EUROPEAN CENTRAL BANK

EUROSYSTEM

The use of DLT in post-trade processes

Advisory Groups on Market Infrastructures for Securities and Collateral and for Payments

April 2021

Contents

Executive summary

In the current fast-changing environment, the adoption of solutions based on distributed ledger technology (DLT) could bring both opportunities and challenges for the financial ecosystem and its stakeholders.

Various institutional actors, such as governments and central banks, are actively undertaking initiatives to investigate and develop potential DLT-based use cases. In addition, market players are experimenting increasingly with the technology, despite the current lack of common practices and standards. While the diverse nature of the initiatives is likely to result in a wide range of different findings and is part of a competitive mechanism in the initial phase of a new technology, it also entails the risk of market fragmentation and potentially of a delay in progressing towards a capital markets union[1].

Market changes prompted the advisory groups on market infrastructures (AMIs) to carry out an analysis. To this end, the Fintech Task Force (Fintech-TF) was established, made up of stakeholders from the European post-trade industry. Over the last three years the Fintech-TF (continuing the work of the former Task Force on Distributed Ledger Technology, DLT-TF) has carried out an initial assessment of the potential impact of the use of DLT in a post-trade environment[2]. It has subsequently identified possible use cases[3] to support the potential development of shared standards for interoperability in the post-trade area.

The present report has been prepared also on the basis of previous work carried out by the AMIs. It is part of the efforts to monitor the potential impact of financial innovation on securities post-trade processes. The report seeks to establish a common understanding among European stakeholders of the progress that the industry has made to date in implementing DLT in line with the current regulatory system.

Focusing on current use cases for equities and bonds, the report describes different types of securities issuance and post-trade processes. These are categorised according to different "models" depending on how DLT is used in each instance. The report also assesses the implications of using DLT on the basis of identified market practices.

The report concludes that the adoption of DLT-based solutions could be driven by projected cost savings and efficiency gains. Nevertheless, the use of DLT would entail similar challenges to those faced by solutions relying on conventional technology (such as fragmentation and interoperability issues) and would potentially create new ones (for instance relating to the legal validity of tokens). Additional costs and

---

1 See Capital markets union 2020 action plan: A capital markets union for people and businesses.

2 See the AMI-SeCo report entitled "The potential impact of DLTs on securities post-trading harmonisation and on the wider EU financial market integration", September 2017.

3 See the AMI-SeCo report entitled "Potential use cases for innovative technologies in securities post-trading", January 2019.

barriers – alongside the existing hurdles – should be avoided when adopting DLT-based solutions.

To mitigate risks of fragmentation and interoperability, a first step is to identify a common technology-neutral taxonomy aimed at enhancing clarity also in terms of the regulatory framework. Consideration should then be given to specific DLT features, to the extent that they may also change the dynamics of current functions, as related life-cycle activities and tasks might be managed on or off the network and aggregated into “smart contracts”.

In addition, DLT-based solutions should be underpinned by strong governance, with interests aligned and properly monitored. This would, for instance, provide an incentive for the wide-scale adoption of the innovative technology while ensuring safety and common rules. Market standards have a critical role to play. In the same way as for incumbent systems, interoperability remains critical in a DLT environment both for (i) migrating efficiently from an incumbent system to a DLT-based system and (ii) connecting DLT-based systems and incumbent systems on an ongoing basis.

The report is structured as follows. Chapter 1 outlines regulatory, governance and interoperability aspects identified in the context of DLT-based solutions. It also outlines key elements in the regulatory framework, defines potential new functions in the DLT environment and explains the concept of interoperability used in the report. Chapter 2 describes two DLT models and their key functionalities. Chapter 3 addresses the key implications of using DLT at different stages of the securities life cycle, from issuance to custody and settlement.

Examples identified in the market are presented in the annexes. Annex 1 illustrates the models by highlighting the key components of specific solutions being implemented in the market, while Annex 2 describes key examples of how interoperability can be ensured in DLT-based solutions.

1 Regulatory, governance and interoperability considerations in a DLT environment

This chapter identifies the key regulatory aspects relating to use of DLT in the post-trade environment in the light of actual market practice.

1.1 Key considerations on digital assets and the related regulatory framework

This chapter identifies the key regulatory aspects relating to use of DLT in the post-trade environment in the light of actual market practice.

1.1.1 Taxonomy related to issuance and tokenisation of assets

The principle of technological neutrality suggests that the use of a given technology, such as DLT, should not be seen as a distinguishing feature for identifying a new category of assets. Instead, classification should continue to be based on the intrinsic risks and characteristics of the activity and the reference market. For instance, financial market regulation considers the inherent financial and investment features of an asset in order to classify it as a financial instrument or, more broadly, as an investment product. Where initiatives leverage DLT-based solutions, they should have a well-defined scope and features that provide clear guidance as to which regulatory framework is applicable.

The existence of a taxonomy for securities in a DLT environment is pivotal to understanding the landscape of digital assets. However, the categorisation of assets available on distributed ledgers still poses significant challenges for market regulators.

In its previous report on the potential impact of the use of DLT in a post-trade environment[4], the Advisory Group on Market Infrastructures for Securities and Collateral (AMI-SeCo) drew a clear distinction between the two concepts of (i) a security that is native to a distributed ledger (a native digital asset) and (ii) a reference to a security which has already been issued and recorded (e.g. in a register as is

[4] See the AMI-SeCo report entitled "The potential impact of DLTs on securities post-trading harmonisation and on the wider EU financial market integration", September 2017.

currently the case) and is kept outside a distributed ledger while being represented (by its token) on a distributed ledger.[5]

The classification of securities must therefore take into account the relevant elements of the asset issuance model, i.e. whether the asset at stake is referenced by a token on a distributed ledger and whether it confers any claims. Another key feature for the identification of an asset is the presence of an entity responsible for the issuance of the token and the intrinsic value it represents.[6] To develop the use of DLTs and promote cross-border transactions with a view to completing a European capital markets union, it is important to foster a harmonised approach to the issuance of digital assets and to tokenisation. In most EU countries, the regulatory basis for the issuance of native digital assets and for tokenisation does not yet exist. Different jurisdictions have tried to address this with new legislation or by clarifying the existing regulatory framework (Table 1).

Table 1

Digital assets in national jurisdictions of some EU Member States

Country	Developments
France	Under Ordonnance n° 2017-1674[7], securities credited to the distributed ledger have the same legal effect as a book entry in a securities account in terms of the transfer of holdings.
Luxembourg	A bill of law[8] enables the use of secured distributed registers, electronic ledgers and databases for the issuance, registration and circulation of securities without altering the regulatory framework and requirements for the security itself.
Italy	It is established under law[9] that storing a document on distributed ledgers produces the legal effect of an "electronic time stamp" as defined in Article 41 eIDAS Regulation[10].
Germany	The German government recently published a draft law with a focus on the concept of electronic securities[11]. This is intended to provide the possibility of issuing securities without issuing a certificate representing these securities, while ensuring in principle that these securities are subject to the same legal requirements as securities represented by a certificate, including the requirements relating to entry into specific registers and disclosure obligations.

In this regard, the recent proposal for a European Regulation on Markets in Crypto-assets (MiCA)[12] and the proposal for a European Regulation on a pilot regime for market infrastructures based on distributed ledger technology[13] include provisions

5 For the purposes of this report, it is therefore understood that, in a securities markets environment, a token merely represents a security which has been issued and recorded in a central securities depository (CSD) and continues to be kept in the legacy system or vault of the CSD. Meanwhile, a security that has been issued, recorded and kept solely on a distributed ledger as a native digital asset should be subject to the current regulatory framework in the very same way as a security issued in a conventional environment.

6 In line with ECB's approach in Bullmann, D., Klemm, J. and Pinna, A., "In search for stability in crypto-assets: are stablecoins the solution?" *Occasional Paper Series*, No 230, August 2019.

7 Ordonnance n° 2017-1674 du 8 décembre 2017 relative à l'utilisation d'un dispositive d'enregistrement électronique partagé pour la représentation et la transmission de titres financiers.

8 7363 – Projet de loi portant modification de la loi modifiée du 1er août 2001 concernant la circulation de titres.

9 Legge 11 febbraio 2019, n. 12 and Decreto-legge 14 dicembre 2018, n. 135.

10 Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p. 73).

11 Entwurf eines Gesetzes zur Einführung von elektronischen Wertpapieren.

12 Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937.

13 Proposal for a Regulation of the European Parliament and of the Council on a pilot regime for market infrastructures based on distributed ledger technology.

on the issuance and recording of “crypto-assets” and “DLT transferable securities” as defined in the texts of the proposals. Both proposed definitions are linked to some extent to the definition of financial instruments provided by the Market in Financial Instruments Directive (MiFID)[14]. Therefore, their qualification from a regulatory perspective may vary across different jurisdictions, considering that MiFID II[15] has been transposed in slightly different ways in the individual Member States. From the perspective of market players, further analysis will be needed in order to understand how these proposals will fit into the current financial regulatory framework (both at EU and domestic level) and what the implications for the market will be.

