DEUTSCHE BUNDESBANK
EUROSYSTEM

DEUTSCHE BÖRSE GROUP

www.deutsche-boerse.com

# How Can Collateral Management Benefit from DLT?

## Project “BLOCKBASTER”

January 2020

## Table of Contents

# 1 Executive Summary

There is a general consensus that distributed ledger technology (DLT) has both disruptive and evolutionary potential for financial markets. This paper focuses on potential implications in connection with collateral management activities for financial transactions, the aim being to analyze the challenges and opportunities of DLT in the current regulatory environment for this specific use case.

It is important to highlight that pure securities settlement services such as those currently provided by TARGET2-Securities (T2S), for example, are beyond the scope of this paper. The typical nature of collateral management activities is the temporary use of assets (securities and cash) for covering risk exposures. In particular, the opportunities resulting from an enhanced mobility of existing assets through the use of DLT will be investigated.

The use cases these considerations are built on are the coverage of exposures ("collateralization") which regularly arise through a variety of underlying financial market activities such as securities lending or repo transactions, CCP and OTC exposures or monetary policy operations of central banks.

The core of the conceptual investigation in this paper is the use of securities - issued in the traditional way - as collateral in a DLT environment. Therefore, a trust model is introduced which blocks securities in existing systems and creates "representative" tokens. It serves as a reliable and neutral link ensuring regulatory compatibility and legal certainty. These tokens can then be transferred instantly between the participants in the network and thus be used as collateral. Token transfers are recorded on an immutable ledger which is shared between relevant parties.

In addition, there are technical requirements derived from the use case that have to be met. "Know your customer" (KYC) and anti-money laundering (AML) rules heavily influence the design choices made for the DLT solution, for example leading to a private and permissioned set-up. Other requirements are the speed and confidentiality of highly critical and sensitive transactions.

Even though considerable challenges exist, DLT has the potential to significantly change the current post-trade environment. Using DLT for collateral management has important advantages for the collateral taker and the collateral giver as the underlying operating model no longer requires securities to be moved across custodians[1], thus enabling 24/7 availability of collateral and improving collateral fluidity. The accompanying removal of complex reconciliation efforts due to synchronized decentralized data structures – which are necessary between various actors in traditional systems – will allow for substantial cost reductions and enable (near) real-time legal title transfer of securities and baskets thereof. Furthermore, DLT-based collateral management will support enhanced regulatory transparency of collateral services by providing specific collateral monitoring tools.

From a purely technical point of view, a holistic DLT set-up of services for collateralization purposes may not be seen as a major challenge. However, given the fact that the financial industry operates with many traditional systems, the introduction of DLT can most likely not take place as a "Big Bang". A significant period of time can be expected in which the existing infrastructures gradually adapt to the new technology. Consequently, old and new technologies will run in parallel during this transitional period. The existing infrastructures are designed to cater for versatile business cases and must take into account the complex regulatory environment. Therefore, the main challenge lies in

[1] For the purpose of this paper the term custodian also includes Central Securities Depositories (CSDs)

designing DLT solutions which fit seamlessly in the current regulatory, process and system landscape and provide instant benefits for market participants. Building such solutions would represent the first steps in the process of utilizing DLT. By developing this process step by step, the potential of the technology could be harnessed in order to continually improve the existing infrastructures over time.

## 2 Introduction

As regards innovation in technology and business, blockchain and DLT continue to be in the focus of financial market players as well as central banks. Even though the general euphoria has cooled somewhat, the technology continues to be intensively explored in various areas due to potential advantages and cost savings. Numerous financial market infrastructure providers, including central banks (e.g. Bank of Canada, Monetary Authority of Singapore, Australian Stock Exchange), are testing DLT technology, e.g. for processing interbank payments and securities transactions in central bank money and other post-trade services.

Deutsche Bundesbank and Deutsche Börse have already successfully completed two joint research projects on securities settlement based on blockchain technology (project “BLOCKBASTER”)[2]. The two prototypes support the settlement of securities transactions, payments, interest payments and redemptions. The technology used in the two prototypes appears, in principle, to be suitable for the productive operation of a financial market infrastructure.

It is now intended to continue this cooperation in order to gain a better understanding of the suitability and potential of blockchain-based or more general DLT-based processes in the area of collateral management. From a central bank perspective, collateral management is of fundamental importance for the operational management of monetary policy. As a provider of large financial market infrastructures and of triparty collateral management solutions, Deutsche Börse is intensively engaged with the possibilities offered by DLT and possesses a wealth of expertise in this area.

On the one hand, regulatory requirements following the financial crisis, e.g. the new Basel liquidity regulations and uncleared margin rules of EMIR, are regarded as major drivers of the substantial increase in collateral demand. On the other hand, the Eurosystem’s Asset Purchase Programmes have influenced the markets for certain high-quality assets. Due to these developments, the issue of collateral scarcity has been discussed intensively. Initiatives fostering the mobility and velocity of collateral have become ever more relevant.

In this regard, several Eurosystem services are already in place. The T2S securities settlement service provides functionality to enhance the speed of collateral movements and to increase liquidity savings due to its centralized pool of cash and securities. Collateral mobility already benefits from the fact that the Eurosystem allows the usage of triparty collateral management services for the purpose of collateralizing refinancing operations. Future milestones in this regard will be achieved with the go-live of the Eurosystem Collateral Management System (ECMS) and with the implementation of the Eurosystem’s AMI-SeCo (Advisory Group on Market Infrastructure for Securities and Collateral)

[2] See BLOCKBASTER Final Report (https://www.bundesbank.de/resource/blob/766672/29feab3f9079540441e3abda1ed2d2c1/mL/2018-10-25-blockbaster-final-report-data.pdf)

Harmonization Standards in the area of collateral management, which are currently under development.

