graphs) do not need to build blocks.
3. **Neither blocks, nor linear chains**: this approach is used especially in newer, more innovative solutions. Since verification is mathematically more efficient, blocks are no longer needed. In addition, an acyclic (i.e. non-linear) chain called a directed acyclic graph is used.

The features which gave their name to blockchain are therefore no longer prerequisites for constructing a distributed ledger. Nevertheless, some types of the new technology are often still referred to as blockchain even when they use neither blocks nor chains. The distinguishing characteristics of DLT are as follows:

Distributed systems: DLT solutions are distributed systems. The systems are distributed in that the data set of all transactions – or at least an extract thereof – is spread across more than one central database (i.e. across so-called nodes). Conventional systems, such as a land register, operate largely with central databases (single point of trust/truth). Unlike central databases, distributed systems are able to systematically exclude inaccurate entries of data from the outset because the protective mechanism of verifying that transactions are correct and

legitimate is built into the technology itself, whereas conventional central systems have to establish separate protective mechanisms. The DLT mechanism does not guarantee the accuracy of the data themselves, but ensures that the transferred data are correctly entered and maintained. Since the quality of the data depends on the data source, the point of trust shifts away from the intermediary to the source of the data.

There is a strong correlation between the transparency of the network, the consensus mechanism used and the level of trust between participants. There are architectures in which there is little trust between participants. In this case, a high degree of transparency is necessary so that a consensus can be reached by means of the predefined majority. This also means that the data stored in the distributed ledger is visible throughout the network. Other architectures, by contrast, aim to ensure that the trust among participants or in the service provider of a purely technical infrastructure (e.g. a regulated company) is great enough to be able to dispense with a complex consensus mechanism for transactions and use heuristic, statistical methods instead (e.g. a technical service to classify and verify transactions). There is no need, in this case, for all data to be accessible throughout the network: a so-called private-channel architecture can limit access to the parties involved in a transaction. This means that all transaction data for a particular transaction are only visible to the specific parties involved, while for all other parties they remain abstract data. Sensitive data, such as those for securities transactions, could be pseudonymised and could only be accessed in full by the parties themselves – and, if necessary, by supervisors.

II. Comparison of platforms

When it comes to possible applications of DLT in the financial sector, several different platforms (or frameworks) would lend themselves to the implementation of different applications. This section describes the three currently most important, namely Hyperledger Fabric, R3 Corda (hereafter "Hyperledger" and "Corda" respectively) and Ethereum. A comparison of the three will show what design possibilities each platform offers. Though these DLT solutions are frequently referred to as blockchain frameworks, they lack the characteristics that gave blockchain its name.

Since the frameworks are still at an early stage of development, however, there are likely to be far-reaching innovations and changes which cannot be anticipated at this stage. It is also important to bear in mind that almost all relevant frameworks are being developed as open source projects, meaning every developer can propose changes, which will then be accepted or rejected by the developer community.

The white papers of Hyperledger, Corda and Ethereum show that these frameworks evolved from sometimes very different visions of possible applications. The development of Corda and

Hyperledger is driven by a vision of specific applications. Hyperledger sees itself as a modular platform with an architecture that can cover different industries and applications. It thus resembles a sort of building block set for the construction of tailored applications. These could be used in sectors such as banking, healthcare and supply chain management, to name but three. The Ethereum platform is not designed with specific application areas in mind. In contrast to the modular approach of Hyperledger, the focus is on providing a generic basis for a large number of different applications. This will allow the development of virtually any application.

Characteristics	**Ethereum**	**Hyperledger**	**Corda**
Type of platform	Generic DLT platform	Modular DLT platform	Specialised DLT platform for the financial industry
Host	Developers	Linux Foundation	R3
Access	Free access, public or private	Restricted access, private	Restricted access, private
Consensus reaching process	Mining based on proof of work, ledger level	Various methods of reaching a consensus allowed, transaction level	Specific method of reaching a consensus ("notary nodes"), transaction level
Smart contracts	Smart contract codes (e.g. Solidity)	Smart contract codes (e.g. Go, Java)	Smart contract codes (e.g. Kotlin, Java)
Currency	Ether	None	None

(Table compiled in cooperation with the Frankfurt School of Finance and Management.)

Access: to obtain a clear idea of the possibilities and limitations of each framework, it is important to first consider its mode of operation since this is key to the process of reaching a consensus. A basic distinction needs to be made between free (or permissionless) and restricted (or permissioned) access. If access is free, any user can join the network and participate in it. This is generally true of the public Ethereum platform. If access is restricted, only participants designated in advance (so-called nodes) are entitled to access the network, as with Hyperledger and Corda. But Ethereum-based solutions can also be developed using a permissioned approach (e.g. quorum) since Ethereum does not exclude the possibility of building permissioned network infrastructures. These different methods of permitting access also give rise to the need for different ways of reaching a consensus.

It is important to realise, however, that free and restricted participation in a network are only the conceptual poles of a continuum. At operational level, further distinctions need to be made

between reading and writing rights and with regard to the number of nodes. One conceivable approach would be to allow a small number of authorised participants to write transactions into the ledger and a larger number of authorised participants to read transactions. This would not make the ledger of transactions public, but access would be differentiated. An approach of this kind could be used to process securities transactions, for example. Such a system could be administered by a number of authorised nodes, one of which could be created for regulators, who would have only reading, but not writing rights, however.

Reaching a consensus: on the Ethereum platform, all participants have to reach a consensus about the sequence of all transactions, regardless of whether or not they are involved in the transaction in question. This is currently achieved by means of mining based on a proof-of-work (PoW) protocol. This has an adverse effect on the efficiency of processing transactions, however. On top of that, all participants are entitled to view all data points in the distributed ledger. Despite the anonymization or pseudonymisation of data, this poses a significant problem, especially for applications which need to comply with strict data protection requirements.

Hyperledger and Corda solve this problem by restricting access rights to the network. Both platforms enable the access rights of individual categories of participants to be designed in a variety of ways. Hyperledger differentiates between "client", "peer", "endorser" and "orderer" nodes in the process of reaching a consensus. Consensus on the Corda platform is reached by verifying the validity and uniqueness of a transaction, with designated nodes known as notary nodes responsible for consensus on the uniqueness criterion. Both frameworks thus make it possible to define the parties to be involved in reaching a consensus and to limit the access rights of participants to certain transactions. This also results in a better scalability of the network.

Smart contracts: all three DLT platforms provide for the development of smart contract code. This means using software written in certain programming languages to automate the exercise of predefined rights and obligations. An asset can then be transferred in the distributed register automatically, for example. Smart contract code can be written in Go or Java for Hyperledger, Solidity for Ethereum, and Cotlin or Java for Corda. The main difference between the frameworks, however, lies in the ability to include legal phrases. The coding can then also contain legal text. The provision of smart contracts of this kind by Corda, for example, can be explained by the platform's focus on highly regulated areas of application, such as the financial industry.