1.1.2 Custody: clarifying the function of holding private keys in safekeeping

The concept of private keys is not new to the financial system, as it is common to several solutions which do not rely on DLT. However, there is no common understanding of the implications of using private keys in the context of DLT-enabled custody services[16]. Some argue that custody services would primarily be a matter of holding private keys in safekeeping. Others consider private keys only as a technical feature to produce digital signatures, as keys constitute neither a means of safekeeping nor proof of ownership, and nor do they provide for the validation of a transaction. In the latter case, it would mean that a custodian of private keys would not have the same ability as a custodian of traditional securities on the basis of specific design features (e.g. regarding the set-up of the transfer instruction).

In general, rules on the transfer of securities and enforceability of rights are based on systems for holding “intermediated securities” and imply the existence of bilateral relationships between the account holder and intermediaries along the custody chain (usually characterised as “deposit/custody” relationships, depending on the applicable law). Rights on intermediated securities are usually constituted through the crediting of securities to the account of the holder/beneficial owner. In this case, the intermediary has a deposit relationship with the account holder/beneficial owner, who can transfer the securities only through intermediaries. The compatibility of such rules in a DLT context, where transfer is usually intended to would take place directly on a peer-to-peer (P2P) basis, would need to be tested and clarified, given that these areas of law are largely based on local rather than harmonised legislation. This does not mean that ownership of securities on a distributed ledger cannot be

---

14 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 of the Council and repealing Council Directive 93/22/EEC, (OJ L 145, 30.4.2004, p. 1).

15 Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (OJ L 173, 12.6.2014, p. 349).

16 In this regard, the German Federal Financial Supervisory Authority (Bundesanstalt für Finanzdienstleistungsaufsicht – BaFin) has developed an approach towards the issuance of securities on a distributed ledger without the application of laws on custody of paper certificates or centrally registered securities, as set out in the German Depotgesetz (Safe Custody Act) or the Central Securities Depository Regulation (CSDR). Such issuance is possible with the concept of the “security of its own kind”. For more details, see Crypto custody business.

intermediated, but intermediation is expected to happen outside the DLT network that is used for settlement.

Another key point for discussion is whether custody of tokens representing securities is limited to the safekeeping of private keys, which would change the current service model and related responsibilities. Rules for the safekeeping of private keys for individual custody of securities certificates should also address the need for preserving principles and safeguards related to know-your-customer (KYC) rules, anti-money laundering and combating the financing of terrorism (AML/CFT) and consumer protection.

1.1.3 Settlement: use of DLT and its implications

A first aspect relates to the implications that finality would have in the context of using DLT, taking into account the applicable framework and the identification of "finality" in a decentralised environment. The lack of recognition by each Member State of the equivalence between the digital form and the dematerialisation of the financial instrument may create uncertainty for market participants and hinder (cross-border) transfer of securities via DLT. A harmonised approach with equivalence recognition among all Member States is essential for the development of DLT securities at EU level.

In addition, a DLT network requires different coordination and synchronisation processes for ensuring consistency and transparency on information that is provided. The production of information data as a result of the consensus mechanism, for example, may lead to the system itself being the owner of the data produced in the form of encrypted information and, as a consequence, being responsible for the use of the data in compliance with the current regulatory framework (which may vary according to the jurisdiction(s) – multiple jurisdictions may even be involved at the same time). In this context, it remains to be understood to what extent the General Data Protection Regulation (GDPR)[17] would apply to networks and nodes from different jurisdictions, i.e. EU and non-EU.[18]

1.2 Governance of DLT-based systems

The transition from a traditional system to a DLT environment is expected to require a new model of communication. A shared communication model enabled by DLT may entail the replacement of the current sequential way of communicating and exchanging information as well as the identification of new functions in the financial

[17] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (OJ L 119, 4.5.2016, p. 1–88).

[18] In particular, data shared within the network may be subject to the GDPR. For example, in blockchain, the public key is shared to the network, and it is possible to link it to its identifiable owner. On this topic, see the briefing by the Scientific Foresight Unit (STOA) of the European Parliamentary Research Service entitled "Blockchain and the GDPR: Can distributed ledgers be squared with European data protection law?".

markets. Some of the relevant functions may depend on the specific configuration, key features and nature of the DLT network, as well as the status and jurisdiction of the providers. In this context, additional functions are likely to be identified alongside the existing ones. The provision of regulatory licences and authorisation should therefore be carefully considered in order to ensure sound governance and create appropriate incentives. Regulation should also clarify how DLT-specific functions could be integrated and/or segregated in the existing framework, along with how to apply conduct of business rules and manage conflicts of interest. A high-level description of functions in a DLT environment is provided below.

1.2.1 Issuance of digital assets and asset tokenisation

Compared with "traditional" issuers, issuers of digital assets need to adopt new technological structures and develop advanced competencies to fulfil their roles and functions as both issuers of digital assets and nodes of the DLT network. In order to ensure efficiency, this function can be outsourced to a third-party provider, especially for the issuance of native digital assets. The function of asset tokenisation could include the possibility of performing activities such as corporate actions and the execution of dividend payments in the smart contract code.

1.2.2 Custody digital assets and tokens

As digital assets emerge, existing tools for custody may require the deployment of new technical solutions while adapting the offering to address the risk of misappropriation of those digital assets. One of these activities could be the safekeeping of the private keys used to conduct transactions and/or access digital assets. In this context, there would be a private key which is used by the custody provider to operate the wallet and another private key to manage the digital assets contained therein. Custody providers may choose to use the keys of their own wallets and provide similar services by conducting transactions and controlling the use and transfer of those assets. Furthermore, access methods and points can change over time: clients might connect directly to P2P systems, and the content of the custody function might evolve from custody of assets to custody of data and information. Custody in a DLT network will need to ensure asset protection, handling of positions and accurate records in the event of continuity issues, cyberattacks, system disruptions and bankruptcy or insolvency. It should also facilitate consensus on transactions. For this purpose, network participants would have to agree on standard protocols and rules to control input into and access to the information so as to avoid instructions by non-authorised parties, asset information leakage and misuse.

1.2.3 Operation of DLT network operator

The function of DLT network operator should ensure the smooth operation of the network and its components through standardised rules. For example, the network

operator would be needed in the event of system failure, especially to ensure that the latest positions were correct.

1.3 Interoperability of DLT-based solutions

In general, standardisation and common rules on a broader set of features and technical aspects are needed for the different systems to interact smoothly with each other. Currently, one key obstacle to the broader adoption of DLT-based solutions is the lack of standards, which prevents fragmented systems from achieving scalability and, in turn, efficiency gains and positive network effects. Specialised technology firms have developed tailored DLT-based solutions, although these can vary significantly in terms of scope, connection speed, scalability and fault tolerance.[19]

The uptake of DLT-based solutions will therefore be influenced by whether it is possible for them to interact with each other and with the existing environment. The current lack of interoperability across DLT-based solutions developed in the post-trade area may give rise to market fragmentation and represent a challenge for harmonisation goals. Therefore, interoperability represents a feature of DLT that deserves careful analysis and further efforts when considering implementation in this industry. This report and the models described in the report cover two dimensions of interoperability: one relates to the level of interaction of DLT networks with conventional systems, while the other refers to interactions between different DLT networks.

1.3.1 Types of interoperability

1.3.1.1 Interoperability between conventional and DLT systems (integration)

The challenge of integrating newly established DLT-based solutions with existing systems persists, but new solutions appear to be gaining traction. Regardless of the technology, integrating existing architecture seems necessary to ensure a smooth transition and prevent the creation of separate technology stacks, including in the case of a planned phase-out of the system.

In this exploratory phase, a major challenge for a DLT-based solution is to accommodate manual processes. If some aspects of processing cannot be automated or programmed into code, the system may not be able to entirely capture the update in its distributed ledger. In addition, data sources should be interacted with secure mechanisms such as oracles, which act as an interface between on-chain and off-chain inputs and where all interactions are digitally signed to provide a basic level of accountability. Further challenges for the integration of DLT with conventional systems are the costs involved and the limited pool of qualified human capital

[19] See the report by the European Blockchain Observatory and Forum entitled "Scalability, interoperability and sustainability of blockchains".

available to lead DLT-based projects. Inherently limited data sources may also be an issue, as a distributed ledger can only access stored data available on the chain. In this regard, solutions exist that make it possible to access off-chain data.[20] In addition, it remains important to enhance efficiency by rationalising duplicated infrastructures and reducing costly reconciliation processes (for example by having a single data version instead of duplicated data).

