EUROPEAN CENTRAL BANK

EUROSYSTEM

The potential impact of DLTs on securities post-trading harmonisation and on the wider EU financial market integration

Advisory Group on Market Infrastructures for Securities and Collateral

September 2017

Contents

List of abbreviations

AML - anti-money laundering

CeBM - central bank money

CMU - capital markets union

CoBM - commercial bank money

CPMI - Committee on Payments and Market Infrastructures

CSD - central securities depository

CSDR - Central Securities Depository Regulation

DLT - distributed ledger technology

DLT-TF - Task Force on Distributed Ledger Technologies

DTT - double taxation treaty

DvP - delivery versus payment

EMIR - European Market Infrastructure Regulation

ENISA - European Union Agency for Network and Information Security

ESCB - European System of Central Banks

EU - European Union

Eurosystem - the ECB and the NCBs of the 19 countries that have adopted the euro

FCD - Financial Collateral Directive

FMI - financial market infrastructure

GDPR - General Data Protection Regulation

HSG – Harmonisation Steering Group

IOSCO - International Organization of Securities Commissions

ISD - intended settlement date

ISIN - International Securities Identification Number

IT - information technology

KYC - know your customer

LEI - Legal Entity Identifier

MiFID II - 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

MiFIR - Markets in Financial Instruments Regulation

MSU - minimum settlement unit

NCB - national central bank

NIS - network information security

PBFT- practical Byzantine fault tolerance

PFMIs - principles for financial market infrastructures

RPO - recovery point objective

RTO - recovery time objective

SDR - settlement discipline regime

SFD - Settlement Finality Directive (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)

SMEs - small and medium-sized enterprises

SSS - securities settlement system

STP – straight-through processing

T2S - TARGET2-Securities

UTXO - unspent transaction output

WHT - withholding tax

Executive summary

Distributed ledger technologies (DLTs) have the potential to promote sharing of data and business processes beyond the level achieved by current distributed databases, which have been used for decades to allow participants spread across locations to read the content of a collection of data managed by a single institution.[1]

DLTs may bring value to market participants by allowing different institutions to share the management of information in a distributed ledger and to follow the same procedures to update this information. Each entity involved in the processing of financial transactions currently keeps an independent central record of its clients' asset holdings and needs to reconcile this record with data kept in other centrally managed databases at different levels of the post-trading value chain. Distributed ledgers could facilitate integration in post-trading by providing an infrastructure ensuring that every user has a consistent and updated view of the assets for which it is responsible and that the same assets can be transferred with a high degree of automation. However, these technologies are still at an early stage of development, so it is difficult to say whether any specific DLT will be widely adopted in the securities market, or whether its adoption will address the current market inefficiencies.

The possibility that DLTs may be adopted in the securities post-trade environment has been widely discussed in financial markets since 2015. Market players and public authorities have embarked on a learning process that has familiarised many of them with the foundations of distributed systems. Yet while the debate on DLT adoption has largely focused on technical features, discussions on the potential impact of DLTs on financial market integration are still at a preliminary stage.

In July 2016, in order to assess the relevance and possible impact of DLTs on the TARGET2-Securities (T2S) stakeholder community, the T2S Advisory Group (AG) agreed on a revised Harmonisation Steering Group (HSG) mandate that covers the potential impact of technological innovation on harmonisation and financial integration.[2] Based on this revised mandate, the HSG established the Task Force on Distributed Ledger Technologies (DLT-TF) to analyse the potential impact of technological innovation such as DLTs on the securities post-trade environment and how such innovation may affect the harmonisation efforts of the T2S stakeholder community. The DLT-TF also examines further harmonisation needs in view of the wider EU financial integration agenda.

The Advisory Group on Market Infrastructures for Securities and Collateral (AMI-SeCo) has produced the present report, which covers a wide range of aspects relating to the possible applications of DLTs, from issuance-related

1 See Chapter 0 for a description of the specificities of DLTs compared with other database technologies.

2 AMI-SeCo has taken over the responsibilities of the former T2S AG.

processes to diverse topics such as cyber security and reporting. However, the clear focus is on DLT applications tailored for use in post-trading services, with a particular interest in the settlement area. To simplify the approach to such a broad and often technical subject, the report is structured as follows: an introductory chapter describes basic concepts of DLTs that are useful for the ensuing analysis; Part I focuses on the possible impact of DLTs on some foundations of current financial markets such as account structures, the issuance of securities, and different forms of cash and their use in delivery-versus-payment (DvP) transactions; Part II is structured around the main issues relating to settlement – namely settlement finality, the settlement discipline regime (SDR), the settlement day schedule and calendar, settlement cycles, and connected services such as collateral management, asset servicing and reporting; Part III provides further insights into the relationship between DLT adoption and certain aspects of financial market infrastructures (FMIs) that do not concern the settlement process directly but which are relevant for their safe interaction with other market participants – such as digital identity, data privacy issues, cyber resilience, reporting and interoperability; and the concluding chapter presents some findings on the impact of DLTs on the securities post-trade industry.

Since it is not yet clear what specific use DLTs may have in the future and what DLT model will possibly be adopted by market participants, the analysis in the report revolves around different implementation scenarios. The choice of these scenarios is explained in Appendix 1. The scenarios are used in each chapter, either explicitly or implicitly, to illustrate the analysis of: (i) the potential impact of DLT adoption on current processes; and (ii) the new processes that could be introduced by DLT adoption.

Impact of DLTs on the foundations of current financial markets

The report addresses how possible implementations of DLTs could alter existing account structures, particularly for the crediting and debiting of securities held by financial and non-financial institutions and central securities depositories (CSDs), takes into account the relevant regulatory constraints when assessing the challenges posed by DLT adoption.

The chapter regarding issuance of securities in a distributed ledger is aimed at providing an understanding of the key challenges and opportunities of DLT adoption around this process in accordance with current regulatory constraints. The main questions addressed relate to the role DLTs could play in fostering the adoption of harmonised issuance processes, and whether current EU and national regulatory frameworks, as well as business practices, would allow such harmonisation.

Possible forms of DvP required to make DLT adoption feasible are assessed, focusing on different approaches to making cash available on a distributed ledger, both in the form of commercial bank money and, if a central bank were to find it appropriate, in relation to central bank money.

Impact of DLTs on settlement-related services

Finding legally defined moments for settlement finality that could be shared across DLT models is a crucial challenge, particularly when dealing with the insolvency of a participant. The report explores different scenarios where settlement is performed in a DLT-based settlement system, while addressing the current legal and regulatory constraints that have a significant impact on the design of such systems.

Regarding the potential adoption of DLTs in the settlement process, the analysis covers both tradeable and non-tradeable securities, stressing differences among the institutions involved and the importance of the roles they perform for the sake of financial market stability.

The impact of DLT-enabled processes on the settlement day schedule and on the settlement cycle are also analysed in order to identify potential challenges and opportunities brought by new arrangements that could differ from current T2S standards.

The potential benefits of using innovative technologies in various areas of asset servicing, collateral management and reporting are also discussed, with a focus on the expectations the market has developed with regard to the adoption of automation via smart contracts and digitised data but also in light of the fact that harmonisation is still needed in the processing of corporate actions and reporting.

Impact of DLTs beyond post-trade functions

DLTs have also been indicated as possible tools to improve the cyber resilience of database systems used by financial institutions and market infrastructures. In this respect, the report focuses on analysing what changes DLT adoption could bring in comparison with mainstream database technology.

Interoperability among different DLTs and with non-DLT solutions would be required in the above-mentioned areas of interest for post-trade functions. Such interoperability would probably be necessary in the case of DLT adoption, at least for a provisional period but possibly permanently.

Findings of the report

The report draws several main conclusions on the potential impact of DLTs on: (**i) harmonisation in the T2S context;** and (**ii) the broader integration of financial markets in Europe**.

With regard to the first point, DLT adoption could impact T2S harmonisation activities in a number of ways depending on the different adoption models. DLTs can in principle accommodate omnibus account structures (T2S harmonisation activity 13 – **Availability of omnibus accounts**), including for the provision of appropriate

services on those accounts (T2S harmonisation activity 14 – **Restrictions on omnibus accounts**). This means that agreed T2S standards could in principle be kept in the case of DLT adoption, but it does not ensure that developers and adopters of the technology will take a unanimous decision in that respect.

An instance where DLT solutions currently under development appear to be diverging from standards agreed in the T2S community is that of securities and cash account numbering (T2S harmonisation activities 15 and 16 – **Securities accounts numbering** and **Dedicated cash account numbering**), where the use of public keys to identify DLT users may diverge from T2S agreed standards.

If DLT and non-DLT solutions are to coexist, interoperability between the two approaches needs to be ensured. There may be a need to provide ad hoc matching fields where a participant holds both a DLT and non-DLT account (T2S harmonisation activity 2 – **T2S mandatory matching fields**).

In T2S, all participants adhere to a harmonised definition of legally defined moments relating to settlement finality (T2S harmonisation activities 7, 8 and 9 – **Settlement finality I**, **II** and **III**). Potential DLT adoption may also introduce fragmentation among the settlement finality rules of different systems, which would hamper their ability to interoperate. For most transactions, there will always need to be a designated system recognised by the EU public authorities to ensure that counterparties are protected against insolvency procedures. Unique settlement finality moments could then be defined by the operator of a securities settlement system even in a DLT environment. However, the technical and operational requirements of DLT adoption could introduce fragmentation since different definitions of settlement finality are compatible with different DLT models.

With respect to the settlement cycle timeline (T2S harmonisation activity 12 – **Settlement cycles**), the adoption of DLT solutions, if fully interoperable across all involved institutions, could allow straight-through processing (STP) and “settlement at trade”. Nonetheless, costs borne by market participants in terms of additional liquidity need to be carefully considered.

Encoding of automated procedures for corporate actions requires a high level of standardisation. To date, standardisation has been slowly implemented using mainstream technology (T2S harmonisation activities 6 and 18 – **T2S corporate actions standards** and **Corporate actions market standards**). In future, standards are likely to require further detailed definition to allow the use of smart contract capabilities. The same is true for tax withholding responsibilities across European markets (T2S harmonisation activity 20 – **Withholding tax procedures**).

With respect to **settlement discipline**, a fully harmonised SDR approach is imminent for European markets, and will be complemented by a specific standard in T2S markets (T2S harmonisation activity 11 – **Settlement discipline regime**). There is a risk that DLT settlement solutions could create different approaches to the settlement model and the use of embedding to deal with settlement fails. DLT-enabled systems with potentially instantaneous settlement would prevent settlement fails. For any other settlement cycle it should be noted that, to the extent that the

functioning of new technologies affects settlement models, amendments to regulations may eventually need to be considered to deal with those differences.

Solutions to allow T2S CSDs to interface DLT-enabled securities settlement systems with the T2S platform based on mainstream technology, possibly allowing DvP via standard real-time gross settlement (RTGS) system dedicated cash accounts, may require the definition of new harmonisation activities to allow such connectivity. The possible introduction of a variety of DLT-based payment systems might introduce the need to ensure technical interoperability between old and new systems dealing with **commercial bank money**. No negative impact on financial integration is foreseen in the realm of **central bank money** in the euro area, since a common DLT model would be developed if DLTs were to be deemed viable for Eurosystem market infrastructures in the future.

Beyond its impact on T2S harmonisation activities, the potential use of DLTs might have considerable implications for EU financial market integration. In particular, the market may want to consider **ISO 20022 extension** into smart contract initiation and coding, as well as DLT-specific concepts.

Regarding collateral management processes, cross-border mobilisation is found to remain a challenge, although DLT-based solutions could bring benefits from the purely operational point of view.

For issuers and investors to have improved access to the capital markets, it is necessary for DLT models to be interoperable and for the same securities to be available through different mechanisms. Creating a post-trade environment where the accounts of different DLT networks would merely **coexist without interoperating** is not an optimal outcome, as it would create a fragmented post-trade landscape.

The report highlights that it is as yet unclear whether a distributed ledger is the best way to control access to data which may be held externally. The need for know-your-customer (KYC) and anti-money laundering (AML) checks may themselves become a hurdle to the adoption of DLTs in financial markets unless participants in a DLT network find a common way to deal with digital identities and to share on-boarding processes, sensitive data and connected responsibilities among them and with the participants in any other interoperable system.

The report stresses that restricted networks are likely to be necessary to ensure proper governance and accountability and that, if adoption of a new technology affects settlement models, the regulatory framework could require amendments to avoid regulatory arbitrage.

Proper **governance** of any market infrastructure is important to ensure its safety and efficiency. It is even more important in the case of a DLT network, where different legal entities share responsibility for at least some processes and data. The potential adoption of DLTs will require the development of appropriate governance to ensure that responsibilities regarding **data handling** are clear and that a **cyber resilience** framework can be adopted in a way that ensures full commitment by all

network participants to the common good of data integrity and protection from external threats. Ultimately, the aim would be to achieve industry-wide international agreement on the approach via the Committee on Payments and Market Infrastructures (CPMI) and the International Organization of Securities Commissions (IOSCO), as this would facilitate long-term interoperability and integration between securities markets globally. Thought should be given to any interfacing systems, as DLT might not be applied as a solution on its own.

It is important to note that a number of elements of a theoretically DLT-enabled financial market have to be properly designed and put together before DLT adoption can be considered a realistic possibility in the securities settlement space.

In consideration of a future scenario where DLTs might potentially be adopted by market participants, the T2S stakeholder community has an interest in fostering safety and efficiency in T2S by maintaining currently agreed standards or even considering introducing new ones, if required.

1 Introduction to the report

Although distributed ledgers were first developed in the realm of virtual currencies, they have emerged since 2015 as an innovation that may change the current paradigm of financial markets, particularly as far as market infrastructures are concerned (see CPMI, 2017). Distributed ledger technologies (DLTs) allow different users to share the management of data, possibly to process financial market transactions and keep track of their holdings of securities and cash.

The Advisory Group on Market Infrastructures for Securities and Collateral (AMI-SeCo) advises the Eurosystem on issues related to the clearing and settlement of securities and to collateral management. The possibility that DLTs may be used in securities post-trading in the future prompted the AMI-SeCo to launch an analysis among European securities market participants in order to develop a view on DLTs in general and their possible impact on European markets.

This report is published by the AMI-SeCo to communicate the main findings of this analysis. It focuses in particular on how the potential adoption of DLTs in the securities post-trade environment might affect the harmonisation efforts of the TARGET2-Securities (T2S) stakeholders, as well as examining further harmonisation requirements in view of the wider EU financial integration agenda. The AMI-SeCo has identified a set of topics of key importance for post-trading and has analysed the potential impact of DLTs on current processes and on the new processes possibly enabled by such technological innovation in different scenarios of adoption, also highlighting specific actions to be taken by all financial market stakeholders where necessary.[3]

This introductory chapter provides a concise background to the analysis covered by the rest of the report. Technical terminology that is specific to DLTs is highlighted in bold the first time it appears in the text and is explained in Appendix 3. Chapter 2 provides a functional analysis of the concept of securities accounts and possible account structures using DLTs. Chapter 3 deals with the topic of issuance of securities in a distributed ledger. Chapter 4 describes **arrangements** that could in theory be used to transfer cash between users of a **distributed ledger** and to achieve delivery-versus-payment (DvP) settlement. Chapter 5 addresses the issue of finality of settlement in a DLT environment. Chapter 6 describes the possible consequences of DLT adoption for settlement discipline. In Chapter 7, the issue of possibly differing settlement calendars and schedules is discussed together with the expected impact of shorter settlement cycles on market liquidity. Chapter 8 describes possible uses of DLTs in the provision of collateral management services. Chapter 9 focuses on asset servicing in the case of DLT adoption, both as a stand-alone process and as part of the settlement process. Chapter 10 focuses on reporting. Chapter 11 addresses the issue of cyber resilience in a DLT environment, drawing a comparison in this respect with current **mainstream technologies**.

[3] See Appendix 1 for an overview on the scenarios considered in each chapter.

Chapters 12 and 13 discuss the issues of identity management and data privacy respectively. Chapter 14 focuses on interoperability among DLTs, and between DLTs and legacy systems. Chapter 15 draws conclusions, from the analysis in the previous chapters, on the potential impact of DLTs on harmonisation in the T2S context and the broader integration of financial markets in Europe.

1.1 A taxonomy of DLTs and DLT models

Distributed databases have been widely used for years, allowing users who are spread across different locations to query and often propose updates of data under the control of a single database management system owned by an institution at one or more **data centres** (see Government Institutes, 1997). The term **distributed ledger** has been recently coined to identify a type of distributed database whose content is not only proposed via – and distributed to – a number of computers. In fact, distributed ledgers are characterised by the possibility for some or all different users to share responsibility for database management, even if they do not necessarily trust one another, and to agree on the insertion of new data records which can nevertheless be considered reliable.

Distributed ledgers can then be seen as a particular type of distributed database – a "shared database" – where a set of mostly well-known technologies are combined in new ways. This allows a division of responsibilities for the decisions as to what information should be considered up-to-date in the absence of full reciprocal trust among users, and for users' infrastructures. A task of this kind is not trivial. A number of new solutions have been suggested since the Bitcoin blockchain (see Nakamoto, 2008) was proposed to resolve the difficulties posed by sharing a database to transfer value with no single validating authority. The issues at stake are not new in the field of distributed systems and include, inter alia, (1) malicious behaviour (such as **double-spending**, **repudiation** and **Sybil attacks**) and (2) the possibility that different users may rely on inconsistent versions of the data (due to network latency or the validation of conflicting **forks**).

DLTs are a diverse set of solutions that combine database technology and cryptography in order to tackle the two above-mentioned issues by allowing ultimate cryptographic auditing of users' activity – in some cases giving economic incentives – and by providing traditional and new mechanisms to achieve **consensus** among users on the status of the database over time. As will become clear in the following chapters of this report, different DLTs have different implications for financial markets, and it is not possible to cherry-pick or to avoid the specific advantages and drawbacks that are bundled in different **DLT models** – i.e. in the different implementations of DLTs with regard to data structures, consensus algorithms, data transparency and roles played by network participants.