Currency: the frameworks also differ with respect to currency. On the Ethereum platform, the integrated cryptocurrency Ether is used to compensate nodes involved in reaching a consensus and to pay transaction fees. This makes it possible to develop applications which involve payment transactions. It is also possible for participants to create their own cryptocurrencies and cryptoassets with the help of standardised smart contracts. Unlike Ethereum, Hyperledger and Corda do not achieve consensus through mining, so these platforms do not require an integrated

currency. But while it is nevertheless possible in principle to develop a cryptocurrency or token in Hyperledger, Corda does not provide for this at all. To process transactions in the public Ethereum network, Ether would need to be acquired, held and used.

For transactions that have to be settled with central bank money (e.g. securities transactions denominated in euros) or should be settled with central bank money (to avoid exchange rate risk, for instance), there is still no way of directly including real central bank money in DLT transactions, as it is neither integrated into DLT systems nor available for this purpose. But there are already solutions, developed by some of our members, for instance, which are based on commercial bank money. These payment claims are also known as "cash on ledger". Although smart contracts cannot yet execute transactions in central bank money, the ability to use commercial money makes their use perfectly feasible. To enable high-volume business to be settled automatically using DLT, cash-on-ledger continues to be a key issue and requires further development.

III. Examples of applications for securities

Securities issues and securities-related services

The use of DLT for securities settlement could bring about fundamental changes in the processing landscape. A sine qua non, however, is that it is legally as well as technically possible to issue and transfer securities using DLT. As explained below in parts B and C, this does not necessarily require a radical overhaul of regulatory requirements. On the contrary: the regulatory regime only needs to be changed in areas where the new DLT processes make existing requirements unnecessary or pointless. What is more, DLT could also be used to implement new regulatory requirements.

DLT thus offers the potential for new applications in the area of securities. These could make existing processes more efficient and also make processes possible that do not yet exist or currently need to be handled manually. They include, for example:

- The exercise of voting rights by shareholders and proxies
- Shareholder identification – a need for digital solutions could arise particularly in connection with the requirements for identifying shareholders under the Shareholders' Rights Directive.
- Corporate actions – DLT also offers considerable potential for improving processes associated with corporate actions, be they processes for carrying out the corporate action itself or for accessing information relevant to a corporate action (e.g. acting as a "golden source" of information). Here, too, the Shareholders' Rights Directive sets EU-wide requirements concerning information on general meetings; DLT could potentially be used to implement these requirements.

- Other instruments which currently require a lot of manual processing but which are similar to securities in many ways (e.g. promissory note loans) could also benefit from the development of the new technology.
- The same applies to procedures which are directly related to securities transactions and still largely require manual processing (e.g. withholding tax rebates).

Task sharing in a distributed ledger with restricted access

Distributed registers are conceivable in which a consortium of participants meeting certain criteria create and operate a common network. Participants joining the network at a later date would also have to meet these criteria. This would allow securities to be created and transferred in a private, permissioned or restricted network. The software for the distributed ledger would be provided and maintained by the consortium. Each party would operate a node in the network. Some nodes could just have public keys, which would give them access to the network and the associated reading rights. Other participants could also have private keys, which they could use to sign transactions, i.e. they would have writing rights.

Issuers of securities could either issue their securities themselves as participants in the network or have them issued via a network gatekeeper, depending on whether or not additional securities-related services outside the network were desired or required.

The gatekeeper would serve as a bridge to the distributed ledger: it could handle the technical recording of transfers of assets registered in the ledger while pricing, for instance, could take place elsewhere (e.g. on a trading platform). The gatekeeper would thus act as the interface with the user (e.g. an investor or issuer) or with other participants (such as stock exchanges, central banks, etc.).

To ensure compliance with regulatory requirements, participants and gatekeepers should be limited to regulated institutions/firms (with writing rights) and government agencies (with reading rights).

B. Legal considerations

The civil law framework governing securities is determined by a country's national law. In contrast to the **supervisory law** governing securities, there is as yet no harmonised, EU-wide **civil law** regime for securities. This means the conditions for issuing and transferring securities in Germany have to be sought in German civil law, which is in competition with other national legal systems.

A key prerequisite for the success of DLT securities systems in Germany and Europe is future **legal certainty** surrounding recordings of transactions. In other words, the issuance, custody and settlement of securities in DLT systems must be recognised as being legally effective. This includes, in particular, legal protection of bona fide transactions, meaning there must be rules that protect an honest purchaser of securities.

DLT securities systems are not projects limited to one particular country, but will normally have a cross-border dimension. The principles of **national civil law** in this area therefore need, as far as possible, to be **recognised in other jurisdictions**. **Supervisory legislation**, by contrast, should as far as possible be developed at **EU level**, either as directly applicable law (regulations) or as a set of binding standards and requirements to be transposed into national law (directives). As in all areas, it is essential to avoid regulatory arbitrage here too.

Below, we will begin by analysing the implications of civil law in Germany for the application of DLT to securities. The legal obstacles will be highlighted and proposals outlined for overcoming them. A subsequent section will then consider securities using DLT from the perspective of supervisory law.

I. Civil law

To avoid hampering the development of technical innovations in Germany and to take account of international developments, the existing law should be adjusted. It should be borne in mind, in the course of doing so, that even today securities do not always take the form of physical certificates. German law recognises foreign instruments, such as dematerialised securities, as securities, just as it defines contractual claims/securities entitlements as securities in certain special laws.

We describe below (1) which provisions of existing law seem incompatible with the use of DLT and (2) possible solutions using as a basis the German Federal Debt Management Act (*Bundesschuldenwesengesetz* – BSchuWG).

1. Existing securities law

Under German law, **securities are property** and represent rights. In the book-entry system practised here, the transfer of securities follows the principles of property law. Securities are certificated in global form and held **centrally** at a central securities depository (CSD). In Germany, the CSD is Clearstream Banking Frankfurt (CBF). At CBF (and, if necessary, at foreign CSDs or foreign correspondent banks), banks each have their own account for their customers' securities and transfers of securities are carried out in practice by crediting and debiting the relevant accounts.

An absolute prerequisite for the creation of a security is therefore the existence of a physical certificate. But as explained above, there is no place for a physical document in a **decentralised DLT system**. Nor, as explained below, would it serve a useful purpose to establish a link to a physical certificate by means of a technical "detour". A **legal requirement that a certificate exists** therefore seems incompatible with a practicable use of DLT systems.