Interoperability between DLT networks and existing infrastructures can be achieved for instance through smart contracts for the on-chain transfer of financial data and can underpin automated workflows (if X happens off-chain, then Y occurs on-chain). It can also be achieved via application programming interfaces (APIs). For interoperability to work efficiently, networks can also operate on the basis of commonly accepted data definitions, transaction formats and processing logic. New technological features can ensure integrity as regards double-spending, authorisation and digital identity. The deployment of such features should be designed in such as way as to avoid additional costs, increases in latency and inefficiencies.

1.3.1.2 Interoperability between different DLT-based systems

A first challenge lies in the diversity of DLT networks, many of which have been developed in isolation for specific use cases. Key differences include (i) data records (on-chain or off-chain), (ii) data structure and transaction protocols, (iii) consensus algorithms and data distribution and (iv) distributed applications (i.e. smart contracts).

In terms of interoperability, DLT networks can adopt one of the two different models below.

- A trusted third-party model, where network members choose a third party to validate transactions or information (usually off-chain).
- A direct link model, leveraging on technical arrangements (e.g. smart contracts or atomic swaps) to ensure interoperability directly on-chain and between-chain. This model requires more complex arrangements and significantly higher development effort than a trusted third-party model.

From an operational perspective, the two main models are as follows.

- Trusted bridging, which takes places with the involvement of an intermediating third party fulfilling the role of a bridge. This requires participants to trust the intermediary during the entire process.
- Trustless bridging, where there is no need for any third-party involvement for the successful use of the solution. This requires more complex arrangements and significantly higher development effort than trusted bridging.

As industry participants are presently building their own DLT-based systems, there is a risk of incompatibility between the different systems, potentially leading to

[20] See Annex I for examples.

fragmentation. Standardised rules are needed and can be ensured by adopting one of the following:

- pre-determined standards and common rules (e.g. for messaging) for smooth interactions (e.g. in the context of a consortium for specific use cases where new entrants with DLT-based business and incumbents have to cooperate as participants);
- interfaces (including those from third-party providers) that can be provided for example when one participant has developed only one of the two systems and must nevertheless interact with other participants that base their business on both systems.

1.3.2 Evaluation of interoperability solutions

Interoperability has several meanings, so different criteria and dimensions can be used to categorise solutions and their impact. For example, the choice of the specific features of a solution could bring consequences in terms of ease of use and compatibility with other systems. In addition, the costs related to the functioning of the solutions and to collaboration among parties could be affected by the specific consensus mechanism used and by its development in terms of scalability and future design choices.

2 Issuance or recording and post-trade handling of securities in a DLT environment – identified practices and key implications

On the basis of market initiatives and practices[21], the report identifies two main models for enabling the issuance or recording and post-trade handling of securities in a DLT environment and providing interoperability with conventional systems:

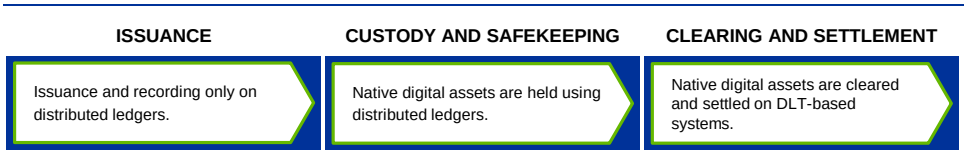
- Model 1 – securities issued as native digital assets; and
- Model 2 – securities issued traditionally and made available on a distributed ledger by either migrating, linking or tokenising them via DLT (Models 2a-2c).

Model 1 – securities issued as native digital assets

Under this scenario, securities do not have any other representation outside the DLT network (and are therefore framed in green in the chart below): the ledger where the native digital assets are recorded constitutes by itself the relevant – and only – bookkeeping system.

Figure 1

Model 1 – securities issued as native digital assets



From a purely operational perspective, the native digital assets could be publicly traded on conventional execution venues and comply with existing regulations. Model 1 has so far been used mainly for the purpose of bespoke over-the-counter (OTC) transactions or private placements.

The implementation of this model is reliant on the applicable regulatory framework enabling issuance of securities through DLT. Illustrative examples taken from different market initiatives are included in Annex 1.

[21] A summary of these initiatives is provided in the annexes to this report; it is based on information publicly available or collected by Fintech-TF members.

Model 2 – securities issued in the conventional system and enabled in a DLT environment

Under this scenario, securities are initially issued within the traditional system, while the recording and post-trade handling of the securities is subsequently enabled in a DLT environment. Many examples of this model already exist. Some of these initiatives are led by incumbent players or consortia. Others originate from new entrants (e.g. start-ups) that might not be regulated at present.

The use cases identified can be broken down into the following three different solutions for enabling the recording and post-trade handling of securities on a distributed ledger under Model 2:

- Model 2a – securities recorded in a conventional system and fully migrated to a DLT-based one (without the issuance of a token);
- Model 2b – bridging conventional and DLT systems to issue and record tradable securities;
- Model 2c – securities recorded in the conventional system but referenced by a token in DLT environment.

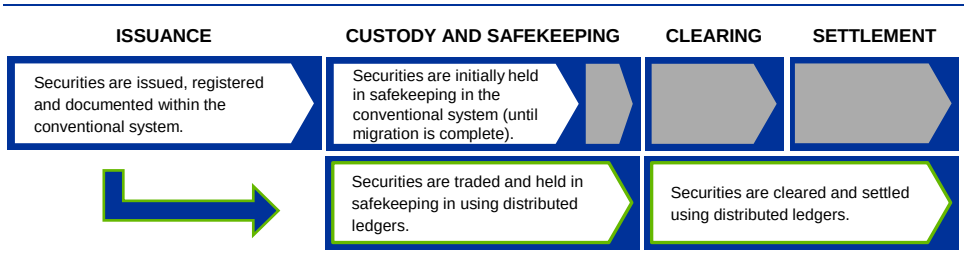
Model 2a (one way) – securities recorded in a conventional system and migrated to a DLT-based solution

This scenario combines both elements of existing systems and opportunities provided by DLT. Securities are initially issued and recorded in a conventional system (which then remains responsible for processing the relevant events of the securities life cycle) while custody activities and settlement (including corporate actions) are arranged with the use of DLT.

In this model, interoperability is needed between the notary ledger handled on the conventional system and the custody ledger, as the distributed ledger would capture transaction flows and related information that might require an update of the conventional ledger. Once the migration period is complete, the asset is available only on the distributed ledger, where it can be traded according to the nature of the asset and the jurisdiction in which the system operates. An illustration of how this model operates is provided in the chart below.

Figure 2

Model 2a (one way) – securities recorded in a conventional system and migrated to a DLT-based solution



Model 2b (two ways) – bridging conventional and DLT-based systems to issue and record digital financial assets

This model assumes that assets are made available either in a conventional or a DLT-based system. Securities are issued and recorded using the incumbent system, while custody and settlement are performed on both the centralised and the distributed ledger. As a result, a parallel system is provided in order to settle trades in the securities both in the incumbent system and in the DLT-based system. It is also possible that one of the two systems might be used to perform the main phases of the securities life cycle. For example, issuance, custody, clearing and settlement might take place in the incumbent system while specific parts of the process are performed in the other.

Figure 3

Model 2b (two ways) – bridging conventional and DLT-based systems to issue and record digital financial assets

For this to happen, tools for ensuring synchronisation between the two systems are needed. Additional complexities can be expected to arise from the coexistence and simultaneous availability of securities in the traditional system and the DLT-based system. In order to prevent any arbitrage opportunities and ensure fungibility between securities recorded conventionally and on-ledger, the two systems should be able to ensure continuous, efficient and rapid synchronisation (reconciliation) for the update and record-keeping of assets, while ensuring the confirmation of ownership at any point in time.

Model 2c – securities recorded in a conventional environment and referenced by tokens in a DLT environment

Under this model, securities are initially issued and recorded in a conventional system. The securities are subsequently tokenised, creating their representation on a distributed ledger. Tokens can be used in DLT-based solutions to enable the transfer of the value and (all or part of the) rights that are embedded in the security that the token represents. To date, Model 2c appears to have been used mainly for back office operations, collateral transfer or lending facilities.

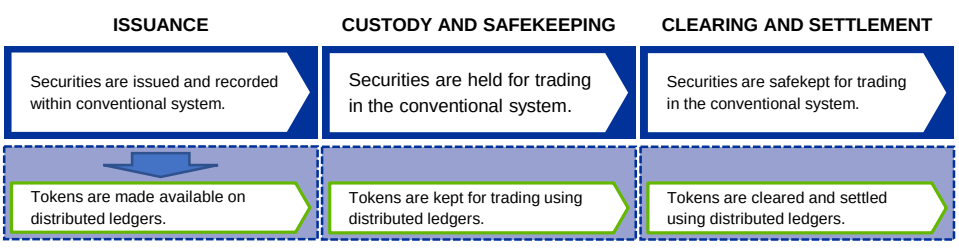
For the purposes of this report, a distinction can be drawn between three different types of token: (i) tokens that refer to assets in a 1:1 relationship (i.e. one token to one underlying security), the aim being for them to represent the securities themselves on the distributed ledger; (ii) tokens that refer to securities in a 1:n relationship (i.e. a token represents a legal claim to a basket of securities); and (iii) tokens that represent fractions of rights embedded in the asset they represent (1:1/n).