Looking at the still-mutable DLT landscape, at a level of granularity just beyond the generic reference to DLTs, the following specific types of DLT can be identified (see Pinna, 2017): (1) **blockchains**, where any changes to the identities of current users entitled to send an **unspent transaction output** (UTXO) representing asset

holdings are processed in batches (**blocks**) which are then linked together via cryptographic techniques (**hashing**); (2) **consensus ledgers**, where snapshots of balances associated with each user are updated in rounds; and, more recently, (3) **synchronised bilateral ledgers**, where counterparties can update the subset of information that refers directly to their bilateral activity (possibly with other elected parties also accessing these records) and make some of that information available to a broader set of users. **Smart contracts** are another technology that can be associated with DLTs when they are processed across nodes in the network. These contracts are written as **executable code.** Under the contracts, the counterparties certify that the respective assets are to be sent or received on their behalf via automated procedures that are processed when a set of pre-specified events happen either inside the ledger (e.g. holding balance of a user) or outside the ledger (e.g. asset price).

Opinions diverge on whether DLTs can be considered truly innovative from an IT perspective. What matters for present purposes is that these technologies could prove highly relevant to financial market infrastructures, institutions, and regulators in the event that they are ever used to record financial transactions or asset holdings in the realm of payments and securities transactions. The main peculiarity of distributed ledgers resides in the opportunity they provide for the network of users – or system participants, in the case of market infrastructures – to rely on a shared source of reliable information, even when a central entity is not available either by choice or by accident. The download of data recorded by a central entity (the server) into copies held by users (the clients) is therefore replaced by **distributed consensus algorithms**, which are intended to ensure, on the basis of certain assumptions, that information is correct and consistently replicated across all users of the network.

1.2 Types of distributed consensus algorithms

Distributed ledgers could represent a paradigm shift in financial markets, where the trade and settlement instructions sent by two counterparties are currently executed, matched, and settled via book entries in proprietary databases, each kept by a specific financial intermediary or market infrastructure for its clients. Widespread adoption of DLTs could in theory mean that market players would interact by participating in a distributed arrangement. The level of peer-to-peer interaction that can be achieved by DLT adoption depends on the specific DLT model considered. In particular, consensus algorithms used to agree on the information recorded in distributed ledgers can be divided into at least the following two types: **probabilistic** and **deterministic**.[4]

Probabilistic consensus algorithms – e.g. **proof of work** and some implementations of **proof of stake** – allow **validators** to independently select a specific set of

[4] Throughout this report, a distinction is made between probabilistic and deterministic consensus. This is in order to capture the level of certainty with which a DLT network participant can consider agreed updates to be irrevocable or not.

pending transactions they would like to process among those broadcast by all DLT network users. Each validator assumes to be aware of the latest agreed version of the ledger and assesses the chosen transactions against it as well as against the rules followed by the network – inter alia, by checking that the sender holds the assets transferred with each transaction.[5] Each validator may propose an updated state of the ledger – either in terms of new valid transactions and/or the ensuing holding balances – to the other validators, who need to decide whether or not to accept it.[6] However, other validators may have performed the same check in the meantime, on a different set of transactions, and proposed the latter to network users. It may then happen that different users momentarily accept different versions of the ledger, each without knowing that the rest of the network is working on a different set of information. In such a case, a **fork** is said to emerge in the ledger, since, starting from a common path, some validators agree on a specific set of new transactions (i.e. ledgers updates) whereas others agree on a different way forward. The persistence of such inconsistencies varies across DLT solutions and depends on factors such as network latency. Users can meanwhile consider a new record in the ledger as being agreed only with a certain degree of probability. This probability increases over time as new transactions are validated on the same grounds, but the record is never certain to remain unchanged (see the reference to the sometimes misunderstood concept of immutability below).

Deterministic consensus algorithms – e.g. **practical Byzantine fault tolerance** (PBFT) algorithms – do not require validators to work in parallel on different sets of pending transactions. For instance, for each round of validation, a leader can be chosen among a restricted set of validators. This leader would be able to propose the pending transactions to be processed by all other validators provided that a prearranged quorum agrees on such a list. This type of consensus algorithm ensures that different batches of transactions cannot be processed in parallel. It therefore rules out the possibility that different updated ledgers may be agreed upon by different clusters of validators, unless the network is for some reason partitioned and different clusters of validators remain isolated and are able to elect different leaders. However, only a cluster containing a sufficient number of validators can reach the quorum enabling validation of ledger updates, and service provision is unaffected as long as update requests can reach such a cluster. The network is unable to validate new transactions when partitioning leaves only minority clusters. That means a fork cannot happen and a record update is never reversed once consensus is achieved, but it also implies the weakness that deterministic consensus requires a minimum number of validators to stay connected to validate new transactions – something that is not necessary in the case of probabilistic consensus. Moreover, the amount of messages exchanged among all participants in

[5] It should be noted that, due to network latency, other users may have meanwhile validated other transactions and agreed on a newer version of the ledger.

[6] Updates can only be proposed under certain conditions – for instance, in the case of proof of work, only if a certain resource-consuming task has been performed by the validator.

the deterministic consensus algorithms limits the number of validators allowed before network bandwidth affects the latency of transaction updates.[7]

1.3 Types of participants

Users of a DLT application can access the network by means of cryptographic keys that allow them to read and propose transactions involving their holdings recorded in the ledger. All or some nodes in the network can also act as **validators**, as previously mentioned, by assessing requests for ledger updates on which they achieve consensus with peers. Other nodes may be requested to act as gatekeepers, possibly connecting their legal identities in the "real" world with those used in the DLT network (see Chapter 10 on digital identity), or as certificate authorities to testify the legitimacy of any user to initiate a transaction.

With respect to access by users to a DLT network and the roles played by different nodes, at least three different types of DLT network can be identified (see Table 1). **Unrestricted systems** are those, like the original Bitcoin blockchain and many other virtual currencies, which any unknown entity can access in order to play any role. In a **restricted egalitarian system**, all users can still play any role but participation is restricted to identified and accountable entities. Finally, **restricted tiered systems** not only restrict participation to identified and accountable entities but also introduce separation between the roles that each participant may play in the network, e.g. allowing only some users to also act as validators.

Table 1

Access to the network

Restricted tiered network	Restricted egalitarian network	Unrestricted network
Only identified and accountable entities use the DLT and can be assigned different roles	Only identified and accountable entities use the DLT and can play any role	Any unknown entity uses the DLT and can play any role

Source: Pinna (2017).

These three different configurations of a DLT system have wide-ranging implications. First, restricted systems provide tools to hold participants legally accountable for their activity in the ledger, whereas unrestricted systems do not. Terms and conditions can be defined, in restricted systems, to allocate responsibilities to accountable legal entities. Rubber-stamping of the latest agreed ledger by an authoritative institution is only possible in a tiered network (see Chapter 5 on settlement finality), and this has conflicting effects on cyber resilience (see Chapter 11).

[7] Having a limited number of validators does not necessarily restrict the number of simple users, as explained in the following section.

1.4 Transparency and “immutability” of distributed ledgers

Distributed ledgers can be either public, in which case they record information in a transparent way and can be read by anyone, or private, in which case data are encrypted and only authorised users can access them. The transparency of data recorded in distributed ledgers was a fundamental feature of the first pioneering DLT applications. Full replication of data allowed every validator to assess the validity of transactions submitted by any other user and ensured that no user could affect the network by deleting or modifying any reasonably accessible number of copies of the ledger. The same level of transparency is unwarranted in financial markets, where the confidentiality of data among market participants is necessary inter alia to hide trading strategies, limit price volatility, and protect the privacy of end investors.

Immutability is often mentioned among the features of a distributed ledger, either with a positive or with a negative connotation. In fact, distributed ledgers managed by any technology, including blockchain, are mutable, and their content can be modified as soon as a sufficient amount of resources are invested. Depending on the DLT model under consideration, necessary resources may include computational power and electricity, a stake in the network (tokens, collateral), or reputation (votes). A common misunderstanding over the concept of immutability comes from the fact that a DLT among untrusted parties can only work if the cost incurred by a malicious user tampering with the ledger is higher than the connected expected benefit – meaning that a rational economic agent would not choose to modify it – and consensus algorithms in the realm of unrestricted networks have been designed to achieve that objective owing to a lack of legal accountability on the part of their participants.

The high cost of validation via proof of work is intended to make validation of transactions profitable only if their validity is confirmed by the rest of network participants, who can access information in the public ledger and is remunerated accordingly. Algorithms such as proof of stake have been used in an attempt to decrease the costs associated with ledger operation by levying a cost on misbehaviour where validation of illicit transactions can be detected and punished by users of a public ledger. In restricted networks, where rules can be enforced on accountable legal entities, the efficacy of a cost-benefit analysis confined to resources and assets recorded on-ledger is unproven. As long as illicit behaviour can be detected by harmed parties and disputes resolved by proper governance or judicial frameworks, the necessity for public ledgers disappears, allowing for some level of data confidentiality (see Chapter 13), although this may mean foregoing part of the cyber resilience brought by data replication in DLT networks (see Chapter 11).

PART I – DLTS AND SOME FOUNDING ELEMENTS OF FINANCIAL MARKET INFRASTRUCTURES

2 Accounts and account structures in a DLT environment

2.1 Introduction

The purpose of this chapter is to identify how DLT adoption could affect existing account structures, notably in view of the regulatory constraints imposed on issuers and central securities depositories (CSDs) by the Settlement Finality Directive (SFD)[8] and the Central Securities Depository Regulation (CSDR)[9].

The notion of "securities" used throughout this chapter and the rest of the report includes both transferable securities within the sense of Article 4(1)(44) of the revised Markets in Financial Instruments Directive (recast – MiFID II)[10] that are admitted to trading or traded on a trading venue, or which are transferred following a financial collateral arrangement as defined in point (a) of Article 2(1) of Directive 2002/47/EC (hereinafter "tradeable securities") and have to be recorded in a CSD under Article 3(2) of the CSDR; and transferable securities within the sense of Article 4(1)(44) of MiFID II that are not admitted to trading or traded on a trading venue (hereinafter "non-tradeable securities"), unless specified otherwise. The following analysis focuses on the function of securities accounts in the lifecycle of a security after its creation – namely for issuance, transfer, and servicing – and is aimed at identifying whether a possibly equivalent notion exists in different DLT environments. The creation of the securities is out of scope, since, under the current legal framework, it is a matter of applicable company law in Member States.

2.1.1 Securities accounts (settlement accounts) and book entries

Securities accounts are provided and maintained to define asset holdings. They are distinct from issuance accounts, which allow recording of all securities of the relevant issue (see Section 2.1.2), and from registers providing evidence for the purpose of national company law (see Section 2.1.3).

Notion of securities accounts

The legal framework applicable to securities holdings and accounts is highly fragmented. At European level, there is no comprehensive definition of the concept

8 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).

9 Regulation (EU) No 909/2014 of the European Parliament and of the Council of 23 July 2014 on improving securities settlement in the European Union and on central securities depositories and amending Directives 98/26/EC and 2014/65/EU and Regulation (EU) No 236/2012 (OJ L 257, 28.8.2014, p. 1).

10 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, pp. 349-496).

of “securities account”. In fact, the legal nature of a securities account (i.e. statutory record, contractual construct or accounting device) and the legal nature and effects of book entries are still embedded in national law.

However, several EU legal acts define in functional terms the notion of a “securities account”. This at least allows its fundamental features to be defined from a functional perspective. In particular, Article 2(1)(28) of the CSDR defines a securities account generically as “an account on which securities may be credited or debited”. In the same vein, Article 2(1)(h) of the Financial Collateral Directive (FCD)[11] defines a relevant account as “the register or account – which may be maintained by the collateral taker – in which the entries are made by which […] book entry securities collateral is provided to the collateral taker”. In addition, MiFID II mentions, among ancillary financial services, the “safekeeping and administration of financial instruments for the account of clients […] excluding maintaining securities accounts at the top tier level”. Hence, maintenance of securities accounts is part of the provision of securities safekeeping and administration by a financial institution on behalf of a client – which does not necessarily correspond to an end investor.

At the global level, Article 1(c) of the UNIDROIT Convention on Substantive Rules for Intermediated Securities (Geneva Securities Convention (GSC), not yet entered into force) defines a securities account as an “account maintained by an intermediary to which securities may be credited or debited”.

In light of the above, AMI-SeCo members have agreed that the substance of a securities account, from a functional perspective, lies in the provision and maintenance, by a financial institution (account provider), of a storage of information that records credits and debits of securities positions of a client (account holder). Securities accounts exist at top level (with CSDs) and throughout the chain of intermediaries.

Functions of securities accounts

The paradigm of a securities account for book entry securities is that the investor or an intermediary entrusts the securities to a third party that is interposed between itself and the issuer. This results in relationships between:

- the issuer and the investor as regards rights and obligations arising from shares and bonds;
- the account provider (financial market infrastructure or intermediary) and the account holder (financial market infrastructure, intermediary or end investor) under a contract for the holding and possibly servicing of the securities.

[11] Directive 2002/47/EC of the European Parliament and of the Council of 6 June 2002 on financial collateral arrangements (OJ L 168, 27.6.2002, p. 43), as amended by Directive 2009/44/EC of the European Parliament and of the Council of 6 May 2009 amending Directive 98/26/EC on settlement finality in payment and securities settlement systems and Directive 2002/47/EC on financial collateral arrangements as regards linked systems and credit claims (OJ L 146, 10.6.2009, p. 37).

Securities accounts fulfil certain core functions that are listed below. How they precisely fulfil these functions is dependent on the applicable national law and is not considered in this chapter.

First function: attributing rights in securities and flowing from securities

Depending on the applicable national law, book entries in securities accounts may create or represent (themselves or along with additional perfection requirements) rights in securities. The content of the entitlement represented by the book entry is to be determined with reference to the applicable national law. Importantly, securities accounts allow also for the acquisition or disposition of limited rights in securities, such as collateral rights.[12]

Securities accounts may also enable securities holders (possibly end investors) to exercise their rights flowing from securities. Depending on the applicable national framework, securities holders may exercise directly the rights flowing from securities or allow intermediaries to exercise such rights.

In a cross-border holding chain, intermediaries may be required to disclose the identity of the securities holders to issuers or pass on information that enables the exercise of the rights flowing from securities from the securities holders (see Chapter 9, Asset servicing).[13]

Second function: evidencing ownership rights or interests

Depending on the applicable national law, the credit of an investor's securities to the account maintained by a direct intermediary may constitute or evidence possession or ownership of the securities, or other interests in securities.

Third function: transferring securities (settlement)

The securities accounts enable an account holder to transfer securities to another party by debits and credits to securities accounts along the chain of intermediaries. The specific rights conferred to investors by means of new records in the relevant securities accounts depend on applicable law, but updating such accounts settles the obligations that are taken by those investors when buying or selling certain financial instruments.[14]

Regulatory constraints

Account holders are subject to several regulatory constraints aimed at ensuring the smooth functioning of securities accounts and investor protection. National

12 Depending on applicable law, collateral might be acquired by debit and credit of securities accounts, by earmarking or control agreements.

13 The recast of the Shareholder Rights Directive (Directive (EU) 2017/828 of the European Parliament and of the Council of 17 May 2017 amending Directive 2007/36/EC as regards the encouragement of long-term shareholder engagement (OJ L 132, 20.5.2017, pp. 1-25)) is expected to improve the cross-border exercise of shareholders' rights.

14 These financial instruments are namely transferable securities, money-market instruments, units in collective investment undertakings and emission allowances (Article 2(1)(7) and Recital 12 of the CSDR).

legislation may require intermediaries to process corporate actions or facilitate the exercise of shareholder rights in securities (Article 3 of the Shareholder Rights Directive (SRD)) or provide information about securities holdings to the issuers.[15]

At top tier level, CSDs maintaining securities accounts for tradeable securities are subject to the regulatory requirements of the CSDR. In particular, CSDs should keep records and accounts that enable any participant to segregate the securities of the participant from those of the participant's clients and must offer the option of omnibus client segregation or individual client segregation.[16] Similar requirements apply in the case of CSDs acting in an "investor CSD"[17] capacity.

2.1.2 Issuance accounts

The notion of an issuance account is not defined in a common European legal act. From a functional perspective, an issuance account is an account opened in the name of an issuer in the books of a CSD, possibly as a way to comply with the requirement set out in Article 3 of the CSDR that securities admitted to trading or traded on trading venues have to be initially recorded in a CSD. In this case, the CSD acts in an "issuer CSD"[18] capacity.

Besides CSDR requirements, the initial recording in a CSD is subject to additional national provisions. All securities of the relevant issue are recorded on the debit of the issuance account, which allows a predetermined and immutable number of securities to be issued in the settlement system in book entry and provides a reference for the amount of securities available in the settlement system.

CSDs have to preserve the integrity of the issue (Article 37 of the CSDR),[19] i.e. to ensure that the number of securities making up a securities issue or part of a securities issue recorded in the CSD is equal to the sum of securities recorded in

---

15 The recast of the SRD, which has to be implemented by 10 June 2019, requires Member States to ensure that issuing companies have the right to identify their shareholders. However, Member States may exclude that right if shareholders of companies having their registered office in their territory hold less than a certain percentage of shares or voting rights which shall not exceed 0.5% (Article 3a of the SRD). Member States must also ensure that intermediaries transmit without delay from the company to the shareholders all information required to ensure that the shareholder is able to exercise rights flowing from its shares (Article 3b of the SRD).

16 See Article 38(3) and (4) of the CSDR.

17 Cf. Article 1(f) of the Commission Delegated Regulation (EU) 2017/392, "investor CSD" means a CSD that either is a participant in the securities settlement system operated by another CSD or that uses a third party or an intermediary that is a participant in the securities settlement system operated by another CSD in relation to a securities issue.

18 Cf. Article 1(e) of the Commission Delegated Regulation (EU) 2017/392, "issuer CSD" means a CSD which provides the core service referred to in point 1 or 2 of Section A of the Annex to Regulation (EU) No 909/2014 in relation to a securities issue.