A number of provisions of general civil law, the law on bonds, corporate law and custody law require the existence of such a (physical) certificate.

Bonds: debt instruments that can be traded on capital markets, such as bonds, must take the form of physical certificates. The general requirements for individual debt instruments under the German Civil Code (*Bürgerliches Gesetzbuch* – BGB) stipulate the need for a certificate, which, in principle, has to be signed by the issuer (see, for example, BGB sections 793 et seq. on bearer bonds). This so-called *Skripturakt* (literally: "act of writing") ties the undertaking of performance to the certificate. Bearer bonds are transferred in practice in accordance with the principles of property law, i.e. by agreement and delivery (BGB sections 929 et seq.), although transfer by assignment pursuant to BGB section 398 would also be legally permissible (cf. Ruling by the Federal Court of Justice [*Bundesgerichtshof* – BGH] of 14 May 2013 – XI ZR 160/12, WM 2013,

1254 para 12 et seq. with further references). In this case, the right of disposal over the instrument would pass to the assignee pursuant to section 952 (2) of the German Civil Code. In the interests of protecting bona fide transactions, however, the system of transferring securities by book entry practised in Germany follows the property-law model set out in section 929 et seq. of the German Civil Code. However, even the ability to transfer instruments by assignment would not remove the need for a physical certificate for the issue and initial acquisition of a bearer bond (cf. BGH, loc. cit., para 9). Bonds covered by the scope of the German Bond Act (*Schuldverschreibungsgesetz* – SchVG) – i.e. all global issues of identical bearer or registered bonds – also require a physical certificate, which has to list or make reference to the terms of the bond (SchVG section 2).

Shares: under the German Stock Corporation Act (*Aktiengesetz* – AktG), shares must also, in principle, be certificated. Two types of share are possible: registered shares and bearer shares. The issuance of **bearer shares**, which are still widely used by public companies, requires either that the company be listed on a stock exchange or that the articles of association exclude the right to hold individual share certificates (AktG section 10 (5)). In the latter case, a global certificate must be deposited with a CSD (AktG section 10 (1), sentence 2 no. 2).

Registered shares, which are now envisaged by law as the standard form of certification (AktG section 10 (1), sentence 1), require all shareholders to be entered in the company's register of shareholders. This used to be a physical record, but can now also be maintained electronically. It is true that physical share certificates are no longer required for this purpose (AktG section 67 (1), sentence 1), nor is an entry a prerequisite for the acquisition of shares, which takes place independently of the register. Furthermore, the articles of association of a stock corporation are not legally required to mention certification, so certification is therefore also not mandatory by law (see AktG sections 214 (4), 320a and 327e).

Nevertheless, it is generally recognised that every shareholder in their capacity as a member of the company has an inalienable right to certification (cf. AktG sections 10 (5) and 213 (2)). The company fulfils this requirement by obtaining the signature of the management board on a share certificate (AktG section 13), which it then deposits (with a CSD) (sections 3, 5 and 9a of the German Safe Custody Act [*Depotgesetz* – DepotG]). Further provisions also make reference to the certification of membership rights (see, for example, AktG sections 64 (4), 65 (1), 72 to 75, 142 (7) and 256 (7)).

Safe Custody Act: German **custody law** also takes the view that securities are governed by property law. The term "security" primarily covers shares and bearer bonds (DepotG section 1 (1), sentence 1). If certain other conditions are met, it also includes registered bonds (DepotG section 9a in conjunction with section 1 (2), sentence 2). Although the Safe Custody Act does not explicitly make physical certification a prerequisite for holding securities in a securities account, there is an underlying assumption in the language used and the actions described that a certificate will exist (e.g. DepotG section 5 (2): "the delivered security"; section 7: "deliver

securities", "delivered securities"; section 9a: "global certificate", "hand over", "individual securities"; section 13: "ownership", "take possession of", etc.). The Safe Custody Act takes the view that securities exist (initially) as (individual) certificates, which the owner (depositor) entrusts to a custodian for safekeeping (DepotG section 1 (2)) either in individual or collective custody (DepotG sections 2, 3 and 5). Under section 688 of the German Civil Code, safekeeping is an obligation to **store a movable item**. Custody services are therefore a subcategory of safekeeping within the meaning of the German Civil Code – to be precise, the safekeeping and administration of securities for others by an entity authorised to do so (cf. KWG section 1 (1), no. 5). The existence of a fungible item within the meaning of section 91 of the German Civil Code is therefore a prerequisite for the provision of custody services.

The custodian may entrust the item, i.e. the security (certificate), to another custodian to hold in collective custody, and this so-called sub-custodian is in turn permitted to pass the security on further (DepotG sections 3 and 5). At the end of the custody chain is the CSD (DepotG section 1(3)). In practice, however, securities traded on the capital markets are no longer issued in the form of individual certificates which investors entrust to their bank for safekeeping. Instead, the entire issue normally takes the form of a single certificate, which is held in custody from the outset by the CSD. Usually, the issuer will also exclude right to hold individual certificates at the time of issuance. The Safe Custody Act specifically provides for this possibility in section 9a (global certificate), so the custody business is able to function without individual certificates. Registered bonds issued in the name of a CSD are also securities within the meaning of the Safe Custody Act, as are collective debt register claims by virtue of legal fiction in accordance with the Federal Debt Management Act. And owing to the provisions of section 5(4) of the Safe Custody Act, there are no obstacles even to dematerialised foreign securities being held in custody.

The Safe Custody Act and its practical implementation therefore show that it is not property law as such that obstructs the use of DLT for securities, but only the legal requirements that a certificate exists.

In addition to the high level of safety as a result of tying credit to debit entries of securities in their capacity as property and the protection afforded in the event of insolvency, the principles of property law also protect purchasers acting in good faith, who can rely on the seller's ownership of the securities. A prerequisite, however, for the bona fide purchase of bearer or registered bonds is that the bonds are acquired in accordance with the principles of property law – in other words, by transfer of title and delivery pursuant to sections 929 et seq. of the German Civil Code. To meet this prerequisite under property law, the system established in Germany for executing transactions in securities by book-entry requires an agreement on the transfer of ownership, and a transfer of intermediate possession by the so-called *Geheißerwerb* (which takes place by power of attorney), and by the CSD changing its intention concerning for which party it wishes to possess the securities, and accordingly, by all parties along the chain of custodian banks up to the end investor, so-called *Umstellung des Besitzmittlungswillen* (see *Decker* in:

Hellner/Steuer, Bankrecht und Bankpraxis, volume 4, para 8/14 et seq. and 8/67 et seq.; *Rögner* in: Scherer, DepotG, section 5 para 72 et seq.; *Klanten*, in: Bankrechts-Handbuch, section 72 para 102 et seq.). Transfer of intermediate possession is evidenced by means of an account entry.