It should be noted that tokens would not be considered securities themselves. In addition, the system for issuing tokens, together with record-keeping and other related activities, can technically be run by an entity that is different from the issuers of the underlying securities.

In this context, the transfer of a token may be – but does not have to be – reflected in the conventional ledger. Consideration should be given to risks stemming from exchanging tokens rather than the assets they represent. Appropriate operational safeguards preventing the parallel use of the securities behind the tokens and the tokens themselves should be ensured in order to prevent double-spending, integrity issues and abuses. Such practices could have an impact on market liquidity and the overall stability of the financial ecosystem. They could also create a risk of regulatory arbitrage (as the tokens could be exchanged without the protections attached to the underlying securities). In addition, the question arises as to what will be transferred via the token (e.g. only a record of the assets belonging to an asset available in a DLT environment, rights of underlying securities, etc.).

Figure 4

Model 2c – securities recorded in a conventional environment and referenced by tokens in a DLT environment



3 Key features of using DLT for issuance, custody and settlement

3.1 Issuance, recording and redemption of securities in a DLT environment

This section outlines the possible added value of issuance via distributed ledger and clarifies how certain functions (e.g. accountability, legal validity) are performed in legacy systems and systems relying on DLT. These findings, together with a legal analysis of key aspects, will enable key implications and requirements to be identified.

3.1.1 Description of business and operational processes

Issuance in existing systems is currently governed by the national laws of the country where the related assets are issued.

With respect to the two models presented above, Model 2 assumes that the issuance of a security is performed in the conventional system, while the other post-trade processes can be harmonised and handled in DLT-based systems by making the securities directly available on distributed ledgers (Model 2a and Model 2b) and via referencing tokens (Model 2c). The details are as follows.

- In Model 2a, securities are issued in conventional systems, but post-processing is then performed within a DLT environment after a full migration from the legacy system.
- In Model 2b, the operations subsequent to issuance are performed either in the DLT environment or in the legacy systems. In this regard, there are two distinct types of “hybrid” treatment, which are as follows.
    - A certain, defined fraction of conventional securities is handled on distributed ledgers, while another certain, defined fraction of conventional securities is handled in conventional systems (i.e. the fractions are not mixed).
    - A “functional” split is performed: some of the post-processing is administered on distributed ledgers, while some is administered in the conventional systems.
- In Model 2c the initial issuance is performed in legacy systems, but the assets are then partially or fully tokenised in order to ensure the transferability of the embedded rights in DLT systems and for operational purposes.

When referring to native digital assets which are issued directly on distributed ledgers (see Model 1), the issuance processes could benefit from the distinctive features of

DLT, as it requires streamlined and uniform documentation such as the operating manual of the system (all elements are digitised immutably within DLT network). This is in contrast to conventional processes, which may involve different intermediaries. In addition, DLT can make the issuance process more transparent, depending on the information that is actually available to stakeholders on the network.

Initial experiments[22] with DLT and smart contracts have revealed few issues related to asset creation and distribution: in Model 2a and Model 2b, DLT running in parallel with a conventional system (on either a temporary or default basis) may give rise to new, different issues relating to interoperability and record-keeping.

3.1.2 Regulatory and governance implications

The successful execution of securities issuance, recording and redemption on DLT will depend on the presence of an entity that ensures interconnection between the off-chain world and the system. If this entity is not regulated, market participants may not have the necessary confidence to engage with DLT-based solution providers. As already highlighted in previous work carried out by the AMI-SeCo[23], proper governance of any market infrastructure is important to ensure its safety and efficiency, including in a DLT environment. In this regard, the question of how DLT solutions should be governed may need to be considered. This concerns platform governance and application governance. It also concerns governance of the intellectual property rights associated with (i) the design of the solution used to provide a service via a platform and (ii) the data recorded/shared through the platform. In any case, any arrangement should aim to enhance the integrity and resilience of information recorded.

As regards the representation of assets in a DLT network, the following considerations should be taken into account.

As in the case of Model 1, challenges may arise owing to different regulations in Member States regarding the possibility of purely native digital assets.

The impact might be mitigated when running the on-chain and off-chain procedures in parallel[24] (as in the case of Model 2b), as the conventional system will be maintained and coexist in parallel with the DLT-based one.

In the case of Model 2c, the process of tokenisation and the relationship between securities in the conventional environment and their representations in DLT environment currently lack clarity from a regulatory perspective. For example, the concept of “issuance of tokens” should be treated with caution and not be confused with the issuance of securities, as the process of issuing tokens merely representing securities is a technical matter which may not be relevant to parties who are not directly involved in operating the system. Tokens in Model 2c are not considered as

[22] See the examples in Annex 1.

[23] See footnote 3.

[24] Local law often requires securities to be issued in paper form.

”transferable securities”, are not regulated by the competent authority according to existing regulatory frameworks and cannot be transferred on regulated exchanges. However, the transfer of tokens can be conducted on non-regulated platforms with the risk of fragmentation and regulatory arbitrage in post-trading processes. Regarding transfers outside the conventional platforms, receipts from third-party wallets may require prior approval by the issuer depending on the way tokens are set up[25]. Tokens may allow for simple fractionalisation of equities via tokens and near real-time settlement. The token owner effectively holds a claim for receipt of the underlying security towards the token issuer[26] (thus generating issuer and settlement risk). In any case, if an underlying security separated from the tokens exists, the act of “tokenising” cannot in itself create a security.

3.1.3 Technical and business perspective

3.1.3.1 Connection to the platform/DLT system

The issuer (or the issuer’s agent) would connect directly to the DLT system via its digital asset custody wallet for the issuance of security tokens and the processing of payments throughout the life cycle of the security. From an operational perspective, some processes (e.g. order allocation and token creation) would be triggered by the arranger on behalf of the issuer, while others would be conducted automatically by the platform (e.g. coupon payouts).

In Model 2b, legacy and DLT systems need common connection and communication standards. APIs could be used to establish an interface between the two systems.

In Model 2c, some means of tracking and ensuring comparability between tokens and underlying securities should be considered in order to avoid any intentional or unintentional misuse of rights related to security or securities represented by the token available on a distributed ledger. In addition, in the event of insolvency, different records could result in legal disputes among counterparties and clients.

3.1.3.2 Network architecture in a DLT environment

As highlighted above, securities can be issued on a DLT network and introduced to the conventional world after the issuance process (as in Model 1). At the same time, the logical sequence in the evolution of securities towards DLT-based solutions may be for securities issuance to be digitised first of all and for the full post-processing to be performed using distributed ledgers (as in Model 2a) only at a later stage, when the technology is more developed. However, a lack of clarity over the post-processing setup (e.g. regarding local security laws and collateral eligibility rules) is forcing

[25] For example, the issuer and arranger currently determine together whether a secondary market investor will need to be approved or if the security tokens can be freely transferred.

[26] This might be different in specific cases, depending on the overall legal set-up and documentation.

innovative companies to re-enter the conventional world and to run DLT-based solutions in parallel with conventional systems (as in Model 2b).

The high-level architecture can constrain the highly abstract hierarchical architecture of distributed ledgers[27], as nodes in a DLT network operate with typical distributed system solutions (including cloud solutions), which require key components such as (i) safe hardware, (ii) extendable protocol communication, (iii) network management (including management of the P2P network), (iv) a consensus mechanism and (v) a smart contract mechanism.

3.2 Custody and safekeeping in a DLT environment

This section outlines the custody and safekeeping arrangements in the different models presented and compares these arrangements with those in conventional systems. It then discusses aspects related to account structure and asset servicing and their functioning in DLT. Lastly, it describes the key implications of the custody and safekeeping of securities in DLT-based systems for market stakeholders and financial market infrastructures (FMIs).

3.2.1 Description of business and operational processes

As described earlier in this report, some of the models identified which make use of DLT also rely on existing systems. In Model 2, the initial issuance of assets takes place in the incumbent system. Only after issuance are the assets either:

- fully migrated to the DLT-based system, terminating custody and safekeeping in the conventional system as happens in Model 2a;
- kept in both systems in parallel, with custody and safekeeping made available in traditional or digital form, depending on the requirements of a particular transaction or specific arrangements for safekeeping and custody, as provided for in Model 2b; or
- tokenised and later managed through a referencing token on a DLT network, with the actual asset being kept in custody in the conventional system at the same time (as in Model 2c).

Regardless of the specific technology, compliance with current regulatory frameworks remains essential for the development and wide adoption of new solutions, and this should also be the case when using DLT. In addition, DLT-based solutions could require the existence or development of different rules, infrastructures and specific record-keeping techniques depending on protocols and the validation process. In this regard, the identification and definition of the structure and overall governance of ledgers should be ensured throughout the post-trade processes.