However, all these projects and initiatives need time to take full effect. Financial market actors need to adapt their business models; this will require not only changes in technology but also considerations regarding the legal implications and not least business policy decisions.

Using DLT for collateral management purposes may – depending on the individual assessment – provide significant additional opportunities to improve collateral mobility and overcome existing process deficiencies. Those could possibly be implemented quite quickly but should be seen as complementing ongoing activities and could run in parallel.

Section 3 below sets out the current operating model of safe custody, settlement and the use of securities as collateral. In Section 4, a possible future model for the use of DLT in the area of collateral management is designed. Legal and regulatory aspects are examined in Section 5. In addition, considerations regarding custody for digital securities as well as cash in collateral management and also possible Eurosystem requirements governing the mobilization of DLT collateral assets are presented in separate boxes. This paper concludes with an outlook on how the usage of DLT for collateral management could evolve and raises questions for further analysis.

## 3 What Does the Current Operating Model Look Like?

Currently the delivery of marketable assets as collateral generally requires an actual transfer of the securities from the collateral giver to the collateral taker, involving all intermediaries in their respective custody chains from the issuing CSD downwards. The relatively cumbersome mobilization and reconciliation processes associated with this make it difficult for business partners to manage collateral efficiently and effectively. As a result, the related collateral management processes are complex, time-consuming, require broad liquidity margins and are therefore in need of optimization.

To optimize collateral usage within the current operating model, triparty collateral management services can be used. In this case, the triparty agent offering these services assumes the task of selecting, moving and valuing collateral based on pre-agreed parameters and criteria, thus enabling participants to optimize the use of their securities portfolios held with one custodian across different products and instruments when collateralizing credit and other exposures.

Current AMI-SeCo collateral management harmonization activities being coordinated by the ECB will lead to a reduction or even elimination of existing differences and complexity in collateral management processing, thus enabling improved mobilization processes across different (I)CSDs and markets. However, restrictions will remain until all parties have fully implemented the standards and adapted their business models accordingly.

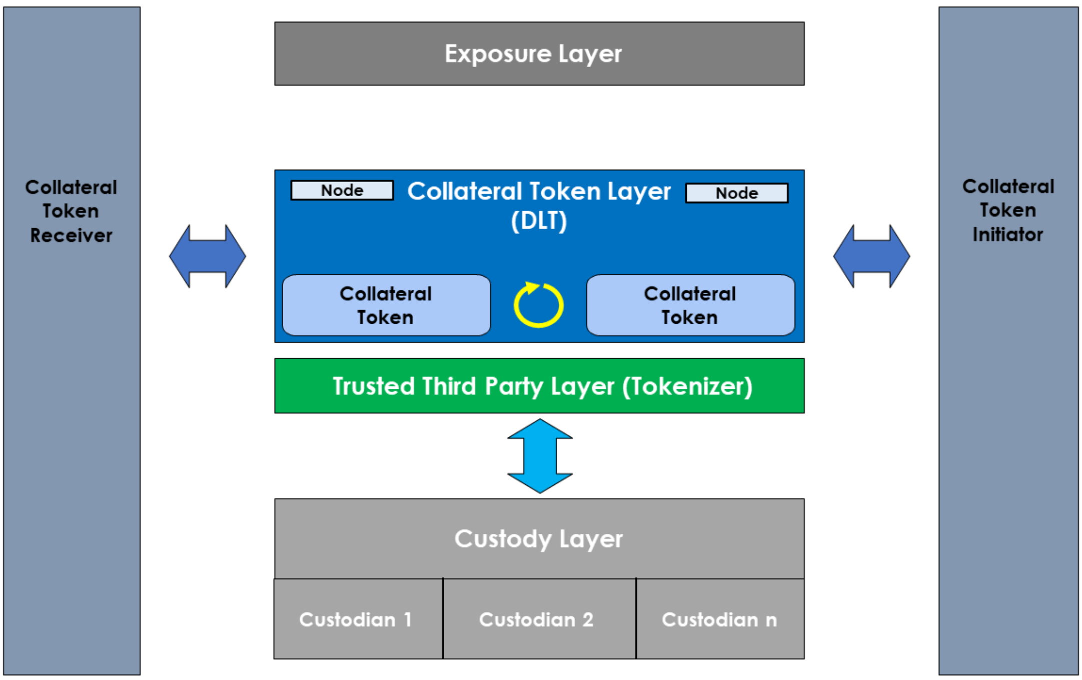
## 4 What Could a Future Operating Model Look Like?

A complementary way to overcome existing inefficiencies is the implementation of an operating model which renders obsolete the movement of securities between custodians. In the model analyzed here, a collateral token managed in a distributed ledger environment is used to record ownership of individual securities or even baskets of securities. The underlying securities remain in an account of a trusted third party (TTP) and are not moved further.

At first glance, as a third party acts as a collateral manager this model may seem similar to conventional triparty services, but de facto goes beyond it. While collateral used for triparty services always has to be mobilized into the custodial account environment of a specific triparty agent (TPA), the TTP model at hand no longer requires collateral movements across different custodians. In addition, once a token has been created it can be directly exchanged between the collateral giver and the collateral taker according to applicable rules.