19 The CSDR does not interfere with the national law of the Member States regulating the holdings of securities and the arrangements maintaining the integrity of securities issues (Recital 42 of the CSDR). However, Article 59 ff. of the RTS on CSD Requirements (Commission Delegated Regulation (EU) 2017/392 of 11 November 2016 supplementing Regulation (EU) No 909/2014 of the European Parliament and of the Council with regard to regulatory technical standards on authorisation, supervisory and operational requirements for central securities depositories, C/2016/7159 (OJ L 65, 10.3.2017, pp. 48-115)) contains numerous provision on reconciliation requirements.

the securities accounts of the direct holders or participants in the securities settlement system operated by the CSD, depending on the holding model.

While the issuance account allows the introduction of securities into the holding chain, settlement of a securities transaction still requires investors who are not direct CSD participants to hold securities in the accounts credited and debited by the relevant account providers.

2.1.3 Registers

Registers are kept by issuers or third parties (e.g. issuer agents, entities authorised to act as a registrar, CSDs), to which this task is outsourced. Registers record ownership or legal holdings in securities for the purposes of national company law, in particular for the identification of securities holders by issuers and the exercise of rights attached to the securities (i.e. corporate actions).

2.2 Possible scenarios under the current regulatory framework

At present there is neither a single DLT nor a single configuration for business interaction among users in a DLT environment. An analysis of different scenarios is therefore required. This chapter examines three main scenarios and their consequences in terms of account structure: a DLT network for securities not issued in a CSD (2.2.1); a DLT network used for the internalised settlement[20] of transferable securities (2.2.2); and a DLT network designated as a securities settlement system (SSS)[21] for securities, such as tradeable securities, that are issued in a designated SSS (2.2.3). Each of these scenarios has different implications for securities account structures. The case of securities issuance in a DLT network is addressed separately in Chapter 3 of the report.

2.2.1 DLT network for securities not recorded in a CSD

A DLT network for transactions in securities not recorded in a CSD, as is possible in the case of non-tradeable securities, is not subject to the regulatory constraints of the CSDR unless the network constitutes an SSS within the meaning of Article 2(1)(10) of the CSDR (see also Section 2.2.3). In this case, the DLT network does not have to be designated as an SSS, and the operator (if any) of such a network may be any financial or non-financial entity (including the issuer of the securities). Also, the settlement finality rules of the SFD do not apply (see Chapter 5 on settlement finality). Although such a DLT network may possibly operate outside the

[20] See Article 2(1)(11) of the CSDR.

[21] See Article 18(2) of the CSDR.

current EU regulatory framework, it may still be subject to national regulation or company laws.

Depending on the specific DLT solution (including the involvement of different parties in the validation of new transactions), an issuance or securities account might not exist in this network. From a functional perspective, in view of the definition of a securities account provided above (see Section 2.1.1), the absence of a financial institution debiting or crediting balances might exclude the existence of securities accounts where the validation is performed by the issuer or by end investors in the DLT network. However, the applicable national law may explicitly recognise ledger records as account.

All in all, the existence of a securities account seems to depend on the types of participants involved in the DLT solution and the applicable national framework concerning the notion of an issuance/securities account and the financial instruments that can be deposited in a securities account. Accordingly, depending on the DLT model and applicable national law, the legal entity using a DLT network might issue non-tradeable securities in the ledger without opening an issuance account at a CSD and might settle transactions without using securities accounts.

2.2.2 DLT network for internalised settlement in transferable securities

A DLT network might also be operated by a financial institution (credit institution or investment firm subject to prudential supervision) acting as a settlement internaliser (as defined in Article 2(1)(11) of the CSDR), either exclusively for its own clients or in a consortium. The adoption of DLTs by financial institutions could allow the use of the new technology also in the case of transferable securities, with a view to making current post-trade processes more efficient, subject to the assessment of safety requirements by relevant public authorities.

In this case, a contractual relationship between account holder and account provider exists, which should be complemented by recognition under the applicable accounting principles. Therefore, the above-mentioned functional definition of securities accounts applies. An account provider would be identifiable in the intermediary who manages the DLT network, when it is the only intermediary involved. In the case of a consortium, the account provider may be identified through a bilateral agreement signed by users with a specific intermediary, whereas the case of a consortium having a bilateral contractual relationship with users would be likely to qualify as a system and is considered in Section 2.2.3 below.

To be more specific, the *first function* of securities accounts could be met in a way that is similar to the current market set-up, since the balances are either available directly in the ledger or can be computed by aggregating asset transfers that are recorded in the ledger. The same applies to the *second function* of securities accounts, i.e. the evidence of ownership rights or interests. The *third function*, the settlement of securities transactions, remains unaffected, since by definition the settlement internaliser executes transfer orders on behalf of its clients.

2.2.3 DLT network designated as an SSS

A DLT network designated as a securities settlement system would need to be operated by a CSD that complies with CSDR requirements (see Article 18(2) of the CSDR), including minimum capital requirements, conduct of business rules, prudential rules, etc. The CSD, as system operator, would need to establish a formal set of rules governing the relationship between the participants and the operator. Where a CSD operates a DLT network, it is technologically feasible to meet the regulatory requirement to offer the option of omnibus client segregation or individual client segregation under Article 38(3) and (4) of the CSDR. This can happen for instance by means of sidechains, which are ancillary ledgers that are able to interact with a main reference ledger. When, in the case of blockchains, a token is credited to the address of a participant or smart contract managing a sidechain, the same token can be assigned to different sidechain participants who would then have their holdings segregated.

In the following, we distinguish among different validation models to address the question of whether a securities account exists in a DLT network.

Validation by the CSD

Where a CSD as the system operator also validates ledger updates, the functions performed by a securities account are not affected by the use of DLTs. This solution refers to an application of distributed databases already in use by some corporations, where data are managed collectively by different machines that are under the control of the same entity. Some market infrastructures have reconsidered this relatively traditional solution and found it might improve the efficiency of securities markets without changing their existing role as account providers. The question whether, from a legal perspective, a securities account exists, would not be affected by the adoption of such technology since the CSD could always hold, in its legacy system, an updated copy of the account balances updated by the CSD itself (see also the relevance of this in relation with settlement finality addressed in Section 5.2.1).

Validation by CSD participants

Where a DLT network is used in a designated SSS, the fact that its participants may update top tier level accounts by validating new transactions could be considered as outsourcing of parts of the settlement service (which is among the core services of a CSD) to third parties. The outsourcing is subject to authorisation by the national competent authority (NCA) under the condition that, inter alia, it "does not result in depriving the CSD of the systems and controls necessary to manage the risks it faces".[22] Hence, a CSD remains fully responsible for ensuring that the DLT protocol

[22] See Article 30(1) of the CSDR.

it adopts does not endanger the integrity of the issue and it stays liable towards direct participants. In addition, it is obliged to monitor the activity of the validators.[23]

With regard to the responsibilities towards end investors in a DLT system, based on ongoing DLT projects two different possibilities are likely to emerge.

1. A specific SSS participant is appointed by each client and is primarily responsible for proposing the validation of all updates related to each client's asset holdings, whereas other participants contribute only by validating those updates. In such a case, there is a contractual relationship between a specific SSS participant (elected primary validator) administering a client's securities positions and the client itself. In addition, there is contractual relationship between the SSS operator and its participants, at least in relation to the outsourcing of part of the settlement function. The SSS participant (elected primary validator), in administering the client's securities positions, might be considered as providing a securities account to its client, if the applicable national law so provides.
2. Each validator can receive update requests (i.e. settlement instructions) randomly from any client, without a specific allocation of responsibilities among validators. Availability of the DLT network would be maximised since failure of a specific validating node would not affect any user's ability to request ledger updates. As mentioned above, there is a contractual relationship between each SSS participant (the randomly picked validator) and the SSS operator. However, in that scenario, there is no contractual relationship between a client and specific validators. The latter could be acting solely on behalf of the operator providing the DLT infrastructure (i.e. the single entity or consortium CSD setting the protocol and providing access to the network), and the provider of such an infrastructure could be considered as being the actual account provider, as opposed to a validator.

Validation by end investors

Another option is a fully open model where a CSD provides the infrastructure and end investors validate ledger updates. Such a scenario is likely to materialise where there is no delegation of core responsibilities (see e.g. Chapter 5 on the subject of settlement finality), and where the CSD rules recognise end investors as validators, i.e. in the case of "direct holding" or transparent CSDs. Insofar as the CSD is the only financial institution involved, the CSD may be considered the provider and administrator of securities accounts in the functional sense. The existence of an account in the legal sense would nevertheless depend on the national legal framework that applies to the system.

[23] Ibid.

2.2.4 DLT-enabled processes

Leaving aside potentially applicable regulatory considerations, the following scenarios could materialise.

- An issuer issues securities directly into a distributed ledger, subject to possible national or European regulatory restrictions.
- Access to the ledger and validation of its content are distributed among a limited and authorised or unlimited number of nodes. This corresponds respectively to restricted or unrestricted distributed ledgers.
- Investors first receive securities from the issuer or from an issuer agent by means of distributed ledger updates.
- The investors qualify as shareholders when the securities of the issuer in the DLT are transferred to the shareholders in the distributed ledger system.
- The positions in the distributed ledger could legally qualify as “shares” or “bonds” or any other type of security that the issuer issued, depending on applicable law.

Whether this is a desirable option is not discussed. It should be noted that DLT also poses the following challenges:

- for payments in fiat currency outside a DLT, the link must be made between the securities delivery instruction entered into the distributed ledger and the cash payment that needs to be irrevocably instructed and executed (see also Chapter 4);
- collateral that is provided without title transfer, i.e. pledge or other form of security financial collateral as defined in the FCD, needs to be enforceable in a distributed ledger.

Although it is technologically feasible for a CSD operating a DLT network to meet the regulatory requirement to offer the option of omnibus client segregation or individual client segregation under CSDR, responsibility for the account structures built out of transactions on a sidechain needs to be assessed in relation to who operates the sidechains (CSD or direct participants) and whether or not sidechain participants are also CSD participants.

2.2.5 Challenges and opportunities

Should DLTs be used widely in financial markets, market efficiency might improve, but a number of challenges would arise. In particular, it is to be ascertained how DLT operators could meet regulatory requirements such as CSDR and SFD, or custody and safekeeping obligations, depending on the DLT model to be adopted.

DLTs also pose the following additional challenges.

- For payments in fiat currency outside a DLT network used for securities settlement, the link must be made between the securities delivery instruction entered into the distributed ledger and the cash payment that

needs to be irrevocably instructed and executed. Interoperability between systems and the provision of safe delivery-versus-payment settlement would be crucial in this respect.

- As regards the provision of collateral, the actual implementation of the DLT network should determine whether a position in a distributed ledger constitutes full title or another form of entitlement. In addition, these positions in the DLT network would need to be recognised as collateral under the applicable law.

3 Issuance of securities

3.1 Introduction

This chapter sets out to address questions such as what role DLT networks could play in issuance processes across the EU, and whether current EU regulations, domestic legislation and current business practices would allow them to play these roles.

3.1.1 Regulatory environment

The issuance process can be defined as a combination of both legal and operational arrangements that enables issuers to create its own securities – usually to satisfy own funding needs – and make them available for securities holders.

Many legal arrangements related to the process of equity issuance pertain to, and are governed by, the company law (lex societatis) applicable to the issuer.[24] This applies to the steps an issuer needs to perform to ensure that the issuance process is valid, as well as to the definition of issuers' and securities holders' respective rights and obligations. These aspects are not harmonised at EU level.

Nevertheless, from an operational standpoint at least, the issuance of securities has assumed a high degree of automation thanks to the representation of securities in book entry form. Book entry securities are legally defined by Article 2(9)(ii) of the Insolvency Regulation[25] as "financial instruments, the title to which is evidenced by entries in a register or account maintained by or on behalf of an intermediary".[26]

Under Article 3(1) of the CSDR, issuers of transferable securities which are admitted to trading or traded on trading venues shall arrange for such securities to be represented in book entry form, either as a direct issuance in dematerialised form or as a subsequent immobilisation.[27]

In this regard, it is worth noting that the European regulation has harmonised neither the process for immobilisation/dematerialisation nor the legal effect of the resulting

[24] The company law applicable to the issuer may not be the only relevant one. Certain aspects of debt issuance may be governed by the law chosen by the issuer (lex contractus). See also Article 49(1) of the CSDR, which requires Member States to communicate to ESMA the provisions of the corporate or similar law of the Member State under which the securities are constituted that apply to cross-border issuance.

[25] Regulation (EU) 2015/848 of the European Parliament and of the Council of 20 May 2015 on insolvency proceedings (OJ L 141, 5.6.2015, pp. 19–72).

[26] This definition is limited in scope to the Insolvency Regulation, but it can be used from a functional point of view in lack the absence of a more general EU-wide definition.

[27] This requirement applies from January 2023 for new securities and from January 2025 for all transferable securities. Under Article 2(1)(4) of the CSDR, "'dematerialised form' means the fact that financial instruments exist only as book entry records". Under Article 2(1)(3) of the CSDR, immobilisation is defined as "the act of concentrating the location of physical securities in a CSD in a way that enables subsequent transfer to be made by book entry".

book entries, which may vary from country to country. Typically, the law applicable to the credit of the securities to the securities accounts is the law of the country where the book of account or the securities account is maintained, although other conflict of law rules may be adopted.

Further to mandatory representation in book entry form, Article 3(2) of the CSDR requires that issuance of transferable securities transacted on a trading venue be recorded in a CSD on or before the intended settlement date. Recording of the issuance in a CSD ensures that transactions in those securities can be settled in an securities settlement system; it also allows the CSD to safeguard the integrity of the issue by comparing the records it maintains of the issuance both with the securities account balances held at the CSD by participants/investors and with the breakdown of intraday transfers performed through the settlement system (reconciliation procedure); finally, recording of the issuance in a CSD on or before the intended settlement date ensures smooth transition from primary to secondary market, mitigating delays in the settlement of secondary market transactions caused by the steps involved in the issuance process.

3.1.2 Overview of the standard issuance process

The following overview describes the market practice for the recording of issuance of securities in a CSD. For securities traded on trading venues, issuance and recording in a CSD are mandated by EU regulation. Further obligations or options are driven by domestic regulation. Peculiarities in this area are driven by domestic regimes for issuance process and the operating models of different entities involved in the process.

Step 1: set-up of relevant data related to the issuer and securities in securities database

The operational process whereby a security is made eligible within an issuer CSD includes the introduction of the new security in the securities database of the CSD. The database should include the following mandatory information: International Securities Identification Number (ISIN) of the financial instrument;[28] Legal Entity Identifier (LEI) of the issuer;[29] other securities reference data that are required for validation of settlement instructions, reporting and securities lending (either optional or mandatory according to CSD rules) such as: short name, long name, classification of financial instrument, country of issuance, currency denomination, issue date, final maturity date (where applicable), settlement type (e.g. face amount or units), minimum settlement (where applicable) and settlement multiple (where applicable).

[28] ISINs are the internationally recognised codes that uniquely identify a particular security. They are issued in accordance with the international standard ISO 6166.

[29] The LEI is a 20-character reference code to uniquely identify legally distinct entities that engage in financial transactions and associated reference data.

Step 2: set-up of issuance account or equivalent accounting mechanism

The recording of the issuance in book entry form is usually performed through the use of an issuance account, which introduces the securities into the intermediated holding chain. The issuance is represented by the debit balance of the issuance account that records the exact number and amount of securities issued and made available in the settlement system.[30]

The balance of issuance could be updated as result of a corporate action that increases or decreases the amount or the number of securities of the issue (e.g. capital increase/reduction, bonus issue, redemption, merger, stock split, etc.) through processes called mark-up and mark-down. Settlement of transactions in securities is generally not allowed on the issuance account, except for some primary market transactions under certain operational models.

Settlement of a securities transaction happens on investor or participant accounts where the CSD records the amounts of securities held by different investors and transferred by means of credit/debit records on the relevant accounts. As mentioned in the previous chapter, the issuance account is instrumental to the ongoing maintenance of the integrity of the issue, which is checked by the CSD acting in an "issuer CSD" capacity in this context through a periodic reconciliation procedure ensuring that the number of securities debited on the issuance account is always equal to the number of securities booked on investor/participant securities accounts.

According to the relevant domestic framework or the type of financial instruments, reconciliation procedures may involve other entities such as registrars, transfer agents or common depositories.

Step 3: crediting of securities issued on investors/participant accounts

There are two different operational models to complete the issuance process by crediting securities on securities accounts of the investors.

In the first model, securities are debited directly on the issuance account and credited on the account of the participant. The corresponding cash movements to the issuer (if any) are settled on a DvP basis by using a cash account associated with the issuance securities account.

Under the second model, securities are transferred free of payment from the issuance account to a distribution account. From a functional perspective, a distribution account is the same as any other securities account held at the CSD, but it is used only for the subsequent DvP distribution of new issues of securities. In

[30] Issuers and/or issuer agents may elect to have a new account per issue of security, or use the same issuance account for multiple issues.

this case, settlement of primary market transactions takes place between the distribution securities account and the account of the participants.[31]

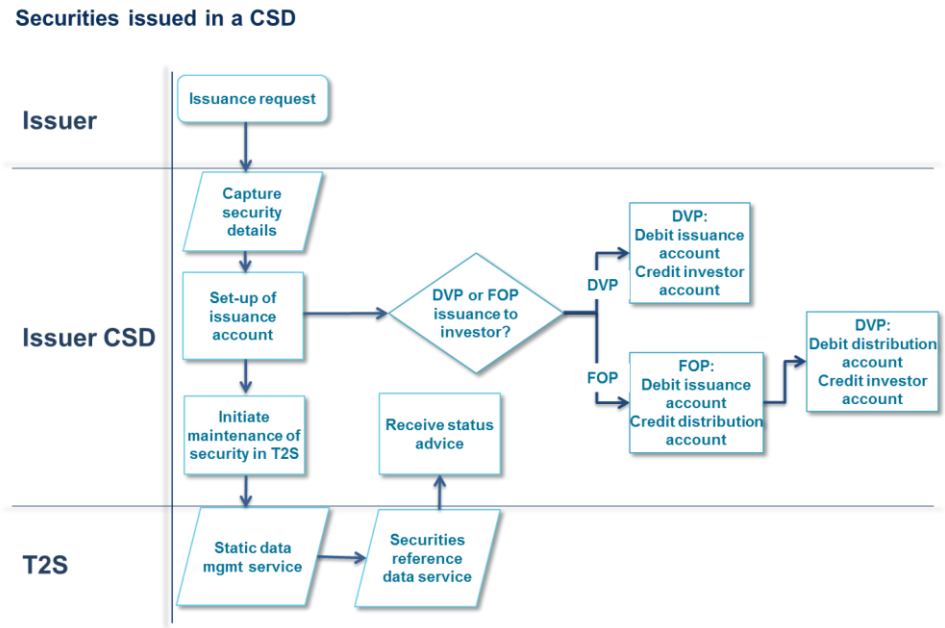
The CSDR requires the primary settlement to generate a corresponding receipt of settlement confirmation. In the current environment, it is possible for investor CSDs to credit participants' accounts prior to the actual receipt from the issuer CSDs.