The mechanics of registering a transaction in a DLT register are different, however, so there can be no question of deeming the procedure an "account entry". In addition to the need for a physical certificate, therefore, the entry in its capacity as a **substitute for the delivery of possession** also poses a problem when it comes to the legal classification of a registration in a DLT register. Despite the obvious act of transferring ownership which the registration in a DLT register is intended to express, it would not be recognised as a substitute for the delivery of possession pursuant to sections 929 et seq. of the German Civil Code. Nor is any real estate being transferred, so section 892 of the German Civil Code can also be ruled out as a legal basis.

2. Possible solutions

DLT securities, i.e. securities that are documented in a DLT system, should be **securities** in accordance with the German understanding of law. This would allow them to continue to benefit from the key advantages of property law (in particular confidence in recordings of transactions, protection of bona fide transactions and protection in the event of insolvency).

Wertrechte: the simplest solution would be to classify DLT securities as *Wertrechte* (literally "value rights"; rights to securities which do not necessarily exist in a physical form). In light of their dematerialised nature, however, some legislative action would be necessary. They could, for example, be regulated along the lines of securities covered by the Federal Debt Management Act with the aim of establishing equal treatment for securities entered in book-entry systems and "securities" registered by DLT. Lawmakers could consider the idea of creating a "**qualified digital register**" (**QDR**) as an equivalent to state debt registers. A legislative project of this kind could be implemented either in the Safe Custody Act or in a special law for DLT securities.

Non-collective safe custody: as an alternative, or in addition, to the model described below, a purely contractual structure could also be considered, like that for securities held in custody abroad. This model would correspond to so-called *Wertpapierrechnung* (non-collective safe custody). Corresponding provisions would then need to be added to the "Special Conditions for Dealings in Securities" used by the German banking industry, though this would not in itself result in DLT securities being classified as securities within the meaning of German law.

A solution based along the lines of the Federal Debt Management Act: in a system similar to that under section 6 of the Federal Debt Management Act (see annex), securities should therefore as far as possible be able to be issued, transferred, encumbered and administered by entering them in a QDR as **QDR claims** up to the nominal amount of the issue in question

(collective QDR claims). By virtue of legal fiction, these claims would then be deemed a **holding in collective custody**. The share of a creditor in the global issue would be determined by the nominal amount of QDR claims held in collective custody and registered in the QDR for that creditor. The party registered in the distributed ledger for the global issue would administer the collective QDR claims in a fiduciary capacity for the creditors without itself having any entitlement to the collective QDR claims. This party would be able to administer these collective claims for the creditors together with any claims of its own. **The relevant provisions of the Safe Custody Act should apply**. This goes especially for the custody chains downstream of the fiduciary agent. Another conceivable solution would be to modify the Safe Custody Act to accommodate QDR claims in a way that takes account of the fact that no (individual) certificates for the securities exist and recognises that registration in the QDR documents the passing of ownership (through transfer of intermediate possession) in the same way as a book entry.

Claims to certification should be excluded, as should claims to the furnishing of (individual) physical certificates unless the terms and conditions of the issue provide otherwise. The debtor of the collective QDR claims should only be able to raise such objections as arise from the entry in the register, concern the validity of the entry or that the debtor is entitled to raise directly against a creditor. The party registered in the distributed ledger should be entitled to demand from the debtor revenue payments (dividends, interest, etc.) for the collective QDR claims registered in the debtor's name and payment of the capital when due. The debtor should be discharged from its obligations to the creditors of the collective QDR claims on payment to the party registered in the distributed ledger.

No certificate is required to issue book-entry federal debt securities. The certificate is replaced by the entry in the Federal Debt Register (BSchuWG section 5 (1) and (3)). In the case of a collective debt register claim registered in the Federal Debt Register in the name of a CSD (BSchuWG section 6 (1)), the claim is deemed by virtue of a legal fiction to be equivalent to a collective securities holding (BSchuWG section 6 (2), sentence 1). To apply this arrangement to the issue of bonds (or other securities) by means of DLT, the associated distributed (decentralised) registration of all data relating to the legal relationship between issuer and creditors would correspond to the registering function of the Federal Debt Register (BSchuWG section 5 (3)). This goes especially for the question of whether, in a bond issue by DLT, a CSD should assume a similar function to that envisaged by BSchuWG section 6 (2), sentences 4 and 5, which sees the CSD as acting in a fiduciary capacity for all holders of the claims entered in the debt register. If this were to be answered in the affirmative, compatibility with the requirements of the Central Securities Depositories Regulation (CSDR) would possibly be established.

Theoretically, other possibilities are also conceivable concerning collective and individual debt register claims. These would necessitate adjustments to the CSDR; see section B.II.2 below for details.

Bona fide transactions along the lines of the Federal Debt Management Act: like in the Federal Debt Management Act, the new legislation governing QDR claims could specify – as in BSchuWG section 8 (1) – that sales of QDR claims need to be **entered** in the QDR to be effective vis-à-vis the debtor. If a QDR claim is to be transferred to another creditor under the terms and conditions of the QDR, this creditor should always be able to acquire it even if the previous creditor is not the owner. Third-party rights to the QDR claim and restrictions on the previous creditor's rights of disposal should only be effective vis-à-vis the new creditor if they are entered in the QDR. This should not, however, apply if, at the time of acquiring the QDR claim, the new creditor was aware or was only unaware due to gross negligence that the previous creditor was not or not fully entitled to the QDR claim, or that the previous creditor was subject to a restriction on their power of disposition, or that the QDR claim was encumbered with the rights of a third party. A party entered as the holder of a contractually established lien on, or beneficial interest in, a QDR claim should always be able acquire these rights even if the previous creditor is not the owner. The QDR terms and conditions should require entries to be made in chronological order. Instead of a certificate, the registration in the QDR would therefore function as proof of entitlement to the security and would thus guarantee protection for bona fide transactions.

Protecting bona fide transactions along the lines of the Federal Debt Management Act would be **appropriate** because the idea of this law is based on the fact that the state itself maintains the register or electronic register, which, as a result, is deserving of special confidence. But mistakes can even creep into a state-run debt register (as a result of human error, for instance). DLT-based QDRs, by contrast, would deserve an even greater level of trust since the technology involved would virtually rule out the possibility of errors of this kind.