This DLT-based set-up will allow collateral givers and collateral takers to take advantage of higher collateral mobility. It will remove complex reconciliation efforts necessary between various actors using traditional services for securities settlement and collateral management, which would open the door to substantial cost savings.

The analyzed model is characterized by four different layers. The Exposure Layer describes the exposure that usually arises between counterparties of financial transactions that have to be collateralized. On the Collateral Token Layer, tokens representing securities or baskets of securities will be exchanged. The Trusted Third Party Layer introduces a neutral and reliable trustee which blocks securities held in the Custody Layer and creates representative tokens. The Custody Layer will work as today but provide its services in this model to the TTP.



### 4.1 Exposure Layer

Exposures regularly arise through a variety of underlying financial market activities such as securities lending or repo transactions, OTC swap exposures, CCP exposures or monetary policy refinancing operations. In general, they define risks against a counterparty and are expressed in a cash equivalent value that needs to be collateralized. The present report only looks at exposures between financial institutions.

### 4.2 Custody Layer

In order to secure exposures resulting from financial transactions it is necessary to make collateral available to the respective counterparties. Within the existing market frameworks, eligible collateral which is safekept in accounts at custodians is transferred from the collateral giver to the collateral taker. For this purpose, multiple parties of the custody chain of both the collateral giver and the collateral taker are required to take action.

In the analyzed model the TTP is introduced as a new actor who creates the link between the traditionally issued securities and their tokenized version on DLT. As such the traditional custodian will provide its services – simply said – only to a new customer, the TTP. To allow a wide spectrum of securities the TTP might open accounts with multiple CSDs or global custodians. These accounts could be omnibus accounts as well as segregated accounts depending on local market practices or regulatory requirements.

The initial provision of securities would still need to be performed according to already-established processes and criteria as defined by collateral takers. However, the securities need only to be moved once from the collateral giver's account to the account of the TTP. This can be done as a direct transaction or through triparty services offered by the custodian. Those triparty services comprise in particular the valuation, automatic allocation and substitution of collateral, the triggering of margin calls as well as the release of excess collateral. Once the securities are tokenized, representative tokens can be transferred and re-used without involving custodians or triparty agents.

**Outlook: Considerations Regarding Custody for Digital Securities**

In contrast to securities issued in the traditional way, in the future it can be expected that securities will be issued directly as a native token on a distributed ledger. The safekeeping, transfer and asset servicing for these digital securities (crypto custody) will imply changes for a custodian. While in conventional custody business physical or de-materialized certificates need to be stored and serviced, in the evolving world of digital securities the storage and management of cryptographic keys becomes an important service. In principle, participants of a DLT network can store their private keys themselves. However, this requires high IT security standards and reliable key backup and recovery procedures. Additionally, it becomes even more cumbersome if access to multiple DLT networks for different assets is needed.

It is rather expected that dedicated crypto custody providers which access multiple DLT networks will emerge. Those would allow their customers to hold assets on these networks and store the respective keys. Although currently lawmakers and regulators are still in the process of defining rules for crypto custody and crypto custodians[3], a functional description of various service elements can already be given. Previous work has already been done by the International Securities Service Association (ISSA) and its analysis for an "Infrastructure for Crypto-Assets"[4].

For the purpose of this document, crypto custody means services around the new token economies representing digital securities on distributed ledgers, in particular, the administration of holdings and management of public and private cryptographic keys (e.g. generation, redemption and recovery). As well the reporting to customers and to regulatory bodies becomes a core functionality. It can be expected that a crypto custodian will offer value-added services similar to those provided by traditional custodians, e.g. concerning asset management or triparty collateral management services. Given the probabilistic nature of settlement on some public blockchains, specific questions arise around the finality of these transactions. Regarding private chains, finality is not a matter of concern due to their deterministic approach.

Further, the proof of legal ownership of tokens via cryptographic keys becomes a core issue. As the private key enables execution of ownership rights, it remains to be seen how today's traditional custody chains within the multi-layered custody model will be transferred to the custody of digital assets.

From a technical perspective, the participants in the network might not want to maintain their own technical environment but want to outsource this functionality. Therefore, the maintenance of nodes could also become part of the crypto custodian service offering.

Crypto assets might represent full rights and obligations in a purely digital form and hence might become a primary target of potential cyber-attacks. This makes cyber security a matter of highest priority.

## 4.3 Trusted Third Party (TTP) Layer

The core of the conceptual investigation in this paper is the introduction of a trust model as a reliable and neutral link ensuring regulatory compatibility and legal certainty. The TTP connects the Custody Layer with the Collateral Token Layer. This means that the TTP ensures that tokens created on the Collateral Token Layer represent assets traditionally issued, booked and held at depositing institutions[5]. The holder of a token on the Collateral Token Layer can exercise rights related to the assets represented in the token via the TTP.

[3] See 5th Anti-Money Laundering Directive, May 2018 (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L0843&from=EN)

[4] See International Securities Services Association: Infrastructure for Crypto-Assets: A Review by Infrastructure Providers, October 2018 (https://www.issanet.org/e/pdf/2018-10_ISSA_report_Infrastructure_for_Crypto-Assets.pdf)

[5] However, it can be expected that in future securities will also be issued directly on DLT (see Box 'Considerations Regarding Custody for Digital Securities').

To mobilize securities into this system, a client needs to transfer securities to the TTP at the custodian level. From that moment onwards, the TTP maintains the securities for the client and any movement of the representing tokens on the DLT Layer will only change the rights and obligations at the TTP level without affecting the Custody Layer.