If the issuer does not decide to be listed on a trading venue, issuance in book entry form is governed by the domestic legislative framework. In this context, national legislation usually requires that dematerialisation take place in the book of an authorised institution – typically a CSD. The analysis of the issuance process and of any possible DLT impact should then take national specificities into account.

For the purposes of comparison with subsequent DLT model suggestions in Section 3.2, Figure 1 provides a high level representation of the current issuance process for transferable securities:

Figure 1

Workflow of the issuance process



3.2 Impact of potential DLT adoption

Regarding the potential impact for securities issuance on distributed ledgers, it should be noted that the notary function and reconciliation processes are essential to investor protection. These functions are provided by authorised CSDs in the case

[31] This second model is sometimes used, where the issuer has appointed an intermediary (lead manager) to coordinate the placement of securities, to open the distribution account in the name of the lead manager or underwriter.

of securities traded on trading venues, but it would be possible for authorised entities to use DLT technology to perform the notary function in accordance with the law applicable to each specific asset class in the relevant jurisdiction. As noted above, the issuance is usually represented by the debit balance of the issuance account that records the exact number and amount of securities issued and that will be available in the settlement system. If issuance and its primary settlement are considered separately, a DLT solution can be used to record the number and amount of securities issued, with smart contracts programmed to implement the business logic and update the issuance, e.g. in the case of corporate actions.

Record-keeping of securities holdings on a distributed ledger raises a number of questions, in particular on the legal enforceability and status of records on the ledger. Since any DLT is a set of database management and transaction processing tools rather than an arrangement per se, the answers to these questions are likely to depend on how DLTs are used and by whom. In unrestricted DLT networks, unidentified nodes are collectively responsible for ordering and validating transactions. No legal entity bears responsibility for reconciling individual holdings with the number for the total amount of the issue, or for managing any potential discrepancies with a view to protecting investors. This potential shortcoming can be overcome in a restricted DLT network with issuer CSDs providing the notary and registration functions and remaining responsible and liable for their provision.[32]

Restricted ledgers, to the extent that they operate with admission requirements and conduct rules, could either be complementary to the central governance and monitoring performed by financial market infrastructures, or could possibly allow changes in the organisation of markets and their processes, subject to the applicable national law.

3.3 Impact on current processes

STEP 1: set-up of a security

DLTs do not remove the requirement for messaging, which needs to be as standardised as ever in order to allow communication among automated procedures such as smart contracts.[33] ISO 20022 would seem to be the logical standard to apply to DLT development as it allows open participation from the user community (key for DLT) along with rigorous procedures to ensure that changes are justified from a business point of view and that the frequency of releases can also be justified (governance of updates is a key discussion point for DLT networks).[34] On

[32] Record-keeping and validation methods provided via a DLT arrangement should be assessed against acquisition and disposition rules applicable in the relevant jurisdiction in which the DLT arrangement chooses to locate itself.

[33] Smart contracts must, by nature, also interact with external data, so further governance and standards on deployment of smart contract oracles in DLT would be required.

[34] Set-up of a security in the T2S platform must comply with ISO 20022 standards.

top of the current ISO 20022 concepts or business definitions such as currency codes, country codes and definition of a payment, new concepts may need to be defined.

T2S requires various securities-related static data set-ups, including a minimum settlement unit (MSU) value which defines the minimum quantity or nominal of a security for settlement.[35] DLT-based solutions may bring benefits if they offer flexibility to change static data such as the MSU.

ISO definitions could be extended to include DLT-specific concepts, possibly leveraging Technical Committee 68, which has the revision mechanism and standard business justification documents for proposing such changes. In addition, there are some ISO 20022 concepts or business definitions which it would make no sense to replace when defining concepts in a DLT environment, namely currency codes, country codes, definition of a payment, and common reference data. The use of ISO 20022 to develop DLT standards therefore seems appropriate.

Records in a distributed ledger are based on cryptographically hashed sequences of characters. Therefore, a digital asset recorded on a distributed ledger would have a new requirement for a cryptographic hash that is not part of current T2S securities set-up. Embedding the current required reference data into a digital asset is possible under the practice of assigning specific tokens exchanged in the DLT network with specific embedded reference data.

Should a CSD operate a DLT network, it is for the applicable national company law to determine whether the digitisation of securities within the DLT network is possible. In particular, it will be crucial to determine the legal nature of the digitised assets, i.e. whether they legally qualify as securities or not.

The function of ensuring that securities are brought into existence in line with issuers' requirements does not need to take place in the distributed ledger. It is an off-ledger control function that allows the bookkeeper to capture the relevant securities data, which need to be recorded in the distributed ledger as a subsequent step. Therefore, there are no practical impediments to this requirement being met in a DLT environment with regard to the introduction of an issue in the holding chain.

The requirement to capture issuance details from the issuer can be fulfilled independently of an issue being introduced into the holding chain.

[35] Most T2S CSDs have set the MSU to 1, although one CSD has set the value to 0.001, ensuring that securities transformations can be settled without creating residual amounts that would have to be claimed bilaterally amongst participants. Each investor CSD applies the MSU set by the issuer CSD across T2S markets, thus leading to different approaches even within single CSDs.

STEP 2: Set-up of issuance account or equivalent accounting mechanism

Scenario 1: tradeable securities[36]

Under current EU regulation, tradeable securities must be recorded in a CSD. Therefore, a DLT network would need to be restricted and have a tiered structure allowing the CSD to perform its functions, including ensuring the integrity of the issue. That could happen by means of a standard reconciliation of the issuance account balance with intermediaries' account balances or, given the single-entry nature of distributed ledgers, directly in the records associated with the beneficiaries of the primary market transaction.[37]

The maintenance of a bookkeeping system outside the distributed ledger to record the amount of securities related to a particular issuance does not present any obvious problems. Maintaining such a separate record that can be reconciled with the ledger could provide an additional layer of security of the DLT records against operational risk.[38]

The private key to modify the number of assets in circulation in the DLT network would need to remain under the control of the operator, e.g. the issuer CSD, and thus the T2S construct of issuer accounts remaining in the name of the issuer CSD could be maintained.

1a) Single issuer CSD

Any CSD could use a DLT internally by setting up a number of nodes to benefit from potential improvements in terms of cyber resilience and automation. The use of distributed ledgers as an alternative way to record securities holdings under extant business processes and regulation does not seem to raise specific concerns.

Another possibility is that a CSD allows its participants to run validation nodes able to find consensus on-ledger updates. This raises a number of caveats in terms of settlement irrevocability and finality, as well as externalisation of CSD core services that are addressed in other chapters of this report. Specifically, a CSD using a DLT internally allows the network of participants to record the settlement of securities transactions on the ledger to enhance the notary function.

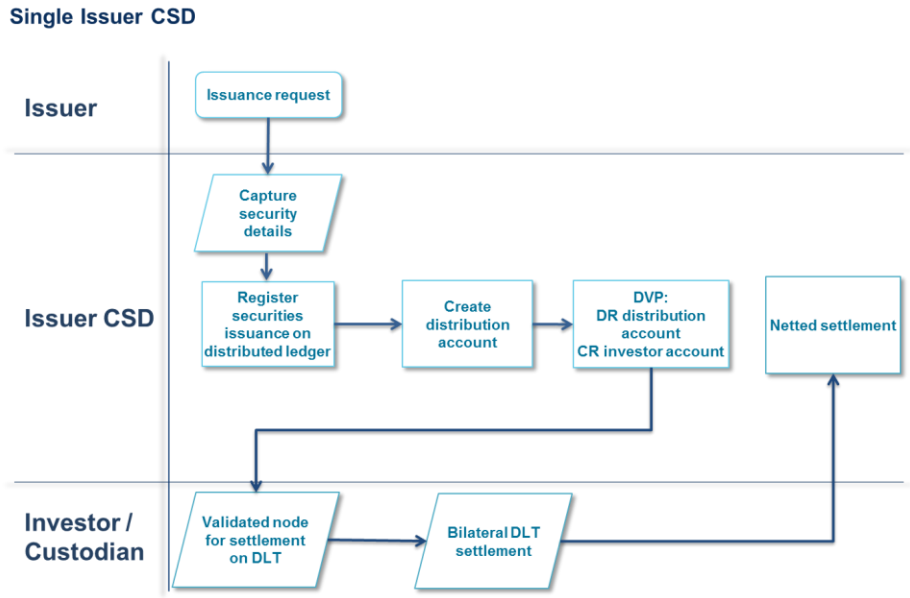
[36] The term "tradeable securities" is used throughout the note for transferable securities as defined in Article 4(1)(44) of MiFID II, which are admitted to trading or traded on a trading venue.

[37] It cannot be excluded that applicable law in some Member States may require the maintenance of a separate issuance account to substantiate the legal relationship between issuer or issuing agent and the issuer CSD.

[38] The set-up of issuance or distribution accounts is not necessary under DLT. Nevertheless, it would be possible to initially credit securities to the address of the issuer in the DLT network and then transfer them to the respective addresses of securities holders.

Figure 2

Single CSD issuing on distributed ledger



1b) Multiple-issuer CSDs

A DLT could be used by different CSDs in conjunction, to allow any specific issuance of securities to be split across multiple CSDs. Some form of restricted governance would be necessary and a common tender process could allocate the outcome of the primary transaction, on an issue whose static data is anyway maintained by a single security maintaining entity, across participating CSDs. Following the allocation of the securities amounts to the CSDs, the latter could validate the settlement of primary market transactions whereby the issuer receives the cash proceeds from the sale of the new securities and the CSDs receive the securities for further distribution down the holding chain.

Scenario 2: non-tradeable securities

2a) Non-tradeable securities issued via financial institutions other than CSD

For non-tradeable securities, EU regulation does not mandate the initial recording in the book of a CSD. The topic is a matter of company law, and issuance in book entry form is governed by the applicable national framework.

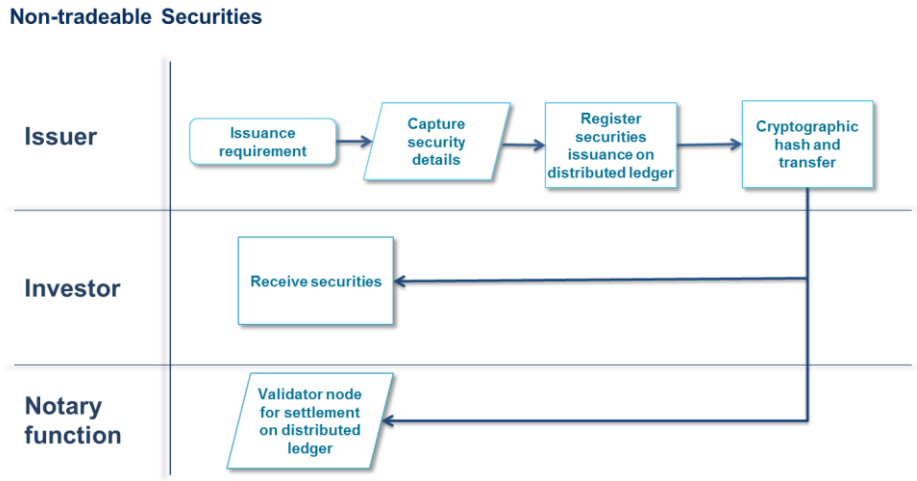
The analysis of DLT impacts should then be conducted country by country. Financial institutions other than CSDs can issue securities, also in a DLT arrangement, if that possibility is provided by the applicable national legislation. In this context, the analysis of DLT impacts on non-tradeable securities (including the issue of who should ensure the integrity of the issue) should take into account national specificities.

2b) Non-tradeable securities issued directly by the issuing entity

Notwithstanding the comments under 2a) above, there is a possibility that issuers may issue their own non-tradeable securities in a distributed ledger. Currently, the fact that various actors are required to facilitate issuance of securities means that there is a de facto minimum issuance size below which it is economically unviable to raise funds via securities issuance. If the auditability typical of a distributed ledger were to reduce the range of institutions involved in securities issuance and the associated costs, it could present an opportunity for small and medium-sized enterprises (SME) to raise financing. There would still be a requirement for an institution carrying out the notary function to act as a node on the DLT to maintain the integrity of the issuance, and there is work to be done from a legal perspective in determining the status of securities settlement in distributed ledgers. Direct issuance, at least for non-tradeable securities, can be a possibility a least in some specific jurisdictions.

Figure 3

Issuance on distributed ledger for non-tradeable securities



STEP 3: crediting of securities issued on investors/participant accounts

While the initial credit of securities to the address of the issuer for further transfer to participants may be preferable, the set-up of issuance or distribution accounts is not strictly necessary under DLT. Securities issued in a DLT environment could equally be credited directly to investor/participant accounts, assuming that the maintenance of a record of the amount of securities related to a particular issuance exists to satisfy notary function requirements. This is at odds with the current practice and regulatory framework, which involve the initial recording of a securities issue in an issuer CSD.

3.3.2 DLT-enabled processes

Double-entry vs. single-entry accounting

Some distributed ledgers do not use double-entry bookkeeping but single-entry bookkeeping with cryptographic linkages. This calls into question the role of an issuance or distribution account. A parallel can be drawn between records of asset holdings in a DLT environment based on UXTOs and containers (accounts) of physical objects (assets): once a pre-specified number of physical objects is introduced in the first container (assets in the issuance account), these objects can be moved to all connected containers (i.e. to investor accounts) and nothing is left in the first one.

Notary checks on the correspondence between the issued amount of securities in the issuance account and the total amount of securities credited to investor accounts are substituted in DLT applications by the cryptographic guarantee that no security can be added to or subtracted from the system. Proper cryptography should ensure that the pipes (transaction messages) connecting the different containers (accounts) do not allow anything to get in or out of the network after its content has been determined by the operator.

The correct performance of such an automated notary function can be verified by any participant (in public DLTs) or at least by validators, endorsers or orderers (in private DLTs) at any time and, ideally, the operator of the network should be able to amend any unwarranted mistakes, similarly to what happens in current reconciliation processes. Governance is therefore of key importance to ensure proper handling of operational risk.

Digital financial assets (native) vs. DLT representation (tokens)

In all cases of issuance on the ledger, the legal nature of tokens as well as the rights and obligations associated with their use are uncertain and depend largely on the applicable national legal framework. Where tokens represent real-world securities, it needs to be determined whether there is a correspondence between a) the token and the real-world securities, and b) the rights represented by the token and the rights in the real-world securities. In the case of native digital assets, it is debatable whether the digital assets could be legally recognised as “securities”. Given the regulatory constraints related to issuance of securities, issuance on the ledger can only be operable if the local law recognises that the assets recorded on the ledger qualify as “securities”, “moveable securities”, “shares”, “bonds”, etc., and that credits/debits on the distributed ledger can evidence rights in such assets. The possibility to issue, on a distributed ledger, representations of securities already recorded elsewhere, is equally a matter of national applicable law. Lack of harmonisation with regard to immobilisation of securities in T2S markets means that there are questions over the feasibility of a pan-European issuance process via DLT regarding the place of issue and the law under which the issue would take place.

DLT for issuance (settlement out of scope)

An issuance service via DLT could be offered to the issuers without necessarily involving on the other side any direct business relationship with the CSDs' participants, i.e. intermediaries and investors.

3.3.3 Challenges and opportunities

Opportunities

In the case of DLT adoption for the issuance of securities compatible with applicable law:

- it is possible that DLTs would be used as "niche" solution for the issuance of specific products that currently takes place in an inefficient way;
- transfer instructions and enrichment to trade data would flow in near-real time.

Challenges

- ISO 20022 is required to connect any DLT-based system to the T2S platform (total of 130 message types). DLT currently encompasses a variety of technical approaches which would make standardisation difficult and could therefore represent a regression from ISO 20022 in terms of messaging harmonisation.
- The long road that leads to ISO 20022 implementation reflects the challenge and transition period required for new standards.
- Real-time and transparent reconciliation procedures are necessary to ensure the integrity of the issue if holdings of a security are held both in a distributed ledger and in more traditional recordkeeping systems.
- National applicable law is of primary importance to determine whether a DLT network can be used for securities issuance.
- A situation where, over the lifecycle, financial instruments are trapped in traditional silos would need to be avoided.

4 DvP and availability of cash on distributed ledgers

4.1 Introduction

The objective of this chapter is to provide an overview of different solutions for DvP in distributed ledgers and their potential impact on market integration. To be successful, the adoption of DLTs in post-trading arrangements will require for instance that principal risk and replacement cost risk, both associated with the failure of a counterparty to meet its obligations, are effectively mitigated. At the minimum, a form of DvP will then be required to make DLT adoption possible. Securities post-trade arrangements on distributed ledgers will therefore require the ability to offset obligations with cash, and the safety and efficiency with which this can be achieved depends on the specific DvP model used. While there are conceptually a variety of possible approaches for introducing cash into DLT systems, the options presented in this paper in the realm of central bank money are at the sole discretion of central banks, and this paper does not advocate any particular solution.