Requirements for QDRs: to enable DLT securities to be considered legally equivalent to *Wertrechte* and thus enjoy the privileged treatment of property law, it is not enough for the markets to have confidence in the technical aspects of DLT (with trust in the functioning of DLT replacing, so to speak, trust in the persons involved). Confidence in the **legal certainty** of the DLT securities system is also essential. This is basically a task for **lawmakers**. When regulating DLT, they should focus on regulating platform operators and participants. It should be ensured that the DLT platforms (i.e. the QDRs) meet some basic requirements.

Restricted network: as described above in part A, a DLT network can be public (or permissionless) or restricted (private or permissioned). The QDR should be designed as a restricted network. An unrestricted DLT securities platform could open the door to money laundering, terrorist financing and other criminal activities. Requirements which are supposed to ensure compliance with existing legal countermeasures would, if applied to so-called whitelisted wallets, need to be supplemented by new legislation and procedures for authorising and effectively supervising the new players involved. Though this may well be theoretically conceivable, we believe further ground would be lost to competing jurisdictions while these (complex) new rules, regulations and procedures were developed and put in place. Furthermore,

we consider solutions which necessitate the maintenance of parallel registers (especially for identity verification) to be less secure than solutions integrated in a single register. Nor, as far as we are aware, would unrestricted networks be able at present to ensure that the regulatory requirements governing securities transactions were met. In addition, operators and participants would need to comply with special IT security requirements and be supervised accordingly. A characteristic feature of a restricted DLT securities system/QDR would be the existence of one or more state-authorised and supervised institution(s) in charge, who could have many names depending on the design of the network in question: DLT, QDR, platform or register organiser, or operator, administrator, registrar, administrator, gatekeeper, etc. This institution or these institutions would distribute the cryptographic keys, which might come with different access rights and which would make participation in the network possible in the first place. A further category of participants could also be admitted to the network, possibly with different access rights again and also with different names, such as users or participants. In any event, certain operating conditions and terms of use would need to be established for the QDR – in other words a DLT governance. This would define essential criteria such as access conditions, the consensus principle, access rights, responsibilities, and validation and correction mechanisms (see also below).

Operators and users of QDR platforms: if DLT securities are *Wertrechte* and thus financial instruments within the meaning of legislation governing financial supervision and capital markets, both the instruments themselves and, above all, all persons issuing, trading or otherwise using them will be subject to a number of statutory and regulatory rules and regulations. Depending on their specific activity, QDR platform operators and users will therefore have to comply with corresponding licensing requirements, follow-up obligations and/or rules of conduct.

(i) Eligibility to act as a **QDR platform operator** would best be regulated by law. There are three possible approaches. Since the role of QDR platform operators is not dissimilar to custody business (KWG section 1 (1), sentence 2, no. 5), the activity could be reserved for licensed **credit institutions** (i.e. banks). Alternatively, the activity could be regarded as similar to the so-called "limited custody business" for alternative investment funds (KWG section 1 (1a), sentence 2, no. 12), so that it would suffice to have a licence to operate as a **financial services institution** (FSI). Finally, (decentralised) custody and settlement could qualify the platform operator(s) as CSDs, which would require special authorisation. A combination of these approaches would also be conceivable. If a platform operator was located, or at least supervised, in Germany, compliance with nationally applicable rules and regulations could be monitored by German supervisory authorities. If this was not the case, the question of appropriate equivalence rules would need to be addressed.

(ii) As to **QDR participants**, lawmakers would need to decide who they wish to allow to participate and under what conditions. They could either open up access to all market participants provided that they met certain requirements, or they could limit access to

professional market participants (within the meaning of MiFID II or EMIR, for example) such as banks, FSIs, insurance companies or certain large firms. Finally, consideration would need to be given to whether issuers participating in a QDR should be subject to special requirements and whether supervisory authorities and other government agencies should have participant status or constitute another category of users.

Technical requirements: **BaFin**, as the responsible national **supervisory authority**, together with a **technical monitoring agency** (such as the Federal Office for Information Security – *Bundesamt für Sicherheit in der Informationstechnik*, BSI), should scrutinise the technology used, both before granting authorisation to operate and later at regular intervals in the course of ongoing supervision. Their analysis should **include IT security and data protection**. **ISO standards** for DLT protocols could be helpful in this respect.

DLT governance/QDR terms and conditions: the platform operators should agree a set of binding rules and regulations (rule book) with all participants. The rule book should set out the QDR terms and conditions (or DLT governance), which should also be binding on participants who join the network at a later date.

DLT governance should define the rules according to which the QDR operates and the tasks and responsibilities of all parties involved. This would cover access conditions, the principle of consensus, access rights, and validation and correction mechanisms, for example.

(i) With regard to **reaching consensus**, lawmakers will want to consider whether to lay down rules and, if so, how specific these should be (e.g. 50 %+1 or higher).

(ii) Aspects where the QDR securities differ from those processed by conventional securities settlement systems could be clarified. This applies particularly to the issue of the **finality of QDR securities transactions**.

(iii) A **choice of law** would be essential. Though it would seem in principle to make good sense to require the choice of German law, it should be borne in mind that the QDR, like all DLT applications, would not be limited in its operation and its impact to a purely national context.

(iv) A (domestic) **legal venue** would also need to be chosen.

(v) Platform operators and participants should also make serviceable (*zustellfähige*) addresses available to one another.

(vi) The **QDR terms and conditions should comprehensively regulate the relationship between the platform operator and all participants**. They should make clear that the participants are not liable to one other and do not form a company or an association and do not

bear joint liability. By law they merely hold fractionally shared joint ownership with respect to their collective QDR claims.

Avoiding duplication of securities in a DLT: DLT securities should not just be able to mirror existing, conventional securities in a DLT environment, but should also be assets specifically created in and for the distributed ledger. It should, however, also be possible to integrate existing conventional securities into a DLT environment and trade them there, for example. Clear rules in the terms and conditions of the distributed ledger need to spell out how this will be achieved. For their part, lawmakers could consider how to legally ensure that there can be no duplication or similar distortion of entries. This could be achieved (i) by means of a **provision based on section 8 of the Federal Debt Management Act** stipulating that sales/transfers of DLT securities or conventional securities using DLT always require a corresponding entry in a distributed ledger to become effective, and that only this entry is relevant (reference to finality rules in the QDR terms and conditions). Alternatively (ii), by means of a kind of "system of communicating tubes" between the virtual and analogue worlds, roughly comparable to the arrangement under **section 5 (4) of the Safe Custody Act**, with the conventional securities integrated into the DLT environment using a mechanism similar to a CSD link.

Signature: the security and recognition of digital signatures will be a key factor in the use of DLT. They should be subject to clear rules in line with **data protection** and **IT security** (see below) and the **EU Electronic Identification and Trust Services (eIDAS) Regulation**.