The TTP and its clients can maintain accounts with different custodians and are hence able to mobilize and combine client holdings from different depository locations into one token. This facilitates the efficient move of collateral tokens on the DLT Layer.

From a service point of view, some of the functionalities the TTP may need to cover include:

- creation of accounts and ongoing due diligence for custodian banks;
- creation and “loading” of tokens on receipt of securities in traditional systems;
- instantiating and maintaining the link of either (1) a single security (one ISIN) or (2) multiple securities (basket of ISINs) to a token;
- inventory reporting of securities linked to any token;
- recording of token transfers amongst participants;
- redemption of tokens combined with back-delivery of securities on the Custody Layer;
- maintaining and applying eligibility rules for securities generally acceptable to the TTP;
- related to baskets: securities eligibility, valuation rules, triggering of margin calls according to applicable rulebooks.

For the purpose of this paper it is assumed that the TTP will operate as a registered and appropriately licensed legal entity in a specified jurisdiction and is bound to a transparent rulebook. This rulebook will, among other things, specify the rights and obligations of the TTP and the participants as well as the nature and functioning of the Collateral Token Layer that is connected to the TTP. The role and the duties of the TTP are very much dependent on the type of assets and the legal nature of the tokens in question.

## 4.4 Collateral Token Layer

The Collateral Token Layer is a DLT-based peer-to-peer network which maintains the registry of issued tokens and tracks token transfers. The peer-to-peer network consists of multiple nodes which provide the hardware and software necessary for participants to access and use the network. When a token is transferred from one participant to another on the distributed ledger, rights to the underlying collateral (i.e. securities) are also transferred to the new owner according to the TTP rulebook.

### 4.4.1 Application Functionalities

To enable a full token lifecycle, there are multiple functionalities which should be implemented in the analyzed system. The TTP needs to be capable of issuing tokens, while preventing other users from using this function. After creation, all participants must have the ability to transfer their tokens.

Enabling the transfer of tokens also includes the handling of queries regarding current holdings and selecting tokens for spending. To use a token as collateral, a token transfer from the collateral giver to the collateral taker has to be processed. In the specific case of a pledge model, an additional functionality is required: the tokens must be locked so that neither the collateral giver nor the taker can make use of them. If the exposure ends, the token will be released to the collateral giver; if the exposure defaults, the locked token has to be released to the collateral taker.

When securities are safekept for the TTP, corporate actions can occur. To handle these events, there need to be either mechanisms in place which handle them off-ledger or the respective functionalities must be implemented through smart contracts as well.

Finally, to move tokens out of the system, like in the issuing process, the TTP needs to be able to redeem the tokens by either burning or archiving them in a way that renders them incapable of being reused.

In the analyzed system, two types of tokens are considered:

- The “ISIN Token” represents a one-to-one tokenization of a specific security position. Each of these tokens is redeemable against a specified amount or nominal value of a specified security. These tokens need to include an ISIN or an equivalent identifier of the underlying security and an amount or nominal value defining the quantity of the underlying security. The collateral valuation of the token – as defined by the collateral taker – varies according to changes in the value of the underlying.

- The “Basket Token” is redeemable against securities which are included in a specified basket and corresponds to the value specified in the token. These tokens need to include the definition of the tokenized basket and the tokenized value. As is the case with the existing triparty services, the TTP Layer is responsible for the valuation and allocation of the underlying securities. Additionally, the underlying securities can be substituted by other securities included in the basket definition. A distinction can be made between standardized and individually agreed baskets. In contrast to traditional triparty services, which are offered within one custodian, DLT-based basket tokens allow the combination of securities from various custodians where the TTP and the collateral giver have an account.

The underlying DLT network records token creation, transfer and redemption. Both types of tokens need to contain information identifying the owner of the underlying security. Additionally, to achieve fungibility, users need to be able to split and merge tokens. To merge ISIN tokens, the original tokens need to have the same underlying ISIN and the same legal status in regard to ownership. The new merged token would inherit these properties from the original tokens. When splitting tokens, consideration should be given to a “Minimum Settlement Unit,” which sets a lower bound on the size of the new tokens.

### 4.4.2 Additional Design Considerations

To decide about the specific technical implementation for the analyzed model, the business requirements for scalability, privacy, security, accessibility for users and compliance with existing regulations have to be considered. Additionally, the governance of the platform is an important issue.

## Scalability and Performance

Scalability and performance are crucial aspects for business and technology decisions, given that transaction systems can affect critical business processes. Key elements regarding the technical design are data structure, degree of system integration, privacy level and consensus algorithms. These have a direct impact on the scalability and performance of a DLT system. The number of nodes can affect the speed and complexity of consensus building. Therefore, the current number of collateral users and the potential growth in network participants and transactions need to be carefully evaluated while designing and developing the analyzed system. Previous studies have already concluded that current major DLT frameworks such as the Digital Asset Platform, Hyperledger Fabric and R3 Corda are capable of processing current financial transactions and respective volumes[6].

## Privacy

Privacy is defined as the right of each individual or legal entity to control the degree to which they are willing to share their personal or business information. In the highly competitive financial market, nearly all information is sensitive. Therefore, any privacy policy has to follow a strict "need-to-know" principle which ensures that all information is only distributed to the relevant parties; at the same time, individuals or organizations are prevented from accessing private data. Sensitive data must be encrypted using certified encryption methods. An optimal solution would also take "forward secrecy" into account, protecting against the possibility of an encryption method being compromised in the future. One way to achieve that is by distributing even encrypted information only on a "need-to-know" basis.