4.1.1 Delivery versus payment

DvP settlement links a transfer of securities with a transfer of cash in a way that the delivery of securities occurs if and only if the corresponding transfer of cash occurs and vice-versa. This is generally seen as an effective method of addressing principal risk, as it avoids a situation where participants in a securities transaction transfer the asset they committed to a trade (securities or cash) before the asset they expect to receive (cash or securities) is guaranteed to be transferred in the opposite direction.

In April 2012, the Committee on Payments and Market Infrastructures (CPMI – previously known as the Committee on Payment and Settlement Systems (CPSS)) and the Technical Committee of the International Organization of Securities Commissions (IOSCO Technical Committee) published the “Principles for financial market infrastructures” (CPMI-IOSCO, 2012). This document suggests the use of DvP settlement, stating that “if [an FMI] settles transactions that involve the settlement of two linked obligations (for example, securities […]), it should eliminate principal risk by conditioning the final settlement of one obligation upon the final settlement of the other” (Principle 12).

Under Article 39(7) of the CSDR, “all securities transactions against cash between direct participants in a securities settlement system operated by a CSD and settled in that securities settlement system shall be settled on a DvP basis”.

Even beyond the above-mentioned regulatory requirements, which are applicable to the case of CSDs, market participants would be likely to require a form of DvP in order to accept the use of a DLT in any form of settlement of securities transactions.

DvP models currently used by securities settlement systems create a trade-off between some form of credit extension and prefunding requirements. It is important to note that DvP can be achieved even when the cash leg and the securities leg of a transaction are not processed simultaneously and the cash leg is instead netted into a single position and settled at the end of the settlement cycle.[39] Whereas the concept of a settlement cycle used to be associated with the end-of-day principle, technological innovation has made it possible to mitigate settlement risk in the case of netting by allowing intraday settlement at any chosen time interval.

4.1.2 Central bank money and commercial bank money

DvP alone is not sufficient to eliminate all types of risk. Although DvP settlement discharges counterparties from their contractual obligations, the cash leg can indeed be settled by means of two different types of money:

1) central bank money (CeBM) is a claim on the central bank issuing the currency in which the payment is denominated;
2) commercial bank money (CoBM) is a claim on any other institution.

Post-trade markets are used to adopt models based on CeBM or CoBM depending on various factors – e.g. the need for multi-currency transactions and the location or time zone of trading participants. Although a payment in CoBM discharges its payer from legal obligations as soon as it is final, only payments in CeBM liberate the securities seller from the risk of default by the institution that is managing the payment and is holding the cash even after settlement has taken place. The PFMIs suggest that CeBM should be used in settlement "where practical and available" (Principle 9).

The European Central Bank (ECB) has implemented the principles for financial market infrastructures (PFMIs) in payment systems by means of a regulation. This has direct relevance for securities transactions since payment systems are typically used for the settlement of the cash leg. Article 10 of the SIPS Regulation[40] states that:

"1. A SIPS operator settling one-sided payments in euro shall ensure that final settlement takes place in central bank money.

[39] For a detailed description of different DvP models (i.e. gross-gross, gross-net and net-net), please refer to the report produced by the Bank of International Settlements, *Delivery versus payment in securities settlement systems*, 1992 (http://www.bis.org/cpmi/publ/d06.pdf).

[40] Regulation of the European Central Bank (EU) No 795/2014 of 3 July 2014 on oversight requirements for systemically important payment systems (ECB/2014/28) (OJ L 217, 23.7.2014, pp. 16-30).

2. A SIPS operator settling two-sided payments or one-sided payments in currencies other than euro shall ensure that final settlement takes place in central bank money where practicable and available.

3. If central bank money is not used, a SIPS operator shall ensure that money settlements take place using a settlement asset with little or no credit and liquidity risk.

4. If a settlement takes place in commercial bank money, the SIPS operator shall monitor, manage, and limit credit and liquidity risks arising from the commercial settlement banks. […].

5. If a SIPS operator conducts money settlements on its own books, it shall minimise and strictly control its credit and liquidity risks.

6. If a settlement takes place in commercial bank money, a SIPS operator's legal agreements with any commercial settlement banks shall state clearly:

(a) when transfers on the books of individual settlement banks are expected to occur;

(b) that transfers are to be final when effected;

(c) that funds received shall be tradeable as soon as possible, at least by the end of the day."

Under Article 40(1) of the CSDR "a CSD shall settle, whenever practical and available, the cash leg of the securities transaction through accounts opened with a central bank". Otherwise, when this option is not practical and available, under Recital 44 of the CSDR "a CSD should be able to settle through accounts opened with a credit institution established under the conditions provided […] and subject to a specific authorisation procedure and prudential requirements […]".

For the settlement of securities transactions in CeBM, models used by central banks can be divided into three main categories.

1) Under the "interfaced" model, a communication protocol allows securities settlement at the CSD and cash settlement in the CeBM payment system to be linked (traditional DvP model).
2) Under the "integrated" model, the CSD can operate its participants' dedicated cash accounts, which remain part of the CeBM payment system only from a legal point of view.
3) T2S has a unique way of providing DvP in CeBM, namely by using the "reverse integrated" model. In T2S, CSDs outsource the management of their securities accounts to the central bank – instead of central banks outsourcing the management of their cash accounts to the CSDs. Although the T2S platform is operated by the Eurosystem, the respective securities accounts remain legally attributed to each participating CSD.

4.2 Impact of potential DLT adoption

4.2.1 Impact on current processes

Delivery versus payment

DvP in a DLT environment is straightforward when the securities leg and the cash leg are settled in the same ledger and are governed by the same DLT protocol, or when settlement in two different ledgers can be linked by means of automatic escrow services.[41] DLTs can typically ensure DvP by keeping a leg of the transaction pending (i.e. earmarked) until the other leg is ready for settlement.

Different DvP models can therefore be implemented, either by means of stored procedures executed outside the distributed ledger or by eliciting the execution of smart contracts that are encoded in the ledger and are programmed to settle transactions – either gross or otherwise netted at pre-arranged intervals. Synchronisation of the business hours of all systems involved – both DLT-based and non-DLT-based – is of key importance. This means time zones need to be catered for, given that current post-trade systems do not work on a 24/7/365 basis (see Chapter 7 on settlement schedules).

Use of central bank money

DLT solutions in securities post-trading will have to prove able to mirror the efficiency of CeBM payment legs in securities transactions currently processed by the Eurosystem infrastructures, since the range of functionalities provided by the current solutions – e.g. service levels and liquidity saving mechanisms such as autocollateralisation – have been developed to meet the requirements expressed by their prospective users. Whereas the joint management of the current Eurosystem infrastructures by central banks in the euro area ensures that integration would be unaffected by any technological change, considerable efforts would probably be needed to ensure that technological innovation in the global dimension can be beneficial.

If a DLT solution were to be adopted for the bookkeeping of securities, the advantages that DvP settlement in CeBM brings in terms of risk mitigation might justify also reflections over making CeBM available on a distributed ledger. This could be useful if it is assumed that no interfacing between the DLT securities settlement system and current non-DLT CeBM payment systems will be able to yield the same safety and efficiency gains.

[41] An escrow service allows a transfer commitment to be made (or a token to be immobilised) in a distributed ledger until another transaction (or token transaction) takes place in another compatible ledger, such as a sidechain.

Some solutions are under development to interface DLT and non-DLT technologies, with a view to allowing DvP settlement to take place on ledgers operated with different technologies. However, the operational risk implications of such interfacing have yet to be ascertained and might favour the implementation of a unified approach where the same technology is used for the settlement of both legs. Very little evidence has been brought to bear on this point to date, but market participants are actively engaged in assessing the possibility.

Access to the system

Rules governing access to a settlement system matter greatly for its safety and efficiency. The adoption of unrestricted DLT systems which allow any unknown party to become a user of the distributed ledger appears unlikely in financial markets for tradeable securities. This assessment is based not only on the issue of users' accountability – know-your-customer (KYC) and anti-money laundering (AML) provisions – but also on the impact of open access on the performance of consensus processes used in the ledger. Unrestricted DLT networks require the adoption of less efficient validation processes, whereas the organisation of financial markets suggests that the rule of law might be sufficient to enforce truthful behaviour.

In any country or currency area, access to CeBM accounts is limited to specific sets of institutions – mainly licensed banks and some ancillary settlement systems.[42] Any weakening of such eligibility rules would have the potential to crowd out commercial banks from deposit-taking, with effects on lending capacity in the economy and on the conduct of monetary policy, along with wider risk implications, all of which would need to be assessed.[43]

4.2.2 DLT-enabled processes

The following stylised models can be used as starting point for reflections on the use of money denominated in legal currencies (i.e. not virtual currencies) on a distributed ledger.

Commercial bank money

If the cash exchanged in a DLT network were not CeBM, it is likely that market participants would want to convert such cash into CeBM at intervals. This would require institutions with CeBM accounts to mirror movements of cash in DLT and in

[42] See Articles 2 and 4 of Annex II to the Guideline of the European Central Bank of 5 December 2012 on a Trans-European Automated Real-time Gross settlement Express Transfer system (TARGET2) (recast) (OJ L 30, 30.1.2013, p. 1).

[43] See Speech by Yves Mersch, *Digital Base Money: an assessment from the ECB's perspective*, 2017, available at https://www.ecb.europa.eu/press/key/date/2017/html/sp170116.en.html

the central bank account under their responsibility. Conceptually, this could work as follows (and as also illustrated in Figure 4).

- As the first step, DLT participants with access to CeBM accounts would create cash holdings on the distributed ledger by confirming the availability of cash to the DLT system. This could be achieved for example by sending a credit confirmation (MT103, MT202 or the ISO20022 equivalent, e.g. pacs.008 or pacs.009 in future) from a dedicated RTGS account to the DLT application programming interface (API).
- A movement of CoBM on the distributed ledger would be settled in CeBM only when the buyer of the security transfers the corresponding cash value via RTGS to the seller also holding an RTGS account, possibly at the end of a settlement cycle. The securities seller would withdraw the cash from the ledger as soon as the same amount was received on its RTGS account. Debit confirmations (MT012) would be used by the DLT to determine central bank cash held by a certain participant.

Settlement in the DLT network would not be DvP settlement in central bank money without formal agreement from the central bank in question to support such a model (e.g. in the form of guaranteeing the fulfilment). The reason is that without the central bank guarantee there is a risk that the buyer of securities would not transfer the CeBM in line with the DLT transaction. Private market participants could mitigate this delivery risk by ensuring that the DLT transaction remained pending until the RTGS movement had been completed. However, this would leave a residual counterparty risk for the buyer if, having moved cash on RTGS, the seller then failed to complete the pending DLT transaction.

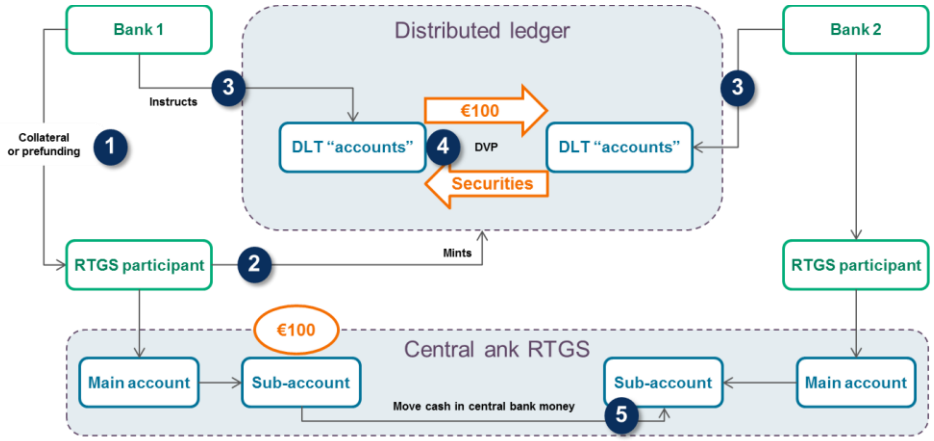
At least two cases might emerge, which are as follows.

- Cash backed by individual DLT participants (CoBM)

Each participant in a DLT network might decide to issue its own representation of cash (loosely called “coins” for the purposes of the two cases described) in the ledger by means of its private key. The issuer could promise convertibility of each coin into a predetermined amount of currency outside the ledger (e.g. at parity, where one coin = €1) but the value associated with each bank’s coin could be impacted if there were concerns over the perceived ability of the individual issuer to convert its liabilities either into coins of another DLT participant/commercial bank or into CeBM upon demand. In the absence of a credit concern, the coin would be treated as a fungible asset in a DLT system, and trading participants would hold coins issued by another bank and use them as settlement assets to offset their own obligations. In such an arrangement, the DLT network would be fully reliant on each issuer to honour its obligations and would not verify whether a segregated holding of CeBM (or CoBM) existed to create the coin.

Figure 4

Coin backed by commercial banks (CoBM)

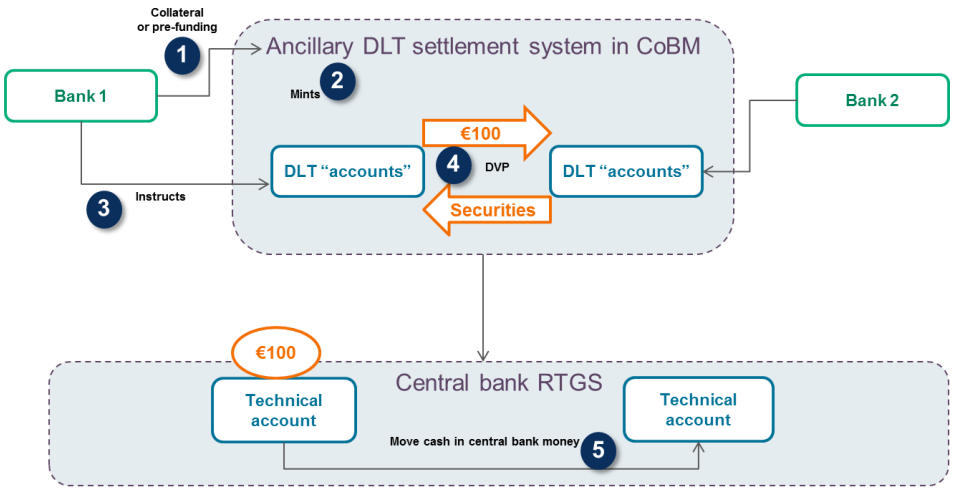


- Coin backed by a private settlement institution (CoBM)

A more sophisticated approach than the one described above would require settlement coins to be issued by the operator of a DLT settlement system in proportion to either an amount of cash for the purposes of prefunding, or collateral posted via standard settlement systems outside the ledger. The coin would still be a form of CoBM and its corresponding real value could theoretically fluctuate with the perceived solvency of the settlement institution. However, differently from the model above, a settlement institution would be able to play the role of the notary and avoid the unwarranted inflation of coins in respect of the actual collateral or prefunding posted by participants.

Figure 5

Coin backed by ancillary settlement system (CoBM)



Central bank money

A true DvP model processing transactions on the DLT in CeBM on a gross basis can only be achieved if a central bank decides to ensure with its own assets the fulfilment of cash claims represented in the distributed ledger.

- Coin backed by a central bank holding the cash of DLT participants off-chain (CeBM)

  - Mirroring of coins transferred via DLT network and CeBM funds held either in the RTGS or in dedicated cash accounts: This solution would require interfacing the two IT systems, with a high degree of involvement by the central bank. Each transfer between two holders of central bank accounts in any of the two payment systems – either DLT or non-DLT – would require, once validated, an instantaneous equivalent update in the other system to achieve a DvP model settling all cash and securities transactions on a gross basis. Besides the possibility of operational issues able to affect the mirroring process, no DLT-specific risk would be borne by the central bank.

  - Prefunding of coins transferred via DLT network with CeBM held either in the RTGS or in dedicated cash accounts: The central bank would allow a DLT network to mint/redeem coins under the limit of funds held in its account with the central bank. Accounts in the distributed ledger would need to interact with those of the central bank only to update the prefunding. This would happen in response to pay-ins or pay-outs that DLT participants may require between their standard accounts with the central bank and the sub-accounts they hold in the central bank account of the DLT operator. Such a model entails the risk of losses for the issuer central bank that would need to fulfil its commitment even in the event of the failure of the private DLT network to prevent the minting of coins beyond prefunded amounts.

    A potential DvP model with cash settlement on a net basis could follow the Depositary Trust & Clearing Corporation (DTCC) model using the Federal Reserve Banks' National Settlement Service (NSS) to process end-of-day net funds as follows.

    - An entity would need to be designated as the system operator and would be responsible for adopting new participants (restricted ledger).

    - Each node would be responsible for the cash creation on the DLT by moving their own cash into a designated RTGS account that delivered electronic updates to the DLT system.

    - At the end of the business day, the DLT would have to calculate the net cash requirements for each node and send instructions against the

respective RTGS accounts.[44] Since RTGS accounts cannot have a negative balance, the total net amount would need to be limited in relation to available collateral and the central entity would need to guarantee the default of a provider.

- The DLT system could be considered an "ancillary system" under RTGS rules to access central bank money for the purpose of achieving DvP, which would allow it to instruct through a power of attorney concept.

- Direct use of DLTs by the central bank (CeBM)

  - Variant A – central bank acting as a participant with special rights in a private DLT network: The central bank would be able to use its private key to issue and redeem coins in the dedicated DLT cash accounts of DLT network participants upon request, and based on their prefunding or collateral held with the central bank. The same coins could then be redeemed by the central bank (e.g. in the case of a collateral margin call) or converted once again into the same amount of currency in the accounts held with the central bank. An important difference between this model and the model with prefunding is that, in this case, the central bank can directly change the amount of coins in circulation and does not outsource such a responsibility to the DLT operator.
  - Variant B – central bank as operator of the DLT system (possibly in conjunction with a platform for securities settlement): The central bank would develop its own DLT network and operate it by providing accounts to its participants, possibly also providing a platform for the interaction between coins accounts and the securities accounts held by securities settlement systems. However, it has been stated recently that "the ECB cannot, at this stage, consider basing [its] market infrastructure on a DLT solution."[45]

4.2.3 Challenges and opportunities

DvP settlement is currently used to limit risk in the post-trading of securities transactions. The same opportunity can be made available in a DLT environment, either by issuing cash in the same type of distributed ledger adopted by the relevant securities settlement system/internaliser or by allowing a seamless interaction between such a ledger and non-DLT payment system(s).