Applicable law: from a property law perspective (assuming that DLT securities are *Wertrechte*), it would make good sense to extend the scope of the conflict of laws provision in **section 17a of the Safe Custody Act** to cover DLT securities. From the contractual perspective, a contractual choice of law should always be specified in the **terms and conditions of the DLT platform** and this choice of law should be binding on all parties involved.

Legal venue: under the German Code of Civil Procedure (*Zivilprozessordnung* – ZPO), this is either the general venue, i.e. the place of residence or registered office (ZPO sections 12, 13 and 17), or the place of performance (ZPO section 29). Distributed ledgers are not really compatible with these principles. The registered office of a DLT platform could, however, be deemed the place where the platform operator or user is domiciled. This would **require legislative clarification in the Code of Civil Procedure** and a rule that the **terms and conditions of a QDR** have to contain a corresponding contractual clause (see above).

Probative value and enforcement: lawmakers will also have to clarify what **requirements** to set concerning the probative value of DLT entries in general and, in particular, in relation to enforcement (e.g. criteria to be met by the electronic keys of the participants). These requirements could be set out in the **Code of Civil Procedure** or in a special law.

Insolvency: lawmakers should also consider whether special rules are required in the **Insolvency Code** (*Insolvenzordnung* – InsO) or in special legislation regarding the insolvency of DLT platform operators or users, in particular concerning the special functions that they perform.

II. Supervisory law

Financial market supervisory law is already **largely technology-neutral** today. Irrespective of their civil thrust and classification, European and national supervisory law are geared to the term "financial instrument", which is broader than the term "security". This is because the primary objective of supervisory law is to establish appropriate rules for dealing with the risks that exist in comparable circumstances. The introduction of DLT securities systems does not face any major supervisory obstacles, as certification of financial instruments is not usually required under supervisory law. At the same time, selected provisions require further modification and clarification which, given the advanced state of harmonisation of supervisory law, are likely to fall to a great extent within the remit of Union legislators.

1. Classification

Securities trading law: regulation of securities trading and market infrastructure under the Markets in Financial Instruments Directive (**MiFID II**), the Markets in Financial Instruments Regulation (**MiFIR**) – and thus also under the **German Securities Trading Act** (*Wertpapierhandelsgesetz* – **WpHG**) – is geared to the terms "**financial instrument**" and "(ancillary) investment services", without calling for any certification. Financial instruments also cover pure contracts, such as derivatives, and are not confined to instruments designed in accordance with property law rules. Physical representation in the form of a certificate is, however, explicitly not required for **securities** either (WpHG section 2(1)). The admission or inclusion of securities in the regulated market on a domestic exchange also does not presuppose their certification (section 32 et seq. of the German Stock Exchange Act [*Börsengesetz* – BörsG]).

Prospectus law: There is also no prospectus law requirement for certain financial instruments to be represented by a certificate. The requirements set out in the **German Securities Prospectus Act** (*Wertpapierprospektgesetz* – **WpHG**), the EU Prospectus Regulation (2017/1129) or in the **German Investment Act** (*Vermögensanlagegesetz* – **VermAnlG**) merely regulate the content of a prospectus.

Capital markets law: the (protective) provisions of European and German capital markets law are geared mainly to the term "financial instrument". For example, the provisions of the amended **Market Abuse Regulation** (**MAR**) apply to financial instruments admitted to trading on a regulated market (MAR Article 2(1)(a)). Much the same goes under the provisions of the German Securities Acquisition and Takeover Act (*Wertpapiererwerbs- und Übernahmegesetz* –

WpÜG), albeit these are geared to the term "security" (WpÜG section 1(1)). A legally sound classification of DLT *Wertrechte* as securities and financial instruments is therefore crucial.

Apart from the topics expressly addressed in this section II, there are numerous others that may also be of importance for DLT securities, though they are not directly connected with the issue and "safe custody" of such securities, e.g. the Market Abuse Directive (MAD) or the European Market Infrastructure Regulation (EMIR).

2. Action needed

Clarification of the term "security": taking up the basically broad definitions of the terms "financial instrument" (KWG section 1(11) and MiFID II Annex I, section C), "security" (WpHG section 2(1)) and "(ancillary) investment services" (WpHG section 2(8) and (9) and MiFID II Annex I, sections A and B), legislators should make clear that DLT *Wertrechte* qualify as securities and financial instruments or are equivalent to these. Because of the now differentiated EU financial market supervisory framework, such qualification should also apply at the level of Union law. As a central point of reference in EU supervisory law, an amendment of MiFID II or inclusion in the long-awaited securities law legislation (SLL) could, for example, be considered. As a transitional measure, thought could be given to a national arrangement or appropriate administrative practice.

Tie-in with QDR regulation: in addition, it would have to be clarified whether regulatory **authorisation requirements and requirements for DLT securities system operators and participants** are to apply (e.g. to banks, FSIs, CSDs, central counterparties (CCPs), possibly trading venues, multilateral trading facilities (MTFs), organised trading facilities (OTFs), etc.).

Tie-in with prospectus requirement: a technology-neutral approach for the issuance of DLT securities would have to be geared to appropriately substituting the functions linked to certification. These functions comprise the certificate as (i) an information carrier and (ii) as a prerequisite for the negotiability of the financial instrument. Where the certificate serves as an information carrier (e.g. SchVG section 2), it would make sense to take the issuing prospectus as an additional point of reference for determining the key content of the contract. In the case of a bond issue, the entire legal relationship between issuer and bond creditor could, for example, be encapsulated in the entry in the digital register (token), the content of which is then set out verbally in the issuing prospectus. Where the content of the token and the prospectus differ, the content of the prospectus would take precedence for investor protection reasons. Through a corresponding provision in SchVG section 2, it could thus be stipulated that the bond terms may not necessarily be provided only by the certificate or its surrogate, the token, but also by other sources, particularly a prospectus issued in accordance with the provisions of the German Securities Trading Act.

Investment law: supervisory law is, however, still geared in the case of open-end investment funds and their admissibility under supervisory law to the existence of a certificate. Units in an open-end investment fund in contractual form (so-called "special funds") may, for example, only be issued if they are represented by a certificate (Section 95 of the German Investment Code [*Kapitalanlagegesetzbuch* – KAGB]).

Regulation of central securities depositories: the requirement in the Central Securities Depositories Regulation (Regulation (EU) No 909/2014 [**CSDR**]) for issuers to record securities in book-entry form if and to the extent that they are traded on trading venues is technology-neutral only to a limited extent. Given the systemic importance of securities settlement and safe custody and the introduction of TARGET2 Securities (T2S), the CSDR is aimed at creating a single European market for securities settlement and safe custody. A key element in achieving this regulatory goal is the requirement for securities to be recorded (before the intended settlement date, if possible) in book-entry form in a CSD (CSDR Article 3(2)).