## Governance

To properly operate in a regulated environment, the analyzed system needs to have a governance structure. Network participants have to agree on a common platform rulebook and terms of use. Major incidents in the public blockchain sector have made it clear that the "code is law" doctrine is questionable in practice. A governing body is needed to design the system architecture and to define and deploy code, including smart contracts. In addition, there needs to be an authority (e.g. network operator) which manages the admission and permission of participants according to the rulebook (e.g. access rights, read/write abilities, exclusion of participants).

## Access Control and Identity Management

In regulated financial market activities, actors need to adhere to strict KYC or AML laws and other regulatory guidelines. For the given scenario, this implies the application of a private permissioned network, where every participant is identified and needs permission to use the service. In general, as part of the onboarding process, a specific network operator registers the public keys of the permitted participants in a whitelist. For privacy reasons the legal entities behind the public addresses in the whitelist might not be known to other participants. To prove identity to other participants for transacting, the system could include a certificate agency and use certificates instead of a static public

[6] See BLOCKBASTER Final Report (https://www.bundesbank.de/resource/blob/766672/29feab3f9079540441e3abda1ed2d2c1/mL/2018-10-25-blockbaster-final-report-data.pdf)) and DTCC press release (http://www.dtcc.com/news/2018/october/16/dtcc-unveils-groundbreaking-study-on-dlt), Oct 2018

key either on a per transaction basis or with limited time validity. Access control serves a regulatory and organizational role which naturally remains centralized. Participants in a private network who violate network guidelines can be expelled from the network. Through these identifying features, the participants' behavior is traceable and auditable, which is essential for regulators.

### Monitoring and Reporting

The network operator should be responsible for monitoring platform health and performance and detecting malicious behavior of nodes. In the latter case, the network operator should also have rights to intervene according to a predefined ruleset. Transaction data should be consistent, and mechanisms must be developed and put in place to prevent fraud and attacks such as double-spending or Denial-of-Service.

For regulatory or supervisory purposes, an Observer Node can be set up which observes the network passively for real-time view of collateral ownership. Additional risk monitoring and reporting applications can be developed to simplify the reporting process and enhance regulatory transparency of the collateral market.

### Node Hosting

Participants interact with the distributed ledger through network nodes. The more nodes the network has, the more pronounced the advantages of a distributed network generally are. Participants can run their own nodes, in which case they need to fulfill certain technical and operational requirements to ensure network security, availability and stability. Alternatively, they have the option to access the network through another participant's node or a node hosted by an approved third party.

### Security

The security policy has to be extended to the network level in addition to the access control and identity management described above. For example, both inbound and outbound internet traffic have to be filtered and monitored. A multi-level firewall has to be implemented on every node. Peer-to-peer communication between nodes has to be secured and encrypted. A Hardware Security Module (HSM) has become a standard to manage the digital keys. To further reduce risk, nodes can also be distributed physically and geographically.

### Outlook: Considerations Regarding Cash in Collateral Management

Within existing collateral management arrangements, cash is an integral element. It is either used as collateral itself or in repo-style transactions as a countervalue to the securities. Cash is available within already established payment systems; the challenge is therefore to integrate cash in a distributed ledger environment.

Cash is usually maintained and transferred within a variety of payment systems of central banks and/or commercial banks involving so-called correspondent banking relationships. Going forward, cash could increasingly be made available for processing within distributed ledger environments. Two options can be considered. Either existing payment systems can be made interoperable with a distributed ledger, or cash can be digitized and directly recorded on a distributed ledger. The latter can either be on-chain issued tokens - so-called native cash tokens – or tokens that represent "classic" cash which is safekept in traditional payment systems and transformed by a tokenizer. In the context of this paper, only these fully backed tokens are regarded as recoverable collateral[7].

If an interoperability solution with an existing payment system is chosen, a technical interface with the distributed ledger processing the securities leg of a transaction would be required. The interface should allow for a payment message to be initiated and processed in the payment system while securely blocking the collateral on ledger. Depending on the successful execution of the payment leg, the blocked collateral tokens could be released and transferred to the beneficiary – conditional settlement would take place. Settlement finality only occurs if both legs (security tokens and cash) are successfully settled. Otherwise, the transaction is rejected. Depending on the specific solution, settlement finality could be achieved close to real time. The implementation of such a model would, however, require a deeper investigation of conditions and requirements (e.g. prolonged opening times and standardized message formats).

Alternatively, if the cash tokens were to be created directly on chain, settlement finality could be achieved instantaneously. If the cash token and the securities token are on the same chain, settlement finality is achieved in a single medium simultaneously for both legs of the transaction. If the cash token and the security token are on different DLTs, as in the interoperability solution, the transactions will need to be coordinated between the different chains e.g. by two-phase/three-phase commit or hash time lock contracts. Finality is only achieved once both chains have confirmed their final step in the execution of the transaction.

# 5 Legal Considerations

## 5.1 General Remarks

A fundamental precondition for the use of distributed ledger systems in collateral management is legal soundness. This comprises the compliance of the technical system with the current regulation regarding the finality of transfer orders. Moreover, all requirements faced by its stakeholders, whether they stem from banking, securities markets and infrastructure regulation or other fields such as accounting principles, have to be complied with. Further, the legal nature of the tokens is a basic attribute which needs to be clarified.