The provision of cash to be used for DvP settlement of securities transactions is an opportunity insofar as DLT adoption is considered to be an opportunity for the securities leg and the related asset servicing activities. This is conditional on the

[44] The concept of "business day" may be difficult to define in the case of a DLT that is in operation 24 hours a day.

[45] Speech by Yves Mersch, Member of the Executive Board of the ECB, 22nd Handelsblatt Annual Conference Banken-Technologie, 6 December 2016

realisation of potential benefits, which DLTs might be able to deliver only if the necessary harmonisation and interoperability among DLT solutions were achieved.

Besides the challenges related to adoption of DLT in general, there seems to be no specific challenge in relation to the use of DLT for the settlement of cash legs in particular. The necessity to represent cash directly in the ledger, as opposed to the possibility of interfacing a DLT with non-DLT systems, has yet to be ascertained.

Given the recognised importance of CeBM as a settlement asset that minimises risks relating to the cash leg of a securities transaction, the possibility of using CeBM in a DLT environment would be an opportunity under the currently strong assumption that all interested parties (market players and public authorities) will find the adoption of a DLT safe and efficient. However, it is not clear what type of CeBM model provides the best combination of safety and efficiency.

PART II – DLTS IN SETTLEMENT AND RELATED SERVICES

5 DLT and settlement finality for securities settlement

5.1 Introduction

This chapter discusses the main features of settlement finality, which is a fundamental feature for payment, clearing and settlement systems. Settlement finality provides legal certainty for rights and obligations processed in these systems through irrevocability and unconditionality of asset transfers. Its importance arises particularly through superseding insolvency laws in the event of participant's insolvency.

It is also important to highlight the distinction between "transfer of ownership" and "settlement finality". Specifically, even where the transfer of ownership is effectively recorded under the applicable securities law, such a transaction may be revoked on the basis of applicable (local) insolvency laws where the transaction is not protected by settlement finality legislation superseding the applicable insolvency law.

Settlement finality is regularly discussed in the DLT context. Often, the discussion is limited to the following:

- a Bitcoin-type DLT model which involves proof of work or other consensus models creating a problem of "probabilistic finality", where already processed transactions may be revoked as a consequence of replacing transactions retroactively;
- a part of the finality, i.e. irrevocability of a transaction (rather than securities settlement in the broadest sense).

5.1.1 General remarks about settlement finality

Where payment, clearing and settlement systems create a significant volume of settlements, this has the potential to create systemic risks, not only in the event of revocation of already processed transactions but also in the event that transfer orders entered into the system by a then insolvent participant cannot be settled. To mitigate these risks, the SFD has extended settlement finality protection so that, in addition to processed transactions, it also covers transfer orders. In practice, not only transactions settled prior to the insolvency of a participant are protected and enforceable under the SFD but also the transfer orders that were entered in the system prior to participant's insolvency, as long as such transfer orders can be settled after the participant's insolvency. This is to protect the other participants in the system so that they can rely on the fact that the transfer orders entered into the system are eligible for further settlement.

5.1.2 Legal framework of settlement finality in FMIs

The PFMIs issued by the CPMI and IOSCO (specifically Principle 8: Settlement finality) require FMIs to provide clear and certain final settlement, at a minimum by the end of the value date. Where necessary or preferable, an FMI should provide final settlement intraday or in real time.

The SFD requires the operator of an SFD-designated settlement system to define in its rules the following moments related to the aforementioned steps of the settlement process: the moment of entry of a transfer order into the system (Settlement finality I – SFI), i.e. the moment at which a transfer order becomes legally enforceable and, even in the event of insolvency proceedings against a participant, binding on third parties (Article 3(1) and (3) of the SFD); and the moment of the irrevocability of a transfer order (Settlement finality II – SFII), i.e. the moment at which a transfer order may not be revoked either by a participant in a system or by a third party (Article 5 of the SFD).

There is nothing in the SFD about the moment of the moment of irrevocability and enforceability of settlement (Settlement finality III – SFIII). However, under CSDR requirements, the settlement finality rules would necessarily apply to all tradeable securities. The same applies also to non-tradeable securities if the issuer decides to perform the initial recording in a CSD. The CSDR obliges CSDs to disclose their rules on SFIII. It is important to note that a potential outsourcing by a CSD should not have an adverse impact on the CSD's ability to fulfil its obligations under Article 30 of the CSDR, which requires for example that "outsourcing does not result in depriving the CSD of the systems and controls necessary to manage the risks it faces".

According to Article 48(8) of the CSDR, interoperable securities settlement systems and CSDs which use a common settlement infrastructure shall establish identical moments for SFI and SFII. In addition, these securities settlement systems and CSDs shall use equivalent rules concerning the moment of finality of transfers of securities and cash (SFIII).

As neither SFD nor CSDR set further constraints for the definition of the above moments, system operators have some scope for taking into account system functionalities when designing their settlement finality frameworks. In the context of T2S, for example, the definitions of SFI,[46] SFII[47] and SFIII[48] have been harmonised.

[46] CSDs using the T2S platform have agreed to an identical moment of entry of transfer orders into their respective systems (SFI). This is the moment when the validation process is positively performed according to the T2S validation criteria, i.e. when the transfer orders have been declared compliant with the technical rules of T2S.

[47] CSDs using the T2S platform have agreed to an identical moment of irrevocability of transfer orders into their respective systems (SFII). This is the moment when the transaction has been given the status "matched" on the T2S platform.

[48] CSDs using the T2S platform are bound to ensure the unconditionality, irrevocability and enforceability of the settlement processed on the T2S platform (SFIII – Article 21(4) of the T2S Framework Agreement).

As mentioned above, the importance of settlement finality arises particularly in the event of the participant's insolvency. Under the CSDR, the CSD that operates a securities settlement system:

- "shall ensure that the securities settlement system it operates offers adequate protection to participants" (Article 39(1));
- "shall have effective and clearly defined rules and procedures to manage the default of one or more of its participants ensuring that the CSD can take timely action to contain losses and liquidity pressure and continue to meet its obligations" (Article 41(1)).

A CSD needs to define and document sufficient processes to suspend an insolvent participant from entering new transfer orders in the system, as such transfer orders would not be protected by the settlement finality rules.[49] Participants need to know that they can rely on the fact that the transfer orders in the system are eligible for further processing, i.e. matching and final settlement. This is to avoid (systemic) risks created by potential revocation of transactions.

5.1.3 Scenario falling outside the scope of the EU settlement finality rules

The application of SFD is limited to the protection of securities transfer orders and settlement in an SFD-designated SSS. Accordingly, the current EU rules on settlement finality do not cover:

1. settlement involving some asset classes other than tradeable securities,[50] unless they are settled in a system designated under Article 2(a) of the SFD;
2. settlement of financial instruments taking place outside a system at the level of financial institutions acting as settlement internalisers (that is, further down the custody chain in a multi-tier holding model);
3. settlement of financial instruments taking place outside a system in the records on entities other than financial intermediaries, if allowed by national applicable law.

In such scenarios, the settlement finality rules under SFD and CSDR do not apply. Therefore, transfer orders or transactions could be revoked in the event of participant's insolvency, under the applicable insolvency laws, potentially exposing a system other than an SFD-designated system and its participants to systemic risk.

[49] The ESMA guidelines on participant default rules and procedures under Regulation (EU) No 909/2014 of the European Parliament and of the Council of 23 July 2014 on improving securities settlement in the European Union and on central securities depositories and amending Directives 98/26/EC and 2014/65/EU and Regulation (EU) No 236/2012 (OJ L 257 28.8.2014, pp. 1-72) specify a non-exhaustive list of actions a CSD may take in order to manage the default of a participant, and set minimal requirements in respect of the testing and review of such rules and procedures.

[50] More generally, the SFD does not cover any asset classes other than financial instruments under Section C of Annex I to MiFID II (please see point h) of article 2 of SFD.

5.2 Impact of potential DLT adoption

5.2.1 Impact on current processes

Under current EU law, and specifically according to Article 30 of the CSDR, outsourcing (i.e. running the system on various nodes) should not result in "depriving the CSD of […] systems and controls […]".

Indeed, securities settlement systems operated by CSDs involve CSDs being considered as responsible for the system. DLTs provide an opportunity for systems to be maintained on a decentralised basis through nodes maintained by multiple participants. Although nodes could be technically maintained for example by CSD participants, as long as the nodes formed part of the CSD system, the CSD would remain responsible for the system under the general principles applicable on outsourcing, as node maintenance could be considered as outsourcing. It is not relevant to make a distinction between different issuance scenarios on the basis of the technology used for the digitisation of asset holdings.

As stated above, settlement finality needs to be considered on each settlement system level separately. This would render irrelevant the distinction between, for instance, whether the assets were "digitised/tokenised" or "digital/native" assets. For example, it would not make any difference to the settlement finality from the investor CSD's point of view whether the issuer CSD was using a DLT-based settlement system or the current T2S platform. Settlement finality would need to be defined in a DLT-based settlement system as well.

Settlement finality regulations require SSSs to have the following features:

- a single moment defined for each transfer order and/or settlement transfer for each of SFI, II and III, which cannot be retroactively changed;
- ability to suspend participants' access to the settlement system to place new transfer orders;
- obligation for the settlement system to be governed by the same settlement finality rules so that, in the event of interoperable systems, SFI, II and III will be harmonised across the systems.

DLT-based settlement systems can be designed in multiple different ways and it is not feasible to discuss in a binary manner whether or not DLT can fulfil the regulatory requirements, e.g. for finality of securities settlement. Instead, the question is more how the system should be designed to accommodate the applicable requirements, namely:

  - a fully decentralised DLT system without a central authority;
  - a system where the processing of new transactions is to some extent centralised and performed by a central authority which certifies ledger updates previously validated by participants;
  - a blockchain-based database maintained centrally (i.e. both processing and data maintenance) which is not a truly "distributed" ledger.

5.2.2 DLT-enabled processes

1. Moment of entry of the transfer order to the system (SFI)

Decentralisation of the DLT-based system may raise challenges regarding the definition of moment SFI. While in a centrally maintained settlement system the moment of entry for transfer orders is obvious, in a system maintained on a decentralised basis there are various options depending on the system set-up.

DLT-based systems can allow technically for decentralisation of transaction validation, which includes ensuring that the transaction has been signed with the appropriate private key prior to its inclusion. As the SFD does not define the relevant SFI moment (that being a matter for the rules of the relevant system), and as the SFD requirements are technology agnostic, in principle SFI can be freely defined in the rules governing the system provided that each transfer order has one single moment of entry.

A major challenge related to the decentralised nature of a DLT-based system is a potential situation where an action taken in one node is not accessible to the operator of the system (as a central authority) or to its participants. Such a situation could occur in the event that the data connection between the nodes is interrupted. This could create a situation where a transfer order would be acknowledged by one node but its existence would not be known by the others.

The above situation creates an issue for settlement finality in a scenario where transfer orders are entered into the system after the moment of opening of insolvency proceedings, because the moment a CSD (as operator of the system) is aware of the participant's insolvency, the insolvent participant needs to be suspended by the CSD from entering new transfer orders into the system.

2. Moment of irrevocability of transfer orders (SFII)

Decentralisation could also involve specific considerations on irrevocability of transfer orders, as the system rules need to include a definition of the moment when the transfer orders become irrevocable. SFII defines the moment when an obligation to settle a transaction cannot be unilaterally withdrawn from the system by a party to that transaction. This is up to the rules of the system but it is often the moment of transaction matching, which normally takes place automatically after the participants have entered into the system both sides of transfer orders including the necessary matching criteria. As DLT adoption provides potential for decentralising the settlement system into several nodes, matching could take place in any of the nodes. A DLT-based securities settlement system would therefore need to be designed in a manner that ensures for each pair of transfer orders only one single moment for matching, allowing the system operator to identify at any time the moment of irrevocability for transfer orders.

3. Irrevocability of settlement (SFIII)

After the assets have been transferred on the settlement system's accounts, such settlement is considered legally enforceable and binding on third parties, i.e. their settlement is final. Again, the system should provide one single moment of irrevocability of asset transfers for each transaction so that the operator (in this case the CSD) is able at all times to recognise the transactions processed by the system and time stamps for the irrevocable asset transfers.

5.2.3 Challenges and opportunities

As mentioned above, the decentralised nature of a DLT solution creates certain technical and/or operational challenges when it comes to ensuring that single moments of finality are defined.

Moreover, real-time (or near-real-time) settlement could have an impact on the relevance of SFD protection. In general, near-real-time settlement would reduce the number of transfer orders requiring SFD protection because the transactions would be settled almost immediately in the settlement system. At the same time, however, if transactions were settled almost immediately after a trade, there would also be a risk that a significant amount of transfer order instructions would be entered into the system and settled after the opening of insolvency proceedings against the participant. This is because the system would not have the time to suspend access to the insolvent participant.

6 Settlement discipline regime

6.1 Introduction

This chapter discusses the implications of potential DLT adoption on the settlement discipline regime. One requirement for the smooth functioning of financial markets is that counterparties in securities transactions reduce or eliminate the risk of settlement fails caused by a counterparty failing to meet its obligations when due. One approach in this regard is to create financial and reputational incentives for counterparties to adhere to the agreed settlement timing – i.e. ensuring settlement on the intended settlement date (ISD).

Settlement fails on the ISD can be caused by many factors, including mismatches driven by wrong or incomplete information in the instruction and the inability to settle other trades, causing onward delivery to fail.

Different EU markets have divergent settlement discipline regimes (SDRs). These frameworks may differ in whether or how they impose a mandatory buy-in process, timelines for SDR actions, recycling procedures, and/or penalty fines in the case of a settlement fail. This lack of harmonisation has raised the issue of potential regulatory arbitrage, particularly in the connected T2S markets, thus leading to a need to establish a harmonised SDR across European jurisdictions.

The implementation of the CSDR will impose a harmonised SDR expected to be adopted at the beginning of 2018 and entering into effect two years thereafter. The CSDR empowers ESMA to adopt regulatory technical standards regarding:

- the process for collection and redistribution of cash penalties imposed on the counterparty unable to deliver securities or cash;
- enforcement of a buy-in procedure in the event that a settlement fail persists;
- a set of technical measures that incentivise and facilitate timely settlement of transactions.

A number of T2S platform change requests are being considered to support CSD compliance with the regulation's requirements. This follows a request from the T2S community to ensure that CSDs ideally share the development cost and make the necessary changes only once and through T2S, where feasible. Hence, any change in business processes brought by the adoption of new technologies is highly relevant for T2S participants and deserves scrutiny from T2S governance.

6.2 Impact of potential DLT adoption

The analysis below assumes a scenario where a CSD subject to the CSDR has integrated DLT into the settlement process, since a settlement fail outside a CSD would have to be resolved bilaterally between the parties.

In this regard, it is important to note that restricted ledgers are likely to work more effectively in the context of SDRs, especially if they involve financial penalties. An unrestricted DLT network would need to ensure that the assets of the failing party are available and sufficient to pay any penalties.

6.2.1 Impact on current processes

Settlement fails can occur for various reasons and as a result of operating characteristics that are inherent in the current market structure. Examples include the following.

- Participants manage a trading position that is separate from their settlement position. The initiation of a trade to sell a security can trigger the initiation of another trade to purchase the same security, to be delivered in fulfilment of the previous obligation. As long as the ISD for both trades falls on the same day, the trading position is closed. However, if the settlement to receive stock fails then this may lead to the failure of the settlement to deliver securities.
- The content of a standard settlement instruction (SSI) is subject to the risk of human error and incorrect information input that will require manual intervention to prevent a fail.
- Market participants may use securities positions to secure other obligations, e.g. in collateral management arrangements. Within this context, there is a risk that the settlement fail of a collateral recall or substitution process will cause settlement fails in other trades.

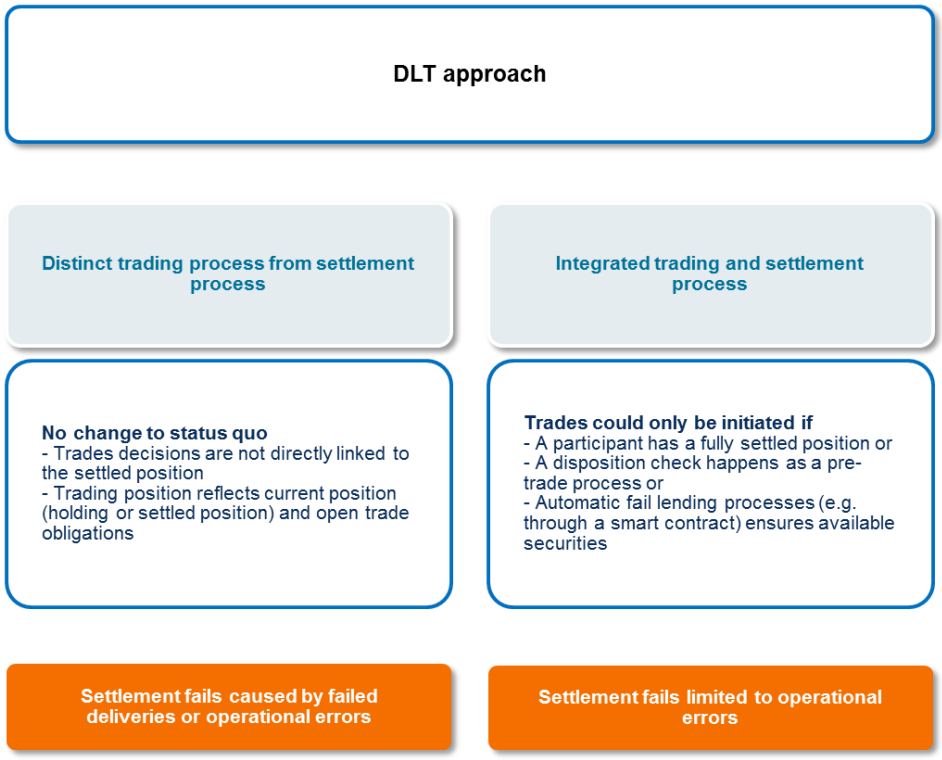
6.2.2 DLT-enabled processes

Today, investors manage a trading position reflecting their current position (holding) and corresponding trades making up this position based on the trade obligations they have entered into. The actual settlement position may differ due to settlement cycles and settlement fails. Therefore, there is a design choice to be made with DLT-based settlement arrangements, namely in deciding how trading activity should be integrated into the settlement process. The options would be to maintain the distinction between the trading position and the settlement position, or to follow an “instant settlement at trading” model. The choice made would reflect the likeliness of settlement fails occurring.