Article 3(1) of the CSDR says that any issuer established in the European Union must arrange for such securities to be represented in book-entry form as immobilisation or subsequent to a direct issuance in dematerialised form.

The CSDR does not stipulate that securities traded on a trading venue should be issued in the form of a certificate. Instead, it puts collective safe custody at a CSD and dematerialisation (i.e. recording in purely book-entry form) on an equal footing. What it does stipulate, however, is that securities should be recorded in book-entry form in a CSD. This requirement could mean that operators or administrators of private QDR platforms would require a CSD licence.

Discussion is needed at European level on whether securities issued via DLT must be recorded in book-entry form in a CSD, as currently stipulated in Article 3 of the CSDR. Article 3 of the CSDR could instead be amended to include the possibility of register entries using DLT. In this case, it must be decided whether, besides CSDs, gatekeepers may also be other (regulated and supervised) market participants and/or whether only CDSs are entered in the QDR as (fiduciary) owners for the entire issue.

Requirements for safe custody business: safe custody business is based historically on the idea of individual certificates being held physically for clients. These can also be entrusted to one or more third-party depositories and pooled to form collective holdings. As a result, there are, among other things, civil provisions on client protection (e.g. general presumption that all securities held by a depository with another depository are client assets (*Fremdvermutung*) (DepotG section 4(1)), as well as corresponding supervisory requirements and administrative practice, particularly in regard to book-keeping and designation of accounts (e.g. safe custody account A and safe custody account B). Depending on whoever is considered to be a QDR

gatekeeper under whatever arrangements, the supervisory requirements and administrative practice would have to be adapted accordingly.

SFTR: Article 15 of the EU Securities Financing Transactions Regulation (Regulation (EU) No 2015/2365 [SFTR]) sets (formal) conditions for the reuse of financial collateral (in the event of full transfer of title and pledge with a declaration of appropriation): in addition to written notification (paragraph 1(a)), a condition for reuse is that the securities serving as financial collateral "are transferred from the account of the providing counterparty" (paragraph 2(b). These formal provisions would have to be adapted.

Anti-money laundering and criminal law: fully recording all QDR entries is important to prevent money laundering, terrorist financing and other criminal offences. Depending on how the supervisory framework is designed, it should be examined to what extent regulated QDR operators and QDR participants, as "obliged entities" under anti-money laundering law, are already subject to effective requirements under the **German Anti-Money Laundering Act** (*Geldwäschegesetz* – **GWG**), the **German Banking Act** and the **German Criminal Code** (*Strafgesetzbuch* – **StGB**), plus the provisions of the **Fifth Anti-Money Laundering Directive** and those governing its implementation, and whether additional requirements are necessary. Furthermore, general criminal law is geared in principle to the property-law definition of "security" that would also require clarification or amendment by legislators (e.g. securities forgery pursuant to StGB section 151 and investment fraud pursuant to StGB section 264a, DepotG sections 34, 35).

Risk management and compliance: as regards the subsequent obligations for banks, FSIs and various other financial market participants, thought should be given particularly also to **adapting/specifying** the requirements for risk management and compliance (in accordance with the **ECB supervisory requirements** as in the **German Banking Act**, the **Minimum Requirements for Risk Management** (*Mindestanforderungen an das Risikomanagment* – **MaRisk**) and the **Minimum Requirements for the Compliance Function of Financial Institutions** (*Mindestanforderungen an die Compliance der Institute* – **MaComp**) issued by BaFin.

IT security: QDR securities system operators and participants should, in principle, be subject to special IT security requirements. Thus, for example, credit institutions within the meaning of the German Banking Act are already subject to comprehensive BaFin security standards (**Supervisory Requirements for IT in Financial Institutions** (*Bankaufsichtliche Anforderungen an die IT* – **BAIT**) and must demonstrate that they have internal control mechanisms in place (**KWG sections 6b, 25a and 25b**).

Data protection: QDR securities system operators and participants must, in addition, comply with the data protection provisions set out in the EU General Data Protection Regulation (**GDPR**) and the **German Federal Data Protection Act** (*Bundesdatenschutzgesetz* – **BDSG**) if data

relating to natural persons (= personal data) are processed within the system itself. The statutory provisions are designed to protect citizens' right to "informational self-determination". Data protection law covers not only "clear text" personal data but also "pseudonymised" data frequently encountered in DLT usage. This raises numerous questions, e.g. regarding the legal basis for data processing, legally secure separation of the functions of the **controller** and the processor under data protection arrangements, supervisory-authority jurisdiction in cross-border cases, the compatibility of DLT protocols geared to the permanent inalterability of data and the requirement under data protection law to delete data on a time-lapse basis ("**right to be forgotten"**). Bearing in mind that certain data are essential to ensure QDR functionality, the latter would have to be examined particularly with regard to data that are either not needed, or no longer needed after expiry of a period of time, for the register to function.

Tax law: the tax classification of QDR securities and the activities of QDR operators and QDR participants – with regard to both **value-added taxes** and **income taxes as well as, where applicable, withholding taxes** – should be aimed at ensuring synchronisation with the rules on taxation of securities represented by physical certificates.

C. Proposals for reform

- **DLT securities as *Wertrechte***: national legislators should create a secure legal framework for the issuance and recording of securities in DLT systems. This should ultimately ensure transfer in accordance with the principles of property law, including protection of bona fide rights and priority rules for DLT register entries and analogue recording (finality rules).

- **Transfer of title by way of agreement and "book entry"**: an acceptable approach would be the introduction of rules for QDRs, comparable to the dematerialised approach adopted in the German Debt Management Act, which could be set out in the German Safe Custody Act or in a special law. These rules should stipulate that transfers of title to securities be made by agreement and register entries. DLT systems that are subject to the special rules for QDRs should be designed as restricted (access-restricted) systems. An appropriate term for entry in a distributed ledger would have to be used, as "book entry" is usually understood to mean an entry in an account.

- **Securities law**: provisions of stock corporation law should be amended so that certification of shares as securities (either in the form of individual certificates or global certificates) is no longer required where these are held in safe custody in DLT securities systems. The same should apply to (bearer) bonds, also with regard to formal requirements for contract provisions.

- **Investment law**: the requirement of mandatory certification of units in special funds (KAGB Section 95(1)) should be dropped and the issuance of units recorded in DLT systems also allowed.

- **Regulation of CSDs**: discussion is needed at European level on whether securities issued via DLT systems must be recorded in book-entry form in a CSD (CSDR Article 3) and under what conditions DLT systems are compatible with this requirement.