[27] As highlighted in the International Telecommunications Union technical specification on distributed ledger technology reference architecture.

In addition, the specific design of particular DLT protocols could raise concerns regarding the use of these technologies in a P2P context, both in terms of compliance, for instance with current AML/CFT rules, and in terms of security.

Another aspect worth highlighting is the concept of asset control for the purpose of custody and safekeeping in a DLT environment, which might be handled and interpreted differently by market players and legislators. This might create a risk of fragmentation and reduce the potential efficiency gains and expected benefits (yet to be demonstrated) resulting from the use of DLT. At national level, there are currently some legislative initiatives that aim to provide clarity on custody when using DLT.

It remains to be discussed how exactly the custody and safekeeping processes would be shaped and organised in a DLT environment. The use of wallets and private keys may imply more difficulties in keeping track of a security's movements and additional risks, as the distributed ledger would be the only source of information. At the same time, the potential benefits (i.e. a wider overview of information and movements among nodes) could be a main driver for the adoption of these technologies. In Model 2b, the possibility of checking for changes in clients' accounts and rights on their behalf could be more complex, as continuous communication between the two systems must be ensured. In Model 2c, tokens merely represent securities which remain in a conventional environment. However, tokens may represent some of the rights that are relevant in the asset servicing, and some form of synchronisation may be required between the two systems.

3.2.2 Regulatory and governance implications

One question to address is to what extent the use of DLT could change the process of custody and safekeeping, particularly with regard to the governance of the system's automated components (e.g. smart contracts).

Key considerations that arise for the automation of services and that have systemic ramifications are the risks of errors, the controls needed to avoid something going wrong and the question of who is accountable for the related (financial and non-financial) losses.

Different forms of governance and consensus protocols provide different specific safeguards against the manipulation of DLT networks, for instance by means of double-spending. In this regard, it remains to be determined which aspects should be subject to regulation and whether the architecture of the network (e.g. restricted versus unrestricted) may change the existing, well-established rules to be applied to it for custody and safekeeping. DLT-based consensus algorithms may have the potential to improve the way in which the current post-trade processes are conducted, but that too can bring threats and negatively affect processes and machines. In any case, the need for an appropriate governance framework goes beyond any specific network or key features, especially taking into consideration the innovations relating to the custody and safekeeping of tokens, cryptography-based tools and "trustless" trust (ensured via IT processes).

Custody of digital assets through DLT requires sufficient safeguards of assets to protect them from misuse and/or malicious activities. In order to mitigate network-specific risks, one option could be to require a licence that is tailored to the specific business and risk profile of the "digital custody activity".

In addition, there are currently several approaches to the safekeeping of private keys that allow assets to be moved in the DLT environment. A wallet holds a private key that authorises the holder of that key to transfer tokens on a DLT network. While tokens may be accessed and controlled via private keys, they are electronically recorded on the network and not in the wallet itself. Therefore, a question worth highlighting is whether having control of private keys on behalf of clients (which may be the preferred option of the client) should be regarded as a safekeeping service and, if so, how rules to ensure the safekeeping and segregation of client assets should apply to the providers of this service. From a technology perspective, this would mean that a custodian of a digital asset does not hold a client's private keys to the digital assets but holds in safekeeping its own private key that operates the client's digital assets.

Differentiating between key storage and safekeeping of the "booked" assets remains important, especially in case of Model 2c, where the key refers to a token rather than a security.

3.2.3 Technical and business perspective

Custody of assets stored on a distributed ledger would be different from custody of securities in the current setting, as the technical design of a DLT storing a security or token in a distributed network may require different steps compared with storing dematerialised assets in a centralised database.

Custody chains are theoretically an option but are hardly compatible with the concept of a DLT-based or other P2P system. This does not mean, however, that ownership of digital assets cannot be intermediated: a key difference compared with traditional custody chains would be that the intermediation at the technical level would usually take place outside the DLT network.

Securities accounts used for settlement and safekeeping need to be enabled to hold all types of assets, including those natively issued in a DLT-based system. The same set of data needs to be available for securities in both traditional and digital form. In this context, reconciliation procedures are in place with the aim of addressing the risks that ledgers organised in a hierarchy (e.g. custody chain) may imply. In a DLT context, the effectiveness of these procedures should be assessed according to the architecture of the specific DLT network. In theory, reconciliation in a DLT set-up would not be necessary as long as relevant data and information are simultaneously displayed and accessible on the ledger itself and then reported to the client. However, one question is whether this would be performed by any internal reconciliation, e.g. due to distributed nature of the ledger. A further reconciliation procedure might be needed to support interoperability arrangements.

In addition, the risk of losing private keys depends on how their custody is performed, as well as the role of custodian and the (co)existence of a conventional environment. The specific case could have a highly adverse impact and must be managed through appropriate models and procedures. There are also concerns regarding a definition of digital assets for custody purposes, which could be limited to the backup of private keys or end-to-end protection of private keys and assets themselves. This can take place through the transfer of assets to the digital wallet address of the custodian, along with the ability of the custodian to directly access, hold in safekeeping and transfer assets via different types of wallets[28].

3.2.3.1 The identification of assets and tokens in a DLT-based system

Unique identifiers for commodities, securities or other assets have long been used in international markets. Typically, assets are represented as book-entry records, tracked via certain identifiers (e.g. International Securities Identification Number, ISIN) harmonising core processing across related asset types. At the same time, currencies are identified through International Organization for Standardization (ISO) currency codes (e.g. EUR for euro), which are internationally recognised. While the current approach clearly supports scalability, this may come at the cost of limiting customised assets that would require a special logic in the approach to identification. This may limit processing by effectively ignoring any idiosyncratic features and conditions. In this regard, it is worth discussing how the market can ensure scalability while catering for innovation.

As for tokens, a key question is whether there is a need for specific identifier. This code could not only capture details of the token, such as the current holding of participants, but could also define the token's logic and the transfer of tokens from one participant to another. The characteristics of a digital asset recorded on a distributed ledger may be different from those of traditional assets within existing market infrastructures, where securities are administered by central agents that record current holdings and transfers in their proprietary systems.

The implications of such a difference for appropriate identification may mean that it is crucial to unambiguously locate the respective token address with respect to (i) the distributed ledger it is deployed on and (ii) the implementation mechanism and address used for deployment.

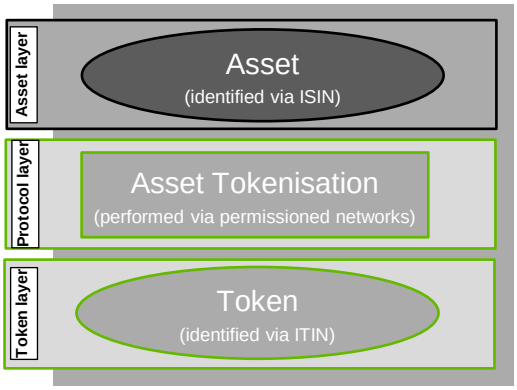
The difference can be best illustrated by the chart below, which shows for instance that while the asset layer is identified by a traditional identifier (e.g. ISIN, Financial Instrument Global Identifier, FIGI), digital asset identifiers such as the International Token Identification Number (ITIN) provided by the International Token Standardization Association (ITSA)[29] are used for the token layer. Consequently, assets being "tokenised" on different ledgers (or even by functionally distinct token contracts on the same ledger) may result in distinct stock tokens that will each receive a different ITIN while still referencing the same stock ISIN.

---

[28] See glossary.

[29] For more information, see the ISTA website.

Figure 5
Asset tokenisation process



3.2.3.2 Connectivity and standards in a DLT environment

In order to ensure clarity, a distinction should first be made between connectivity and standardisation of messaging. Connectivity ("the pipes") can currently be ensured via SWIFT, FIX, API, MQ or bespoke links. At the same time, messaging (the syntax and "content") should be standardised to allow straight-through processing (STP) in the systems of participants and their clients. Regardless of the connectivity mode, the messaging/reporting should adhere to existing or widely used standards. With the final aim of further contributing to the wide and efficient use of DLT networks for custody and safekeeping purposes, (new) common rules and standards should be developed and/or applied rather than have each system develop its own bespoke messages, which would increase fragmentation and reduce the benefits of the solution. In the current ecosystem, with initiatives making use of different protocols and technologies, common rules still seem to be indispensable. However, at some point in the future, new ways of interacting and performing transactions in a fully decentralised ecosystem will make it necessary to establish new standards or redefine the concept of standardisation.

Different network purposes and project scopes may require different connectivity solutions. DLT adoption in FMIs so far seems to have developed into three use cases that involve: (i) standardising data and account structures, (ii) mutualising multi-party workflows on distributed ledgers and (iii) building applications on top of rich data sets that will eventually underpin FMIs.