A DLT solution could integrate the execution of a trade with the settlement into a single process, in which case trades could only be initiated if a participant had a fully settled position to commit. Alternatively a disposition check could be carried out as a pre-trade process, or fail lending processes would be automatically triggered (e.g. through a smart contract). This would imply that settlement fails were limited to operational errors (see Figure 6).

Figure 6

Settlement discipline regime in a DLT-enabled securities market



If a DLT system were adopted based on significantly reduced standard settlement cycles, e.g. frequent intraday trading/settlement cycles, then the trading and settlement positions would become closely aligned and further reduce settlement risk based on economic considerations, whereas the impact on settlement fails driven by operational issues would be affected differently depending on the level of straight-through processing (STP). Under these circumstances, the requisite SDR approach would be primarily concerned with establishing rules for following the agreed process by agreed timelines, as opposed to setting financial or reputational incentives to address settlement fails. The extreme case of "instant settlement at trading" would eliminate the concept of an ISD for spot transactions: a matched trade would have no ISD as the settlement would take place immediately.

However, there will still be a need for a comprehensive SDR if DLT-enabled processes do not fully contain all the following characteristics:

- no difference between a trading position and a settlement position, e.g. a security can only be sold from a settled position, or securities fail lending is integrated in such a way as to ensure settlement;
- the largest possible universe of market participants involved in trading in a specific asset (e.g. ISIN) is represented on the blockchain, thus removing the need to reconcile with databases outside the system that otherwise could cause further operational errors;
- no operational dependencies on systems that do not interoperate with the DLT system, e.g. settlement of the cash leg must be possible either via DLT

or in a way that does not affect the consistency of data accessible by the DLT system in real time;

- the instruction method is highly automated, with unambiguous static data to ensure low possibility for human error to instruct trades;
- assets in securities financing transactions are fully fungible, e.g. if an asset is subject to a collateral arrangements there is no risk of assets being recalled when needed as part of a substitution process.

6.2.3 Challenges and opportunities

The adoption of a distributed ledger for the post-trade processes could potentially reduce settlement fails by eliminating the need to reconcile information across databases of financial institutions and market infrastructures, with STP and no need for human intervention in transaction processing. That would reduce the need for an extensive SDR, both in the case of CSD involvement and in the contractual case of internalised settlement. Settlement fails could potentially even be eliminated if the differentiation between a trading and a settlement position were superseded in a "settlement at trading" or "T-instant" scenario. Such an extreme shortening of the settlement cycle would, however, affect the liquidity management of market participants, since a sell trade could only be concluded if the participant already had a fully settled position for the share amount available, as further explained in Chapter 7 of this report.

However, in the absence of the conditions mentioned at the end of the previous section, a DLT solution would not diminish the risk of settlement failures. Moreover, there are other considerations in the context of DLTs that would need to be addressed on a future SDR approach for DLT arrangements, including the following.

- DLT systems need to be designed in such a way that the agreed content of the ledger cannot be modified, ex post, by malicious users. If the need were to arise for corrections to be made to erroneous trades/transactions, this would require the creation of new instructions as opposed to the cancellation of already settled instructions.
- Depending on how the DLT platform was designed (assuming a CSD subject to CSDR requirements would adopt a DLT-based settlement model), "matching" of settlement instructions might not be required, whereas CSDR technical standards provide that settlement penalties are only applied after an instruction is matched. A settlement discipline would have to be defined without the need to refer to settlement matching, or to change the definition to identify DLT-related processes (e.g. "signing" a transaction) as matching. This would create fragmentation among DLT systems and inconsistency with non-DLT systems.
- Roles and responsibilities assigned under the CSDR to specific actors (e.g. entities designated as CSDs to enforce a settlement discipline) might no longer apply on a one-to-one basis to a DLT arrangement. This would depend on whether CSDs operated DLT systems or whether a financial institution such as a CSD participant used a DLT solution for internalised

settlement among its clients. In the latter case, settlement fails would need to be reported but would not necessarily require a dedicated settlement discipline.[51]

- Back-dated transactions clash with the logic of some DLT arrangements, namely with those based on UTXOs, where the chronological ordering of transactions matters for their validation. In contrast, contemporary settlement systems, including T2S, allow for the creation of back-dated instructions (e.g. a settlement instruction sent today with ISD yesterday). Any future SDR would still need to be concerned with interest or other compensations.
- Some DLT arrangements might require that a certain percentage of nodes were active at a given moment in time to perform the validation of new instructions. A participant might be unable to have a new instruction added to another block due to the technical failure of a significant number of other participants (not even related to the participant's instruction), thus increasing the risk of settlement fails. In a DLT environment, the question of settlement fails under an SDR might not easily be separated from the question of business continuity.
- Participants have to opt in to partial settlement for transactions failing for a specific period. It is questionable whether partial settlement would be feasible in a DLT-based settlement model if there were no single party able to modify the content of the distributed ledger.
- Cash penalties are applied from the ISD even if transactions are matched only after ISD. Today's settlement systems may allow the instruction of back-dated trades. Some DLT arrangements would not allow this anymore.
- Recycling rules (e.g. whereby a CSD must recycle settlement instructions that have resulted in a settlement fail until they have been settled or bilaterally cancelled) might no longer be relevant in a DLT concept, as an instruction either settles or does not.

[51] See also *The Distributed Ledger Technology Applied to Securities Markets*, Section 6.2, ESMA, 2017.

7 Settlement day schedules and settlement cycles

7.1 Introduction

Innovative technologies such as DLTs have the potential to redefine the scope, format and content of many of the products and activities that are currently part of the financial services industry. This chapter is an initial discussion of how the adoption of STP and, more specifically, DLT-based technical solutions might impact (positively or negatively) T2S harmonisation activities in the area of settlement day schedules and settlement cycles.

Whereas for transferable securities executed on trading venues a common settlement cycle has been set by CSDR to a maximum of two days after the trading day, settlement day calendars are part of the rules of any settlement system and left to the discretion of its operator.

7.2 Impact of potential DLT adoption

7.2.1 Impact on current processes

A DLT solution applied to securities settlements would imply that by design all participants in the holding chain are bound by the same day schedule and calendar and would necessarily be bound by the same rules on the permissible settlement cycles, as further explained below.

One of the key benefits being discussed in relation to the adoption of a DLT solution for settlement is that STP may be established between trading and post-trading services as well as between parties involved in the post-trade processes.

Under a rather radical adoption scenario, the execution of a trade on a DLT-enabled trading venue would immediately trigger the related DvP 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).

This scenario would effectively allow settlement on trading date (T+0), or even instantaneous settlement at trade (T-instant), on a 24/7/365 basis. This might be associated with efficiency gains in transaction processing and the reduction of systemic risk. However, this extreme scenario would potentially bring a number of practical difficulties, such as requiring a closed system with a captive membership, currency and eligible securities – as well as the need for the seller to have all securities in its possession and for the purchaser to have sufficient cash in its account before a trade can be initiated. In addition, the abolition of the benefits of

netting, along with the removal of other agents – and thus the removal of the intraday liquidity that these agents provide – is also likely to cause a series of adverse effects that have not yet been quantified, most notably on market liquidity.

An alternative scenario for the settlement day schedule with a less radical impact on the securities post-trade industry would be that of DLT networks in operation with a five-day-week operating schedule and a 12 to 18-hour operational day to allow a wider geographical zone to be effectively covered than is currently the case. This schedule for the operational day could allow for an efficient alignment of technical and operational procedures in the DLT network with the requirements of other market infrastructures. Furthermore, an optimal solution for the interconnection between trading and post-trading might retain some elements of netting periods and a role for clearing institutions to address some of the negative impacts on liquidity, while reducing timeframes, enhancing automation and minimising risks and costs.

It should also be noted that a single settlement day schedule does not necessarily mean that all settlements take place in the same settlement cycle. Different markets and different instruments might reasonably require some specific operating schedules. Some DLT projects are looking at technological solutions for post-trading that would allow a flexible settlement cycle. This could be useful for some participants in the chain utilising securities financing transactions (SFTs) for coverage of short-selling, for instance.

Smart contracts or other automated solutions might be implemented in order to minimise the impact of the shorter settlement cycle on funding and liquidity (e.g. auto-collateralisation, auto-securities lending, etc.).

7.2.2 DLT network scenarios

The key characteristic of DLT networks that would be likely to have a considerable impact on the adoption of different possible settlement day schedules is their geographical reach, i.e. the set of securities and participants (operators and/or validators). This could either be limited to the EU or it could span continents. Depending on this aspect, a number of technical and operational factors need to be considered.

Single-region DLT network

Under this scenario, the issues faced in the adoption of a DLT-based settlement network are essentially similar to the issues that are currently faced by any settlement system. In fact, restricting the network geographically to Europe, for instance, would eliminate the need to adopt solutions that would allow access to the network during business hours in more than two or three time zones.

In this scenario, the settlement day schedule of the DLT network could be aligned to the day schedule of other existing settlement infrastructures, so as to ensure the maximum degree of interoperability (for instance, alignment of maintenance periods,

of critical operational milestones at the start of day, during the day and at the end of the day, and of other specific processes such as funding, collateralisation, repos and securities lending, corporate actions processing, etc.).

Global or multi-region DLT network

A higher degree of complexity arises in a scenario where a DLT network is designed to operate across multiple geographical regions.

Various proponents of DLT solutions for settlement services highlight the possibility of wide and seamless, 24/7/365 coverage of business needs, based on the fact that each new settlement transaction would be performed through largely automated processes that could be programmed to execute immediately after the execution of a trade. However, unless the DLT network is designed to be completely isolated from other market infrastructures, a seamless and efficient interaction between a continuously running DLT network and other existing clearing and settlement systems currently in operation could be difficult to achieve.

The ability for a DLT network to become interoperable with other market infrastructures worldwide that are currently designed around quite substantially non-harmonised operating day schedules and calendars would not be easy: all business processes and operational day milestones would need to be carefully analysed to highlight differences and overlaps between the existing systems and the potential DLT-based solutions, so that appropriate interfaces and synchronisations could be adopted to ensure efficient interconnection and communication of relevant information and resources. This would add to the same technical and business aspects as those noted in the section above on single-region DLT networks.

It is worth noting that the flexibility of programmable functions and processes achievable by a DLT solution might itself become the solution to the needs of global interoperability. Global interoperability is a new problem to be tackled by the financial services industry. It did not exist, or was largely avoided, before the start of discussions on DLT-based solutions. Global interoperability was not considered within the framework of traditional technologies, simply because the technical hurdles would have been so great and difficult to resolve that there was no business case and no interest to pursue a search for possible solutions. The adoption of innovative technologies based on DLT, smart contracts, etc. might effectively lead to the definition of new standards for interoperability that would allow for new business and operating models to evolve in response to ever-increasing demands for global integration in the financial markets.

7.2.3 Challenges and opportunities

Under a single-region model, it is likely that the technical and operational issues that might arise would be addressed in a similar fashion as in current traditional systems. Hence, the adoption of a common settlement cycle could be easily achieved, in line

with current business practices. However, in the case of a wider geographical region, the alignment of settlement calendars appears challenging unless the 24/7/365 option is chosen, which entails radical changes to the current business of market participants. Unless all segments of financial markets adopt the same schedules, there may be significant hurdles arising at the interconnecting points (e.g. significant funding and transferability issues between DLT-based settlements and traditional settlements).

Challenges:

- the net effect of shorter settlement cycle for securities transactions, potentially enabled by the level of STP of an all-encompassing (or fully interoperable) distributed ledger(s) is unclear and warrants additional analysis, since the effect would be a lower amount of counterparty risk and higher availability of collateral, but also possibly a decrease in market liquidity unless mitigating tools are made available such as autocollateralisation, automated securities lending, etc.;
- interoperability issues will of course arise in the case of multiple settlement DLT solutions for different markets, different geographies or different user groups.

8 Collateral management and DLTs

8.1 Introduction

This chapter focuses on the possible use of DLTs in collateral management processes, i.e. the services via which collateral can be mobilised by counterparties in a transaction or participants in a system. Following the 2008 financial crisis, regulators increasingly require market participants to provide collateral to mitigate risks in the financial system. Driven by the reform agenda put in place by the Group of Twenty (G20) and aimed at reducing systemic risk in the non-cleared over-the-counter (OTC) derivatives markets, regulators are making collateralisation mandatory to secure and offset losses caused by the default of a counterparty. The importance of collateral to ensure risk management in FMIs is recognised in the PFMIs issued by the CPMI and IOSCO. The same agenda has resulted in a wave of regulations in all major jurisdictions and especially in the EU, with the issuance of the European Market Infrastructure Regulation (EMIR)[52] for central counterparties (CCPs) and trade repositories, the CSDR for CSDs, and the SIPS Regulation for certain payment systems. The Basel Committee on Banking Supervision and IOSCO put in place a global policy framework and timetable for rolling out the new margin rules in non-centrally cleared OTC derivatives markets.

The impact of these new regulations on the industry is far-reaching and makes efficient mobilisation of collateral to cover financial exposures a key priority for buy-side and sell-side alike. Moreover, the Basel III capital rules reinforce the drive for collateral efficiency and the need to overhaul current practices by penalising long-standing margin call disputes. Collateral management services are currently provided by, among others, triparty agents, whose operational models developed over time in a non-harmonised manner, with in-house custody being a prerequisite for the service, resulting in a lack of interoperability between these actors.[53]

8.1.1 Services included in collateral management

Collateral is the amount of cash or securities given as a guarantee by the counterparty debtor (collateral giver) to the counterparty creditor (collateral taker) to cover the credit risk resulting from financial transactions negotiated between these two parties. In the event of default on the part of the debtor, the creditor has the right to retain assets used as collateral as compensation for the financial loss suffered.

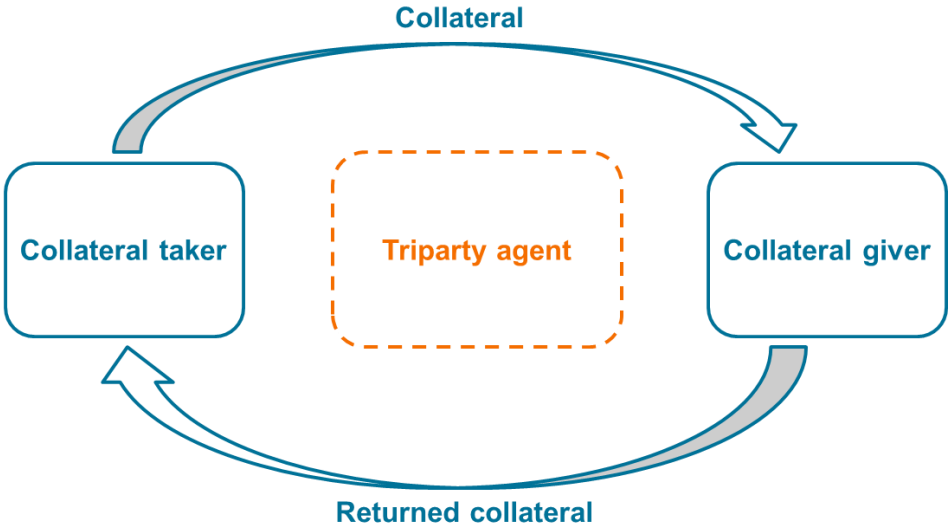
---

[52] Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories (OJ L 201, 27.7.2012, pp. 1-59).

[53] Significant progress has been made in recent years to bridge this gap, with initiatives to link international CSDs' triparty collateral management systems with those of domestic CSDs and agent banks to facilitate cross-border collateral mobilisation.

The rules for collateral management are usually defined in a bilateral agreement (framework agreement) signed by the two parties prior to the start of negotiations or via their triparty agent, which opens security and/or cash accounts in its own books for the two parties in order to initiate and record cash or security flows related to the collateral flow. This agreement stipulates a certain number of factors such as the types of transferable assets as collateral, the valuation rules of these assets, the thresholds for margin call, whether the collateral received can be reused, etc.

Figure 7
Bilateral and triparty models of collateral management



Pledge vs. title transfer

Current collateral management processes distinguish between transfer of title, where the ownership of assets moves from the collateral giver to the collateral receiver, and pledge, where for the duration of the loan the collateral remains owned by the collateral giver but is blocked in favour of the collateral receiver throughout the lifecycle of the transaction. In a triparty collateral management system, this distinction is implemented via the ownership of the accounts at the triparty agent. Accordingly, in the case of pledge, the account is opened in the name of the collateral giver, although collateral movements to release the securities are only executed on matching instructions from both counterparties, while for title transfer the account is in the name of the collateral receiver.