Currently, in the absence of a specific regulatory framework for a token economy, all actors must ensure that their token activities comply with the “traditional” rules and regulations applicable to their respective field of business. This means seeking legal opinions and making individual inquiries with their regulators. Since the token economy is not yet mature, many jurisdictions are just beginning to formulate legal frameworks regulating tokens and the associated activities. In the European Union a first effort has been made to implement a coordinated framework in the form of the current version of

[7] The classification as either central bank money or commercial-backed money and other legal questions regarding such tokens are beyond the scope of this study.

the Anti-Money Laundering Directive[8]. However, there remain differences in national jurisdictions of member states. Therefore, actors must rely on national legal frameworks where they exist or use contractual arrangements as a legal framework instead. In addition, technology-agnostic regulation for certain existing products may also apply to new offerings on a DLT basis.

## 5.2 Legal Classification of Tokens

A key question is which rights and obligations are represented by a token. Three broad legal concepts for the nature of a token can be distinguished. Those determine the requirements that must be fulfilled from a legal and regulatory point of view by the various actors of a specific DLT set-up.

The following discrete categories should be considered for tokens related to securities:

(1) Information Token

The least extensive category would be where securities are stored in conventional legacy systems (i.e. a custodian-controlled database, a vault, etc.) and corresponding tokens just carry specific information on these securities. The information stored in the legacy system would take precedence over the information stored on the DLT. And the factual control over the token, or more precisely, its transfer from one participant to another, would not entail a transfer of any rights or obligations with regards to the corresponding security.

(2) Extended Token

In the second category, the same information stored on the DLT would take precedence over the information stored in the legacy system. Control over the security token would provide evidence of rights/obligations regarding the corresponding securities (like for example ownership of the security). However, while control over the token would only *indicate* e.g. ownership, it indirectly *affects* it through an additional legal construct like for example a TTP which ensures that ownership of the security and control over the corresponding token do not diverge. This is because the main legal reference object would still be the security existing outside the DLT Layer.

(3) Native Token

The third and most consequential category would therefore mean the security in total is issued in the form of a token and therefore carries all information as well as all rights/obligations to the security. The legal reference object would be the token and the DLT system itself; any change in token ownership would also automatically trigger legal consequences.

The issuer or creator of the token needs to define the nature of the token in its respective rulebook. The model at hand relates to “(2) Extended Token”.

[8] The 5th EU Anti-Money Laundering Directive (Directive (EU) 2018/843 of 30 May 2018) introduced a definition of cryptographic values (in the Directive: “virtual currency”) and made the safekeeping of cryptographic values subject to certain supervisory requirements.

**Securities represented on a DLT**

| | 1<br>Information Token | 2<br>Extended Token | 3<br>Native Token |
|---|---|---|---|
| ‚Nature of the token' | ▪ Digital twin carrying information only, no legal rights | ▪ Digital twin certifying certain rights and obligations | ▪ Original asset carrying all information and all rights and obligations |
| Location of security | ▪ Off-DLT | ▪ Off-DLT | ▪ On-DLT |

## 5.3 Legal Classification of the Stakeholders Involved

The collateral taker and collateral giver need to acknowledge tokens and need to trust both the technological and functional set-up. Specific regulations facing them in their roles as giver and taker of collateral in the form of tokens are currently often not available or in an early stage of development.

More complex is the role of the TTP. The TTP provides services which are comparable to those of a custodian. It holds securities on behalf of the beneficial owners at one or even multiple custodians and allows the beneficial owner to transfer ownership of these securities through the transfer of tokens. As in the case of a traditional custodian, insolvency of the TTP should not affect the holdings of its customers. It has to be guaranteed that the TTP does not misuse the securities of a customer and makes sure that all tokens are backed by securities.

Following the principle of “same risk, same rules”, regulators might think about treating TTPs similarly as custodians. In the absence of regulation for TTPs, trust must be established by incorporating these rules in the contractual set up.

A further function of great importance in a DLT network is the operation of the IT infrastructure; this includes e.g. the definitions and oversight of hardware and software or IT security and business contingency measures. The operator of such a DLT network could well be a specialized provider of IT services who has no role in providing financial services. However, such a service provider also needs clear governance and liability provisions.

## 5.4 Legal Obstacles Posed by the Current Regulatory Environment

The current regulatory environment has grown over many years and is designed to regulate actors and services regardless of the technology used. The challenge in regulating DLT activities is not so much the new technology but the new business models they allow.

The current regulatory environment affects entities which render financial services and assumes that these entities also maintain the relevant IT infrastructure. Where they outsource any IT activities, they still remain responsible and have to ensure that applicable regulations are also met by their subcontractors.

Therefore, there will be operators to be regulated even though they might only provide IT services like the maintenance of the DLT network while financial services are provided by the actors using the DLT network. Nevertheless, there is already practical experience with overseeing these so-called Critical Service Providers[9] which could be applied to DLT operators as well.

Another aspect is that a distributed ledger system used to settle securities might be classified as a "Securities Settlement System" (SSS)[10] and the functional operator would therefore need to adhere to the respective requirements.

**Outlook: Considerations Regarding Eurosystem Requirements for the Mobilization of DLT Collateral Assets**

All credit operations of the Eurosystem are required by its statute to be based on "adequate collateral". Collateral must be able to protect the Eurosystem against losses in the event of a counterparty default. The Eurosystem's legal framework for monetary policy instruments specifies the criteria for the eligibility of assets determining which assets can be used as collateral for monetary policy operations and which risk control measures the Eurosystem has introduced.