Migration to and adoption of standards is determined by different factors including harmonisation processes (e.g. ISO 15022 to ISO 20022) that involve many stakeholders, are undertaken in waves and take time to become widespread. Costs and other priorities are also a consideration as regards timing. Nevertheless, standard modes of connectivity are needed in FMI initiatives and will remain in place, principally to ensure that isolated pockets are not created, as well as to avoid the need for users to redesign/redevelop their own mid-office/back office platforms and/or to have separate workflows for legacy and DLT-based systems. Currently, different types of

connectivity already exist in the market: they are aimed at ensuring standardisation of processes, actions and events, such as in the TARGET2-Securities (T2S) environment. FMIs/projects adopting DLT are offering API-based connectivity as an alternative rather than as the only option. However, the content of the messaging needs to be standardised: for example, market-wide initiatives and programming languages will need to be aligned with market messaging standards (e.g. ISO 15022, ISO 20022).

In addition, FMI operators wishing to use DLT to synchronise multi-party workflows in order to achieve efficiencies in post-trade services will have to provide multiple connectivity methods to ensure no participants are excluded from the new infrastructure.

The deployment of new/expanded standards could be a way to prevent the development of bespoke messaging and thus ensure the efficient use of a DLT network. Some initiatives have been developed by market participants to this end. Specifically, in terms of communicating into and out of matching, asset servicing, mid-office and other necessary systems, clients (or their service providers) may want to connect directly to such systems so that all parties can see or match results at the same time without having to go through chains of intermediary messaging flows. This needs to be taken into account when designing a system. In some projects being carried out in the market, FMI operators are offering web portals or API-based connectivity and traditional connectivity models. Other projects have been developed within narrower contexts, as asset tokenisation allows P2P market places made up of a closed loop of players: messaging standards may be driven by the needs and requirements of members participating in the project to support connectivity options that work for all stakeholders.

3.2.3.3 Potential changes in asset servicing (including corporate actions)

In asset servicing, the mechanism for performing key processing services may require additional consideration when making use of DLT. For example, DLT can deliver concurrent communication of real-time information to multiple parties so that they can be aware of requests at an earlier stage and prepare for them. The aim here is to remove the time pressure currently created by having sequential steps between parties. The immutability of information provided via DLT and ensured via cryptographic tools could, technically, bring benefits in terms of asset protection, certainty and transparency in the market, together with cost savings. In addition, asset servicing instructions in securities lending could benefit from smart contract-driven execution, although the complexity of the code may mean that additional steps are required before execution.

New technologies (including DLT) can ensure greater automation of contracts, for example in the area of corporate action announcements[30]. In this regard, information extraction and machine learning techniques could improve efficiency and streamline

[30] On this topic, see the Ami-SeCo report entitled "Follow-up analysis for the HSG Task Force on Distributed Technologies (DLT-TF) on Issuer Corporate Actions Golden Copy".

processes. A key issue in this field is the ability to ensure that there is a trusted copy (ideally a golden copy) that can be used as the single source of legally binding information on corporate actions. In a distributed environment, more effort may be required to validate the process and clearly identify roles and functions, especially in unrestricted networks. Based on the role of participants, smart contract information could also be enriched, increasing the value of the trusted copy. Reference data on corporate actions in the form of records in the DLT environment would initially be created at securities set-up for predictable events documented in the prospectus of the issue, while additional corporate actions throughout the life cycle of a security would constitute updates to this original record. However, it remains to be clarified how unpredictable events can be flagged and monitored in a decentralised environment, and what protocols and standards to adopt in order to ensure the integrity and consistency of the information and the efficiency of data flows among network participants and external parties.

3.3 Settlement in a DLT environment

3.3.1 Description of related business and operational processes

In Model 1, settlement processes are performed within a DLT-based solution. As these native digital assets would be securities, the same rules as those in place for the conventional environment should apply. This model is used in particular in the case of private placement issuance. The use of private and closed systems may facilitate the transfer of securities among parties in a way that is closer to an update of the ledger.

In Model 2a, settlement is performed in the conventional system until the migration to the DLT-based system is complete.

In Model 2b, settlement happens either within a conventional system or a DLT-based system and may require reconciliation procedures supporting interoperability.

Model 2c would allow tokens to be transferred in a DLT-based solution which, in any event, would need to ensure that the information is verified and the embedded rights can be enforced by the entity that receives the token from an entity that was entitled to transfer those rights. In this context, settlement finality is linked to the concept of immutability of the transfer of rights. In addition, the synchronisation of the conventional system (in which the underlying assets are traded) with the DLT-based system (in which tokens partially or fully represent the underlying assets) is needed to perform settlement while ensuring integrity of the assets and enforceability of the transfers among parties (including external parties).

3.3.2 Regulatory and governance implications

In traditional systems, settlement finality is a well-defined point in time[31] and has an unambiguous legal basis. The Settlement Finality Directive (SFD)[32] guarantees that transfer orders which are entered into designated systems are irrevocable and final, regardless of whether the sending participant becomes solvent or not after the defined moment of finality of the transfer order. For DLT arrangements, the moment of technical irrevocability of transactions is linked to the features described below.

DLT-based arrangements rely on consensus mechanisms to ensure the technical irrevocability of a settlement transfer. However, the specific protocol used by the networks may imply different and/or additional steps and processes to be agreed by its operators and/or its participants for the purpose of achieving finality at a point in time that is agreed by the network and enforceable to third parties.

In addition, DLT-based solutions can be used for synchronising the value date and trading date according to the consensus mechanism. DLT may thus reduce the hurdles of complex reconciliation thanks to its distributed data structures. The execution of a trade in a DLT environment would immediately trigger the related transfer directly between the accounts of the two contracting parties (i.e. between the digital wallets containing keys to the holdings of cash and securities of each participant). In this context, the value of a golden record can be twofold. First, it can ensure certainty, as synchronisation between systems will be performed almost in real time. Second, it can reduce the risk of arbitrage between two systems (i.e. the traditional and DLT-based systems) that need to interface with one another for clearing and settlement purposes, as it provides an agreed and unique set of information that both systems "trust".

3.3.3 Technical and business perspective

3.3.3.1 Digital assets: delivery versus payment in DLT environment

In a DLT environment, securities could be settled on a delivery versus payment (DvP) basis, and reconciliation efforts could be efficiently conducted, with operational transaction finality achieved within seconds. The European Central Bank (ECB) and Bank of Japan (BoJ) carried out joint research[33] in which they considered the possibility of DvP being conceptually and technically designed in a DLT environment with cash and securities on the same ledger (single-ledger DvP) or on separate ledgers (cross-ledger DvP). However, the specific design of DvP depends on the characteristics of the DLT platforms (e.g. the range of information shared among

---

31 Settlement finality is the legally defined moment at which the transfer of an asset or financial instrument, or the discharge of an obligation, is irrevocable and unconditional and not susceptible to being unwound following the bankruptcy or insolvency of a participant.

32 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 (OJ L 166, 11.6.1998, p. 45).

33 See the joint ECB and BoJ report entitled "Securities settlement systems: delivery-versus-payment in a distributed ledger environment".

participants, data structure and locking of delivered assets). In addition, depending on the use case, DvP design can be influenced by a number of factors, including the interaction of the DvP arrangement with other post-trade infrastructures.

The expected gains from tokenising securities and creating “cash on ledger” to settle transactions, compared with settling transactions on existing systems, along with the rationale and business case for such an investment, are still to be explored.

Real-time processing of assets with liquidity saving mechanisms could be possible, as there would no longer be a need to close incoming/outgoing feeds for maintenance or to adhere strictly to batch times. At the same time, the network could still enjoy the benefits of netted settlement, if required. Although network parties ultimately need to agree to certain settlement procedures if netted settlement is desired (e.g. settlement times and windows), it still allows for greater flexibility.

In this context, a clear distinction should always be drawn between commercial bank money and central bank money. Several providers claim they offer the service of “putting cash on ledger”, i.e. by offering a form of token in a network (mainly DLT-based) in order to ensure, in the same system, a form of delivery of assets for another transfer of value (i.e. payment or delivery of asset). However, in order to have a claim on the central bank on the ledger, additional features are needed, which mainly depend on the specific design chosen, the regulatory framework of the issuer central bank and the impact on the financial ecosystem. In any case, a claim on a private institution will not be central bank money or “cash” in digital form.

3.3.3.2 Immediate settlement: implications for value chains and market structure

DLT-based systems could be adopted with the aim of standardising and streamlining processes, leading to cost savings (by reducing unnecessary duplication of activities, e.g. for reconciliation) and better risk management. As new solutions may emerge in response to evolving market needs, an important consideration for investors, banks and FMI operators that may want to adopt DLT is how significant the expected cost improvements are compared with the investments required. Another question is whether these advantages can be achieved within the current ecosystem or through other means. In addition, when looking at benefits such as immediate settlement, one could ask why, if cash and assets can be made available upfront for a DLT-based solution to enable immediate or same day settlement, the same cannot also be achieved in the existing ecosystem (as this is technically feasible, although is not market practice). Another question to be considered is whether cost benefits relating to more automated asset servicing via smart contracts could translate into lower fees for the end investors or greater transparency towards issuers.