- **SFT Regulation**: adaptation of the formal requirements (written notification and transfer from an account) for the reuse of financial collateral should also be discussed at European level.

- **Safe custody law**: bookkeeping and account designation requirements would have to be adapted.

- **Supervisory framework**: discussion is required at national and European level on which supervisory access criteria and general conditions should apply to DLT securities system

operators and participants. This depends largely on how their functions and activities are classified under existing financial market supervisory law.

List of abbreviations

AktG	*Aktiengesetz* (German Stock Corporation Act)
AML	Anti-money laundering
BaFin	*Bundesanstalt für Finanzdienstleistungsaufsicht* (German Financial Supervisory Authority)
BAIT	*Bankaufsichtliche Anforderungen an die IT* (BaFin, Rundschreiben 10/2017 (BA)) (Supervisory Requirements for IT in Financial Institutions – BaFin circular 10/2017 (BA))
BDSG	*Bundesdatenschutzgesetz* (German Federal Data Protection Act)
BGB	*Bürgerliches Gesetzbuch* (German Civil Code)
BörsG	*Börsengesetz* (German Stock Exchange Act)
BSchuWG	*Bundesschuldenwesengesetz* (German Federal Debt Management Act)
BSI	*Bundesamt für Sicherheit in der Informationstechnik* (Federal Office for Security in Information Technology
CSD	Central securities depository
CSDR	Central Securities Depositories Regulation (Regulation (EU) No 909/2014 of the European Parliament and of the Council of 23 July 2014 on improving securities settlement in the European Union and on central securities depositories and amending Directives 98/26/EC and 2014/65/EU and Regulation (EU) No 236/2012
DepotG	*Depotgesetz* (German Safe Custody Act)
DLT	Distributed ledger technology
eIDAS	EU Electronic Identification and Trust Services Regulation (Electronic Signatures Regulation)
EMIR	European Market Infrastructure Regulation (Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories)
FSI	Financial services institution
GDPR	(EU) General Data Protection Regulation
GwG	*Geldwäschegesetz* (German Anti-Money Laundering Act)
InsO	*Insolvenzordnung* (German Insolvency Code)
KWG	*Kreditwesengesetz* (German Banking Act)
KYC	Know your customer
MaComp	*Mindestanforderungen an Compliance* (Minimum Requirements for Compliance)
MAD	Market Abuse Directive (Directive 2014/57/EU of the European Parliament and of the Council of 16 April 2014 on criminal sanctions for market abuse)
MAR	Market Abuse Regulation (Regulation (EU) No 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse (market abuse regulation) and repealing Directive 2003/6/EC of the European

	Parliament and of the Council and Commission Directives 2003/124/EC, 2003/125/EC and 2004/72/EC)
MaRisk	*Mindestanforderungen an das Risikomanagement* (Minimum Requirements for Risk Management)
MiFID	Markets in Financial Instruments Directive (Directive 2004/39/EC of the European Parliament and of the Council of 21 April 2004 on Markets in Financial Instruments amending Council Directives 85/611/EEC and 93/6/EEC and Directive 2000/12/EC of the European Parliament and repealing Council Directive 93/22/EEC)
MiFID II	Markets in Financial Instruments Directive II (Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on Markets in Financial Instruments and amending Directives 2002/92/EC and 2011/61/EU)
MiFIR	Markets in Financial Instruments Regulation (Regulation (EU) No 600/2014 of the European Parliament and of the Council of 15 May 2014 on Markets in Financial Instruments and repealing Regulation (EU) No 648/2012)
MTF	Multilateral trading facility
OTF	Organised trading facility
PoW	Proof of work
QDR	Qualified digital register
SchVG	*Schuldverschreibungsgesetz* (German Bond Act)
SFTR	Securities Financing Transactions Regulation (Regulation (EU) No 2015/2365 of the European Parliament and of the Council of 25 November 2015 on transparency of securities financing transactions and of reuse and amending Regulation (EU) No 648/2012
StGB	*Strafgesetzbuch* (German Criminal Code)
VermAnlG	*Vermögensanlagegesetz* (German Investment Act)
WpHG	*Wertpapierhandelsgesetz* (German Securities Trading Act)
WpPG	*Wertpapierprospektgesetz* (German Securities Prospectus Act)
ZPO	*Zivilprozessordnung* (German Code of Civil Procedure)

Excerpt from the German Federal Debt Management Act (Bundeschuldenwesengesetz [BSchuWG])*

§ 6 Collective registered claims (Sammelschuldbuchforderungen)

"(1) The Federal Government and its special funds may issue bonds by registered claims being entered in the Federal Debt Register (Bundeschuldbuch) in the name of a central securities depository (Wertpapiersammelbank) up to the nominal amount of the respective issue (collective registered claim).

(2) The collective registered claim shall be deemed to be a collective securities deposit. The creditors of the collective registered claim shall be deemed to have fractional co-ownership rights. Their respective share shall be determined by the nominal amount of the registered claim placed in collective management for the creditor. The central securities depository shall manage the collective registered claim in a fiduciary capacity for the creditors without itself having any entitlement to the collective registered claim. The central securities depository may manage the collective registered claim for the creditors together with its own shares. The provisions of the German Safe Custody Act (Depotgesetz) shall apply accordingly.

(3) Entitlements to issuance of debt certificates shall be precluded unless the terms of issue explicitly provide for such entitlements.

[…]"

§ 8 Public faith in the Federal Debt Register

(1) To become effective against the debtor, disposals of individual registered claims require entry in the Federal Debt Register.

(2) If, following a request by an entitled party within the meaning of Section 7 (4), an individual registered claim is transferred to another creditor, this creditor shall acquire the claim insofar as the previously registered creditor was not entitled to it. Third-party rights to the claim and restrictions on disposal by the previous creditor shall only be effective against the new creditor insofar as they have been entered in the Federal Debt Register. Sentences 1 and 2 shall not apply if, when acquiring the registered claim, the new creditor was aware, or as a result of gross negligence, was unaware that the previous creditor was not, or not fully, entitled to the claim, that the previous creditor was subject to a restriction on disposal or that the claim was encumbered with a third-party right.

[…]"

*Unofficial convenience translation provided by the Association of German Banks

We wish to expressly thank

- Professor Dr. Philipp Sandner, Frankfurt School of Finance and Management
- Peter Scherer, GSK Stockmann
- Dr. Christian Schmies, Hengeler Mueller
- Dr. Tobias Wohlfarth, Hengeler Mueller
- Dr. Lars Röh, lindenpartners
- Dr. Stefan Saager, Bundesverband der Deutschen Volksbanken und Raiffeisenbanken (BVR)
- Olaf Christmann

and our members for the exchange of ideas, their cooperation and contributions.