In addition, as the provision of eligible collateral does not eliminate credit, market and liquidity risk, the Eurosystem has a specific risk management framework in place. It consists of four risk mitigation elements: (1) the Eurosystem's Credit Assessment Framework (ECAF) which includes measures to mitigate credit risk, (2) the Eurosystem valuation framework specifies how collateral is valued to minimize interferences with market prices, (3) the Eurosystem haircut framework defines specific valuation haircuts, (4) other risk control measures such as variation margins, limits on the use of collateral or even the exclusion of specific closely linked assets aim to further mitigate specific risks.

The collateral and risk management framework, which regularly undergoes amendments, would also apply in case DLT-based collateral assets might be eligible for use with the Eurosystem. In addition to these eligibility criteria and risk management measures, the Eurosystem has defined specific requirements with regard to the mobilization of eligible assets. Currently, when mobilizing eligible marketable assets to the Eurosystem, counterparties make use of eligible SSSs operated by eligible CSDs, eligible links between such CSDs or eligible triparty agents. In order to ensure the safety and efficiency of these infrastructures, the Eurosystem has defined specific eligibility criteria that have to be fulfilled when the respective CSDs, SSSs and links between them or Triparty Agents (TPAs) are used. If DLT-based collateral assets were to become eligible for use in Eurosystem credit operations, these criteria would remain valid to ensure that - before and whilst being tokenized, - these assets are safekept under Eurosystem rules. Provided that an operational model as considered in this paper is

[9] CPMI/IOSCO Assessment methodology for the oversight expectations applicable to critical service providers; December 2014.

[10] Securities Settlement System as defined in the Directive 98/26/EC of the European Parliament and of the Council of 19 May 1998 on settlement finality in payment and securities settlement systems.

applied, additional eligibility criteria will be needed at least regarding the TTP to also ensure safety and efficiency for this potential new mobilization channel. These criteria are likely to be closely aligned with existing standards for TPAs such as:

- insolvency-proof claim to securities held with TTPs and pledged to central banks, obligations of TTPs vis-à-vis central banks, liability regime, etc.;
- settlement of corporate actions, substitution of collateral and retention of funds from corporate actions;
- compliance with the Eurosystem eligibility criteria for collateral and their mobilization channels;
- realization of collateral;
- risk management;
- confidentiality of data.

In addition, there might be requirements for the custodians of the TTP with regard to access rights required in the event of a TTP failure to the accounts on which the deposited securities are held. Specific requirements on the DLT Layer for availability and corresponding contingency methods for redeeming the tokens in the event of non-availability might also be of importance.

To conclude, there is still the need for further legal analysis and assessment prior to the acceptance of DLT collateral assets as eligible collateral for Eurosystem credit operations.

## 6 Conclusions

Several financial institutions and market infrastructure providers have already investigated distributed ledger technologies. Prototype systems have been built and tested in various proof-of-concept studies; first use cases are in the process of being implemented. Over time, the underlying protocols have become more and more mature and suitable for the processing of financial transactions. It is expected that distributed ledger systems will become more common in the financial industry due to their potential for delivering efficiency gains and new business opportunities.

The intention of the paper at hand was to analyze in more detail the appropriateness of distributed ledger technology in the context of collateral management. Since the financial crisis, the importance of collateral management arrangements has grown due to regulatory requirements and increased risk aversion of market participants. Consequently, collateral has become a concern of financial markets focusing on the aspect to put the right collateral at the right time at the right place. This is why we as a central bank and an infrastructure provider are working on this subject.

Collateral mobility has already begun to derive benefits from several Eurosystem projects and initiatives such as T2S or the usage of triparty collateral management services. Other gaps have been addressed by the Collateral Management Harmonization Standards of the Eurosystem’s AMI-SeCo. However, the associated adaptations made by market participants in order to harness these opportunities will need time for their impact to fully unfold. In addition, it remains to be seen whether the necessary business policy decisions will actually be made by relevant parties or whether persistent forces predominate, and no corresponding adjustments are made.

A complementary option enabling more efficient mobilization of collateral is the use of distributed ledger technology. With the introduction of tokens representing underlying securities and specific related rights, collateral can be mobilized without moving underlying securities in the related custody environments. This opens up the opportunity for efficiency gains as cost- and time-intensive reconciliation processes become obsolete. Another substantial benefit is the combination of the client's traditional securities holdings with different custodians into one collateral token.

From a custody perspective, a distributed ledger system has the capability to record positions at an end-beneficiary level. This increased transparency and resulting operational efficiencies open up opportunities for service providers alongside the custody chain.

On the technical side, decentralized data management of distributed ledger technology enables extended system availability potentially around the clock, every single day. Currently, international financial market activities are limited by settlement windows which usually prevent trades from being settled during the night in the specific time zone. One of the reasons for this limitation is to allow for maintenance and system housekeeping. In contrast, due to its distributed nature, a DLT-based system is innately capable of allowing maintenance to be done on a single node without affecting the availability of the full system. In this way global integration of financial market activities could be further fostered.

To allow the full potential of this technology for the financial industry to unfold, legal and regulatory aspects need to be tackled as a matter of priority. Market participants need leeway for further analysis and investigation to develop new business cases as well as legal reliability and certainty to integrate these new services into the productive environment. Therefore, European lawmakers and regulators need to ensure that coordinated and harmonized laws and regulations are put in place within a short timeframe.