It is worth highlighting that real-time settlement, which is also performed in the most up-to-date legacy systems, would only reduce and not eliminate credit risk, e.g. the risk that the counterparty does not have the requisite cash or securities (as only pre-funded transactions eliminate this risk).

3.3.3.3 Funding and market liquidity issues arising from asset clearing and settlement on a DLT network

The specific arrangements needed when using DLT, as compared with existing arrangements, may have implications for funding and market liquidity, either at the level of the single entity or for the whole financial ecosystem. For example, the risk that DLT-based solutions might create a closed-loop network may have an impact on overall liquidity. This may result in liquidity management issues and fragmented liquidity pools, as well as having a negative impact on the overall adoption of DLT-based solutions. For example, in the case of privately issued securities not intended to be transferred through a settlement system under Model 1, it is to be assumed that a closed system will be used for these services. Liquidity risks may arise during the migration period in the case of Model 2a, with consequences that range from loss of efficiency to additional costs for the issuer and service providers. Model 2b involves the use of non-DLT and DLT-based systems in parallel and may entail a reduction in overall liquidity as the securities would be available in only one of the two systems and, as a consequence, would be blocked (or "frozen") in the other one. In Model 2c, the use of an additional layer "on top", bridging the two DLT-based systems with the use of a token for settlement, would not need to be subject to the same regulations as those applicable to securities and could meanwhile drain the liquidity that is available in the market, resulting in efficiency losses and market fragmentation.

Conclusions

In the current landscape, a clear business case has not yet emerged for the use of DLT in post-trade processes. The solutions that exist at present are mainly real-life experiments and internal prototypes. There are also many other ongoing DLT-based initiatives to improve the financial landscape that could coexist with current processes or even enhance them.

This situation might evolve rapidly in the future considering the changes in the regulatory framework and rapid technological innovation. In this context, it is essential to ensure the safe and efficient coexistence of different types of architecture and networks to support innovation while maintaining an integrated market for post-trade services and infrastructures.

Most current initiatives focus on the proprietary business rules and technical requirements (e.g. standards) of individual groups of market stakeholders. This could lead to a lack of interoperability between the different solutions and hinder the opportunities and benefits that developments and improvements are expected to provide.

Interoperability is necessary for the implementation of new financial market technologies that are characterised by interdependencies and network effects. To improve the use of such new technologies (both DLT and others) and to avoid further fragmentation, common protocols and standards are needed. Legacy and DLT-based systems need connection and communication standards that are robust in the face of technological innovation. This will help to avoid a situation where each system becomes a different ecosystem isolated from the others. It will also help to ensure a level playing field among market participants, irrespective of the underlying technology.

Interoperability should therefore be seen as a crucial feature when developing any post-trade solution based on DLT. It should also be a key consideration when addressing preliminary issues, such as the business design – and in some instances even the technical design – of a solution and how to link the entire chain of stakeholders and mechanisms, including end users and existing engines/tools that need to remain accessible.

In parallel, clear and sound governance of services and functions should also be ensured in a DLT environment. In this regard, a consolidated approach based on regulatory licences and conduct of business rules will create appropriate incentives to manage conflicts of interest. It will also ensure a sound basis for issuance, custody and settlement through the presence of licensed and trusted parties. This consolidated approach should additionally allow for platform governance and application governance. In addition, it should take into consideration governance of intellectual property rights associated with (i) the design of the DLT solution used to provide services or functions via a platform and (ii) the data recorded/shared through the platform.

Glossary of definitions

Consensus algorithm	Set of rules used in a DLT environment to find agreement on what the current status of the ledger is at a specific point in time.
Distributed ledger	A shared database where records can be updated by a set of participants, with no need for the central database management system used to validate such updates in traditional databases.
DLT network	A set of nodes that share the management of a common set of information, which is recorded in a distributed ledger.
Native digital asset (cf. Model 1)	A security that is originally issued, recorded and kept in a DLT-based system.
Node	Any machine (such as a computer) that is connected to the DLT network.
Oracle	A node of the DLT network that certifies to other nodes the occurrence of specific events outside the network (e.g. change in asset prices, weather conditions, etc.).
Participant	A legal entity or natural person that connects via a node to use a distributed ledger, and the technology behind it, to manage information.
Restricted network	A DLT network that can be accessed only by a specified set of participants, who can then be assigned different roles. See also unrestricted network.
Smart contracts	Algorithms coded to update records when a set of conditions are met.
(Asset) Tokenisation	The process of creating a token (of an asset); a token of this kind is merely a representation of an asset already available elsewhere.
Unrestricted network (also open network)	DLT network that has no restrictions on participation (see also restricted network). Any entity can become a participant without having to link its identity to its network address or public key in the network.
Validator	A participant that takes part in the consensus process in a DLT network to confirm the validity of an update and to synchronise the information held by its participants.
(Digital) Wallet	Software that stores private keys used to initiate transactions and provides additional customisable services, e.g. an overview of asset balance and transaction history.

Annex 1: Examples of models[34]

Issuance and settlement of shares as native digital assets on a private blockchain via the LiquidShare platform[35]

LiquidShare is a platform based on a private and restricted blockchain network for the issuance, holding and transfer of securities. The entirety of the issuance is registered onto LiquidShare's blockchain and accounted for via an issuance smart contract that keeps track of the total number of securities for each issuance. Settlement is arranged through an atomic DvP in the blockchain of securities versus tokens backed by commercial bank money and central bank money.

Issuance and safekeeping of bonds as native digital assets via the Bitbond platform[36]

Bitbond is a platform built on the Stellar protocol. It enables securities (bonds) to be issued on a distributed ledger.

The securities issued are distributed directly into investors' digital asset custody wallets. The securities remain in the issuer account at the custodian until investors have funded their account and the DvP is triggered.

The custody of the asset issued takes place via the Bitbond platform. Bitbond utilises key management software replacing private keys with multi-party computation. Investors can access and use their custody wallet via a web-based interface.

Issuance and safekeeping of bonds as native digital assets by Banco Santander

In September 2019, Banco Santander issued a bond as a native digital asset registered in the public Ethereum blockchain. Banco Santander bought and held the full quantity of the security until maturity, and there was no secondary market. Assets were issued as a set of fungible ERC-20 tokens. The bond could only be accessed by the owner using their private key, while parties other than the custodian could only interact with the asset on the blockchain via an application by authenticating themselves. Corporate actions, including the issuer call used to trigger the maturity of this security, were initiated by user authentication to the blockchain, i.e. by users entering their PIN to access their private key. Post-trade processes were managed on the chain by the smart contracts and the application.

---

[34] The set of examples provided is illustrative and not exhaustive. Please note that the use cases describe the views of the companies leading the initiatives and not those of the Fintech-TF.

[35] See the LiquidShare website.

[36] See the BitbondSTO website.

Issuance of debt securities as native digital assets by Dealfabrix[37]

Dealfabrix is a capital markets platform enabling the issuance of 'Schuldscheindarlehen' (debt securities) on a permissioned blockchain. The entire workflow in the issuance is conducted digitally, directly on the platform. The legal validity of the contracts concluded and of the securities or obligations issued on the platform is ensured through DLT specificities such as immutability and distributed information by means of integrated technology (e.g. electronic signature and two-factor authentication).

DLT-based system for safekeeping and settlement of native digital assets by SIX Digital Exchange (SDX)[38]

SDX is implementing a distributed securities settlement and custody system on DLT. The system operates on three main types of node:

- the notary node (operated and controlled by SDX), which controls finality and prevents double-spending of assets;
- the participant node, where new transactions can be initiated and business logic executed;
- the SDX node (operated by SDX), which initiates new transactions and executes special business logic available only to SDX.

SDX controls access to its ledgers (private DLT instance). It has full control over who can participate and who maintains a node in the SDX DLT-based infrastructure.

For the purpose of safekeeping of native digital assets, SDX uses hardware security models which store private keys. The central securities depository (CSD) application, built on top of SDX DLT-based infrastructure, is account-based.

SDX offers a market model that makes use of atomic trading and settlement. Settlement is conducted on a P2P basis between the nodes involved. For bilateral settlements, the participants instruct SDX to settle the respective transaction on the intended settlement date. The payment leg is organised with the use of private stablecoin that is fully funded through a dedicated SDX account in the Swiss real-time gross settlement (RTGS) system Swiss Interbank Clearing (SIC).

[37] See the Dealfabrix website.

[38] See the SDX website.