Relevant actors in the securities services industry are closely interlinked and bound by existing regulation. Hence, changes regarding the actual business models are much more likely to evolve gradually over time. Accordingly, it is not expected that securities issuance in its entirety will happen via tokens in the short term. Instead, there will probably be more intermediate use cases utilizing tokens as a mere carrier of information or using them to represent claims.

Another key element is whether and when market participants will be able to integrate DLT-based solutions into their existing technical environments. Given that existing well-functioning traditional systems will not be replaced soon, it is expected that they will run in parallel with new solutions reaping the benefits of DLT. For the time being, the challenge will be to efficiently interface both worlds.

In addition, internationally agreed market standards would be helpful for the market to develop efficient business solutions. Standardization would be required from both the functional and the technical perspective. This could be common identifiers for tokens or communication standards between different chains.

Finally, disintermediation is always seen as an issue when discussing distributed ledger technology. However, regulation of services and actors in the trading and post-trading sector constitute a limitation for such disintermediation. In the end some functionalities and roles in the current value chain might be reduced or will even no longer be required with DLT. However, as shown in the analysis with the example of the TTP, it can be expected that - with the evolution of this innovative technology - various new roles will develop instead.

## Glossary

**Consensus Algorithm**
A process, encoded in software, by which nodes in a network agree on validity and order of transactions appended to the ledger

**Delivery versus payment (DvP)**
A DvP transaction involves the settlement of two linked obligations, namely the delivery of securities and the payment of cash. DvP avoids counterparties being exposed to principal risk, i.e. the risk that the seller of securities could deliver but would not receive payment or that the buyer of securities could make payment but would not receive delivery.

**Denial-of-Service (DoS)**
A Denial-of-Service attack is a very common method of cyberattack. By sending large amounts of requests to a server in a very short time, the server is not able to keep up with processing the requests and eventually crashes. If the requests are sent from multiple different computers and connections, it is also called a Distributed-Denial-of-Service (DDoS) attack.

**Double-spending**
Double-spending is an attack where a given set of coins or digital tokens is spent in more than one transaction.

**Finality**
Finality is a state of a transaction at which point it is guaranteed to be irreversible. In most cases finality refers to deterministic finality which describes a state where there is no possibility of reversing the transaction. In contrast to that, most public blockchains can only reach probabilistic finality, which is defined by the point in time at which the probability of a transaction being reversed is tiny enough that it is reasonable to assume that the reversal is never going to occur.

**Hardware Security Module (HSM)**
A Hardware Security Module is a device which enables encryption which can only be performed with physical access to it, eliminating the possibility of a remote cyber-attack.

**Hash time lock contract (HTLC)**
HTLC is a conditional transfer agreement of certain assets where the condition is enforced by the underlying protocol. Time-lock ensures that a transaction is time-bounded: the recipient only has a certain amount of time to accept the payment, otherwise the asset is returned to the sender. Hash-lock prevents counterparties of a transfer to claim the intended assets without fulfilling the conditions stated in the transaction agreement. The combination of hash-lock and time-lock ensures secure asset transfer and can be used for delivery versus payment between different chains/protocols.

**Network Operator**
The Network Operator is both a technical and a business role. Technically, the network operator is responsible for the infrastructure and makes sure that the nodes can connect to each other. It is also responsible for handling any technical failures which are not limited to one node. On the business side, the Network Operator is responsible for the institutional setup between the participants, it grants and revokes permissions, authorizes updates and handles other necessary auxiliary processes.

**Node**
In the context of blockchain systems, nodes are the peers of the peer-to-peer network which can take on different logical roles. A "node" is a logical function in the sense that multiple nodes of different types can run on the same physical server. If a node is maintaining a full copy of the distributed ledger it is usually referred to as a "full node".

**Public Key**
A unique string of data which can be used to encrypt data that can then only be decrypted by the corresponding private key. The public key can also be used to decrypt data that have been encrypted by the corresponding private key. This property can be used to identify the sender of a message within a network. It can be shared publicly.

**Private Key**
A unique string of data which can be used to decrypt data that has been encrypted by the corresponding public key. The private key can also be used to encrypt data that can then be decrypted by the corresponding public key. This property can be used as a proof of identity within a network, for example the right to access and own that participant's wallet within a cryptocurrency. It can be compared to a personal password which must be kept secret.

**Smart Contract**
A computer program stored in a blockchain that can be executed by participants of the blockchain system. It serves as a way to create a mathematically guaranteed promise between two parties.

**Token**
Tokens are a digital representation of one or more assets or rights. Tokens can represent basically anything, not only cash and securities, but also real estate or precious metals. Security tokens are units of value which represent similar rights to those of a security and therefore are usually treated as such.

**Tokenization**
The issuance of a digital representation, called token, of a certain good or right after locking away the good/right in the existing ledger.

**Triparty agent (TPA)**
Triparty collateral management services (TCMS) provided by triparty agents (TPAs) allow market participants to optimize the use of their securities portfolios when collateralizing credit and other exposures stemming from different products and instruments (e.g. repo, securities lending, central bank credit, secured loans and exposures arising from CCP or OTC transactions).

**Two-phase/Three-phase commit protocol**
Two-phase or three-phase commit protocols are algorithms which let all nodes in single or multiple distributed systems agree upon a transaction and its related conditions. The protocol ensures that the transaction is committed, otherwise it will undo the changes which is also known as a rollback.

**Wallet**
A software program capable of storing and managing public and private key pairs used to access digital assets.

Contacts

Deutsche Börse: thomas.wissbach@deutsche-boerse.com

Deutsche Bundesbank: antje.heikamp@bundesbank.de