Blockchain as a data recording system for transactions by ID2S central securities depository[39]

ID2S is an EU central securities depository (CSD) providing issuers with a process for negotiable European commercial paper (NEU CP) issuance from initial set-up in its static data environment until final settlement in T2S. The CSD operates the ID2S securities settlement system (known as the Rooster Securities Settlement System, or RSSS) via a permissioned blockchain dedicated to transactions in NEU CP issued within ID2S. The use of blockchain is limited to it acting as the golden record of both securities transactions processed through ID2S and asset/security ownership recorded on ID2S. Primary market issuance is processed within RSSS using blockchain technology. ID2S creates the issuance account in the blockchain and then records subsequent state changes in the blockchain relating to the movements between issuance, distribution and custodian/investor accounts.

Tokens to denote baskets of bonds for collateral swaps via HQLAx[40]

The HQLAx DLT-based platform allows for collateral swaps in the securities lending market. The securities are issued in a conventional environment and grouped in the form of baskets of securities. For the purpose DvP, the baskets are tokenised, i.e. represented on distributed ledgers by tokens. This process is aimed at eliminating the operational requirement to physically move securities across securities settlement systems.

Use of tokens to represent shares on a crowd investing platform provided by Conda AG[41]

Conda AG is a crowd investing platform that allows existing assets to be represented by tokens on blockchain and thus offered to potential investors. The platform is responsible for ensuring that only identified investors can purchase tokens. Whenever a token is transferred from one shareholder to another, an entry is created in the underlying Ethereum blockchain, on the basis of which the entry into the company's share register is made.

[39] See the ID2S website.

[40] See HQLA operating model.

[41] See Conda website.

Tokens representing securities registered outside the exchange to enable clearing and settlement in Australian Securities Exchange (ASX) CHESS[42]

Under the ASX value chain system, securities are recorded traditionally in a register outside ASX, while the Clearing House Electronic Subregister System (CHESS) securities are represented by tokens.

Issuance, custody and safekeeping take place outside ASX. All positions deposited in ASX Settlement are automatically recorded in an electronic subregister. ASX performs clearing and settlement functions under the supervision of the Australian competent authorities.

The payment leg is operated outside ASX in a real-time gross payment system (the Reserve Bank Information and Transfer System, RITS) by the Reserve Bank of Australia.

[42] See About CHESS Replacement.

Annex 2: Interoperability solutions[43]

System for on-chain communication of different blockchains by Cosmos[44]

Cosmos is a decentralised ecosystem of independent and parallel (proof-of-stake-based) blockchains that can scale and interoperate with one another using the Inter Blockchain Communication protocol. The Cosmos network operates as a central hub (the Cosmos Hub). The main token of the Cosmos Hub is called ATOM. It is used for staking and governing the blockchain. In particular, the token holder can be either a validator or a delegator. Validators operate a full node, which secures the network and processes transactions, while delegators delegate their ATOM tokens to validators based on their personal review regarding the trustworthiness of the validators and their ability to operate a node. A token also grants governance rights: one ATOM represents one vote for any proposal on the network, such as for software upgrades.

Interoperability platform by Polkadot[45]

The Polkadot project aims to deliver an interoperability platform for exchanging information and conducting transactions. The network contains four major stakeholders: validators, nominators, collators and fishermen. Validators do not maintain the fully synchronised database of all parachains; they delegate the task of storing to a collator. The main task of collators is to produce valid parachain blocks. The collator executes an unsealed block with a zero-knowledge proof and offers it to one or more validators, who take the responsibility for proposing a parachain block to the relay chain. Collators and validators receive transaction fees for their tasks. Fishermen are independent and monitor the behaviour of collators and validators.

Interoperability system for on and off-chain solutions via Digital Asset Modelling Language (DAML) by ASX[46]

The “CHESS replacement” will be within the ASX security perimeter on a permissioned network where only licensed participants will be authorised to access the system. Private contractual information will be encrypted and segregated. The shared aspect of the solution serves as a transaction notification and synchronisation mechanism and includes only hashes (one-way cryptographic functions). The DLT-based replacement for the CHESS system allows other companies to build new

---

43 The set of examples provided is illustrative and not exhaustive. Please note that the use cases describe the views of the companies leading the initiatives and not those of the Fintech-TF.

44 See the Cosmos website.

45 See the Polkadot website.

46 See About CHESS Replacement.

services that interact with the system via DAML, with the following three main connectivity options.

- Direct integration: a user transacts with the new system via a node. Initially this is only being offered to clearing and settlement participants but will be made available to other users over time.
- Messaging: The second option is messaging. It is similar to the way in which users currently interact with CHESS, i.e. by sending and receiving messages (using ISO 20022) to keep systems updated.
- New solution: A new secure browser-based solution can be used by low-volume users but also provides a channel for entering ad hoc messages which are not supported elsewhere.

Interoperability solution based on routing by Interledger Protocol (ILP)[47]

The ILP is a proprietary protocol based on routing and aimed at enabling the exchange of value across payment networks using "connectors" (“routers”) and "interledger packets". The details are as follows.

- The sender constructs and sends a “prepare” packet as a request to the connecting router. The packet is then forwarded until it reaches the receiver.
- The receiver accepts or rejects the packet by sending a “fulfil” or “reject” packet as a response. When the sender receives a “fulfil” packet, it knows that the packet was successfully delivered to the receiver.
- The sender then continues to send the remaining “prepare” packets until the value is fully transferred. The transactions are secured by means of conditional transfers.

Open source solution for connecting blockchains by FUSION[48]

Fusion aims to connect different DLTs by means of a common public blockchain using decentralised control rights management (DCRM), where assets are held and transferred on behalf of the user across heterogeneous chains. DCRM offers hot wallet liquidity with cold wallet security, a key recovery system, a settlement network and an option to introduce protection requiring multiple approvals for both on-chain and off-chain workflows.

---

47 See Interledger overview.

48 See the Fusion website.

Middleware solution for on-chain and off-chain systems by Chainlink[49]

Chainlink provides smart contracts with inputs and outputs in order to prove contractual performance, as well as multiple outputs to affect outside systems and send payments to complete the smart contract. Chainlink aims to facilitate the interplay of smart contracts and "real world" data, allowing them to be connected with key external recourses such as off-chain data and APIs. In addition, Chainlink aims to eliminate the problem of "single point of failure" that arises when smart contracts are connected to data input through a single node: before any data item becomes a trigger, it is evaluated multiple times in the decentralised oracle network, enabling the overall value of smart contract to be maintained.

DLT-based system for DLT solutions by Quant[50]

Quant's Overledger operating system is a DLT-based system for interconnecting and enabling interoperability between DLT-based and conventional systems. It is aimed at facilitating the communication, migration and exchange of information/value among different systems by allowing general purpose applications to run on top of them.

[49] See the Chainlink website.

[50] See the Quant website.

List of contributors

Participant's organisation	Name of participant
Monte Titoli – LSEG	Ms Chiara Rossetti (Chairperson)
European Central Bank	Mr Francesco Gavanna (Rapporteur)
BNP Paribas Securities Services	Mr Uwe Dreger
BNY Mellon	Mr Dirk Ooms
Citi	Mr Marcello Topa
Clearstream	Mr Michael Crezelius
Commerzbank	Ms Alexandra Rimpu
Deutsche Bank AG	Mr Boon-Hiong Chan, Ms Valerie Hoess
European Central Securities Depositories Association (ECSDA)	Ms Anna Kulik
Erste Group Bank AG	Mr Christoly Biely
Euroclear	Mr Glen Fernandes
European Banking Federation (EBF)	Mr Julian Schmucker
European Central Bank (ECB)	Mr Andrea Pinna
Frankfurt School Blockchain Center	Mr Philipp Sandner
HSBC Trinkaus Burkhardt AG	Mr Götz Röhr
Iberclear	Ms Lara Cortes
International Capital Market Association (ICMA)	Mr Gabriel Callsen
JP Morgan	Ms Montserrat Farina
KBC	Mr Koen Mertens
LBBW	Mr Florian Sager
Liquidshare	Mr Thibaud de Maintenant -
Main Incubator	Mr Michael Spitz
SIX-Securities Services Ltd. Switzerland	Mr Urs Sauer
State Street	Ms Ines Cieslok

Observers	
European Securities and Markets Authority	Ms Anne Choné
European Commission	Ms Bettina Friehs, Mr Peteris Zilgalvis
Bank of Greece	Mr Yorgos Korfiatis
Banque de France	Ms Anne-Catherine Bohnert
Deutsche Bundesbank	Mr Andre Witt
Oesterreiche National Bank	Mr Johannes Duong, Mr Hannes Hermanky
Suomen Pankki	Mr Aleksi Grym

Significant contributions were also made by Mr Rainer Olt and Mr Stefan Kromolicki.

Postal address 60640 Frankfurt am Main, Germany
Telephone +49 69 1344 0
Website www.ecb.europa.eu

For specific terminology please refer to the ECB glossary (available in English only).

PDF ISBN 978-92-899-4732-9, doi:10.2866/98734, QB-08-21-057-EN-N