Collateral management can be broken down into three steps:

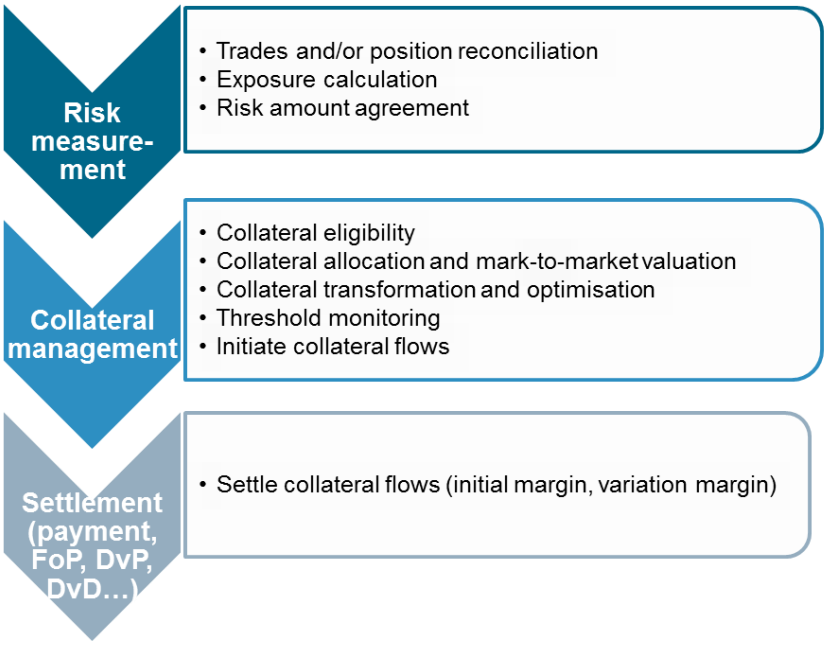
- the measurement of the counterparty credit risk that has to be collateralised;

- the collateral management strictly speaking (allocation, evaluation, transformation, substitutions, reuse, income/corporate actions management, etc.);

- the settlement and restitution of collateral.

These processes require substantial technical and human resources, which is the reason why they are often dealt with by a third-party agent.

Figure 8
The three steps of collateralisation



Collateral management practices

Coordinated regulations at a global level are introducing daily exposure valuation and margin exchange, along with narrower windows for dispute resolution and for portfolio reconciliation. The increasing use of electronic messaging for margin exchange is also enhancing current practices, but despite these improvements the market is a long way from reaching a satisfactory level of automation and efficiency in the bilateral collateral management space.

Communication still occurs to a considerable extent by email and sometimes by fax; spreadsheets are often used for margin calculations; known reference data and calculation differences between counterparties are persistent; margin call disputes are left outstanding for long periods of time; reconciliations are done manually; and the smaller market participants in particular do not have automated systems linking the collateral management applications with their settlement systems.

At the beginning of the operation and then at regular intervals, the underlying risk[54] that the collateral covers must be reconciled, valued and compared with the marked-to-market value of the posted collateral in order to ensure its adequacy. Differences between the risk exposure and the collateral value that exceed agreed thresholds trigger margin calls to mitigate excess or deficits that may arise during the lifecycle of the transaction.

[54] The underlying risk of a transaction consists of a stock of contracts (on the OTC market) or open positions (on organised markets).

In the case of OTC derivatives, the “initial margin” collateral protects counterparties against potential future exposure before the positions are closed out, while the “variation margin” is the change of collateral at regular intervals or when the underlying exposure fluctuates beyond agreed limits.

Collateral can be valued at a price lower than its market value as a risk mitigation technique to effectively over-collateralise the exposure. The aim of this mechanism is to add a security margin (or haircut) to the creditor, taking into account possible fluctuations in the value of the collateral between the two margin calls.

The current services often rely on a custody offer for collateral used and available, so these services are usually offered by custodians or investor CSDs. The multiplicity of operations, actors and places of custody results in fragmentation of collateral pools. This hinders collateral mobility and optimisation, especially when securities are held in different countries.

The FCD and SFD set the groundwork for conducting collateral management and securities transfers in the EU. The directives are principle-based and would be a necessary point of reference for developing a new platform for collateral management using DLT technology.

8.2 Impact of potential DLT adoption

8.2.1 Impact on current processes

Only a restricted DLT network could guarantee investor protection and be consistent with measures against money laundering and the fight against terrorism.[55]

The main potential advantage of DLT adoption in a restricted environment is the ability to rely on a distributed database enabling all participants to share consistent information at the same time while a database centralised by a single entity requires other participants to manage their own databases and to regularly ensure the coherence of the latter with those of other intermediaries located up and down the processing chain. At the same time, a distributed ledger provides logical unity and ubiquity thanks to the consistency of data available to different participants.

Use of DLTs should prevent the need to reconcile collateral positions between the collateral giver, the collateral taker, and their intermediaries.

Another potential advantage of some DLTs is the possibility of launching automatic processes directly on the platform via smart contracts. However, each new smart contract theoretically generates a new risk in the event of security issues within the

[55] See general market agreement on this topic as shown by the ESMA Consultation on the Distributed Ledger Technology Applied to Securities Markets: https://www.esma.europa.eu/press-news/consultations/consultation-distributed-ledger-technology-applied-securities-markets

smart contract code (the reference here is to the DAO heist – see Chapter 11, Cyber resilience).

For collateral management as well as other post-trade market services, it is important to assess whether it is better to set applications within or outside the DLT platform.

In a DLT environment, smart contracts defined by counterparties could be used to enforce collateral arrangements in the distributed ledger and to identify “pledged” securities that cannot be released or transferred to other participants.

With the volumes of margin calls increasing and delivery windows narrowing, there is a clear need to address the lack of automation and standardisation in bilateral collateral management. DLT is well placed to boost STP and to deliver additional enhancements such as facilitating the use of securities collateral, easing the substitution process, promoting the standardisation of reference data across participants and automating income payment and corporate action processing. Smart contracts can also be used to represent the contractual information behind collateral operations, as opposed to account structures, removing the need for securities to be substituted during custody events.

Marking to market could additionally be conducted in real time as part of the collateral smart contract if a reliable data source becomes available. This does not exclude the possible need for some manual validation by customers prior to the transfer of additional collateral following a margin call.

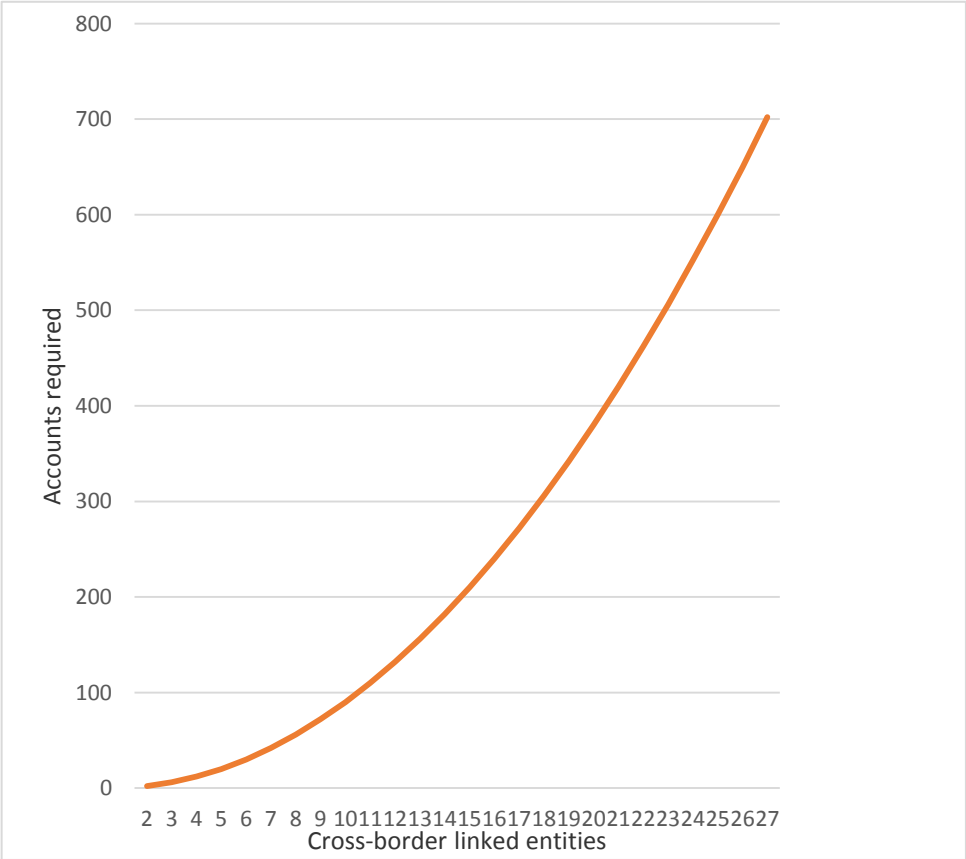
Cross-border scalability benefits

Whereas mobilisation of collateral in a domestic market only abides by national legislation and is thus less complex, cross-border mobilisation is largely cumbersome given the need to use multiple non-harmonised connections between financial market infrastructures. Currently, the cross-border mobilisation of collateral generally requires bilateral agreements between the custodians/CSDs in the respective markets, with subsequent mutual account opening and bilateral reconciliation. This model runs into scalability issues when an attempt is made to create a truly interoperable collateral pool. This is because, as the number of cross-border linkages increases, the number of accounts required across the pool also increases, but exponentially (see Figure 9).

The overhead for each new linkage relates not only to account opening, but also to settlement and reconciliation procedures connected to the movements of collateral.

Figure 9

Number of links required as a function of linked entities



8.2.2 DLT-enabled processes

The service coverage dimension of a DLT network is relevant in the context of collateral management. This is because DLT implementation could be used either exclusively to register collateral movements (for information/accounting purposes only) in the accounts of a collateral management service provider, or additionally for settlement of collateral transactions among all market participants. This leads to the two scenarios explored below.

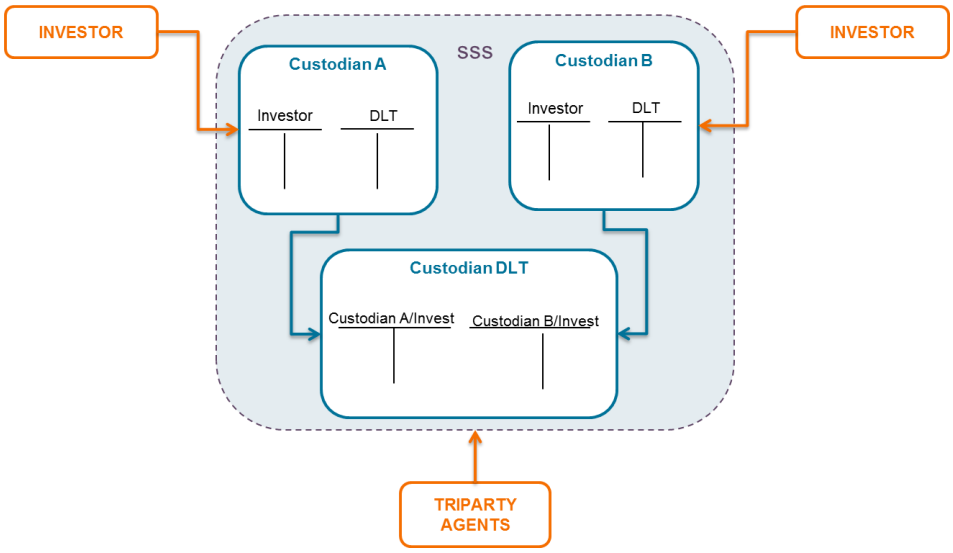
Scenario 1: DLT limited to managing a single collateral ledger

In this scenario there is a separation between a DLT arrangement following collateral management logic and an SSS which may or may not be DLT-based. The securities are transferred to the DLT platform managed by the participating custodians when their use as collateral is requested. Collateral represented on the distributed ledger would not be DLT-native assets, but instead tokenised representations of non-DLT assets.

Therefore, there are ultimately no significant differences in relation to current practice, since the ledger of a custodian still depends on separate records in the separate databases of other financial institutions and FMIs. A possible consideration would be to open the DLT platform more easily to multiple triparty agents, but if this function is offered by the DLT custodian, it is not granted that its ledger will be open to potential competitors.

The primary interest of DLT, which is to be able to connect information held in transaction databases of different institutions, is not leveraged in this scenario.

Figure 10
DLT limited to managing a single collateral ledger



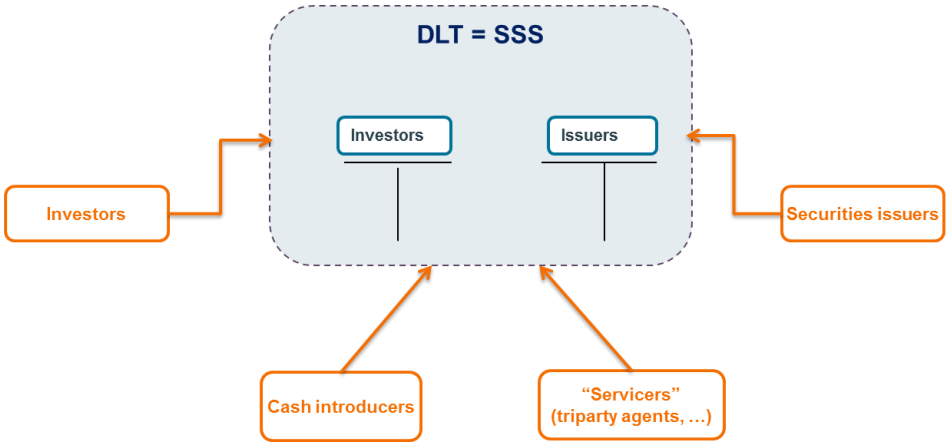
Scenario 2: use of a distributed ledger for both settlement and collateral management

In this scenario, a distributed ledger is available to all market participants involved in collateral management and in the post-trade processing of securities transactions. A higher level of automation could be achieved in the collateral management process, since the settlement movements that may be necessary as a result of collateral management processes could be automatically linked to the collateral management activity itself. In other words, smart contracts processing activities such as margin calls and substitutions could automatically initiate the necessary settlement operations.

In this scenario it is assumed that both the securities and the cash settlement take place on the DLT platform. It therefore seems appropriate to include in the DLT platform not only the securities issuers but also the issuers of cash (or of its representation) either from central banks and/or from the commercial bank.

Figure 11

Distributed ledger for both settlement and collateral management



8.2.3 Challenges and opportunities

The use of a distributed ledger accessible by all interested market participants and providing a common set of rules and standards allows straight-through processing of transactions and removes the need for a mutual account-opening process between institutions active in different markets. Adding a new cross-border linkage only requires the new participant to connect to the platform for all existing participants to gain a link. Of course, the legal issues with regard to the opening of links between financial institutions and market infrastructures from different jurisdictions need to be properly tackled in such a scenario, and harmonisation of rules or clear solutions to disputes over a conflict of laws would be required for it to be viable.

Further consideration needs to be given to defining the potential scope of collateral management in a DLT network, in terms of asset classes, the nature of the assets recorded on the ledger. The actual implementation of the DLT network needs to provide certainty on whether a position in the ledger constitutes full title or another form of entitlement. In addition, these positions in the DLT network would need to be recognised as collateral under the applicable law. If the DLT implementation is based on a tokenisation of assets outside the distributed ledger, there is still a need to track the ownership of the assets themselves outside the DLT and ensure that it is possible to transfer the assets or make them available to the non-defaulting party in the event of a counterparty default. This process may be complex if the DLT implementation does not also handle settlement and custody of assets.

9 Asset servicing

9.1 Introduction

This chapter proposes initial reflections on how the adoption of STP and more specifically DLT-based technical solutions might (positively or negatively) impact T2S harmonisation activities in the area of withholding tax (WHT) processing, the registration and identification of shareholders, and portfolio transfers, as well as possibly fostering a more streamlined and automated process for the distribution of income, for shareholder registrations and for the processing of double taxation treaty (DTT) benefits where applicable.

The area of asset servicing is potentially a candidate for a highly beneficial adoption of innovative automated processing solutions, possibly using DLT networks and smart contracts. This expectation comes from the fact that asset servicing requires a large number of dedicated resources, along with ad hoc and specialised expertise. Multiple data feeds and information sources need to be interconnected and reconciled, and there is a high degree on manual intervention in each step of these processes, with a high risk of error due to the lack of automation.

Asset servicing is an area of great interest to European market participants and more specifically to the T2S stakeholder community, since the incomplete adoption of harmonisation standards, particularly in areas such as corporate actions on flow, is a significant barrier to smooth direct links among CSDs. Under current market practice, a complex series of back-to-back contractual arrangements exists between data originators (mostly issuers), data providers and data users (mostly intermediaries, custodians and end investors). This series of contractual arrangements is put in place to address the risk of incorrect data being used somewhere along the chain of actors, and to define the respective responsibilities and liabilities of each actor within this complex information processing network. Furthermore, it is quite common that any specific set of reciprocal liability clauses between two actors in the holding chain would need to be replicated, in a substantially similar form, at all the next levels in the holding chain, thus adding further complexity and redundancy in the overall structure. It could be argued that, in a DLT network, the initial engineering design of how each actor would have access to the data in accordance with its role or function would effectively be an efficient substitute for all such bilateral or multilateral series of legal contracts, so that all the reciprocal responsibilities and liabilities for the origination, provision and usage of the data would be defined in one single step within the operating and functional design of the DLT network itself, provided that appropriate governance is in place.

The term “asset servicing” relates to events during the life of a security. From the point of view of an investor, the term relates to the process whereby an investor is able to exercise rights relating to the ownership of a securities position during the period of holding securities, i.e. subsequent to settled acquisitions in the primary or secondary market and prior to dispositions by way of sale. In order to exercise such

rights for securities held through an intermediary, the investor is dependent on the assistance of the intermediary, and thus on the specific services provided by the intermediary. The specific asset services include custody services and related corporate action processing, tax processes, registration processes, shareholder identification processes and general meeting processes as well as value added and ancillary services.

In many cases, asset servicing processing results from corporate events, i.e. special occasions in the life of an issuing entity that are reflected in various different ways in its securities. Even the most complicated corporate actions can be viewed as consisting of a combination of comparatively simple actions, listed below. This process involves a chain of actors, including the issuer, the issuer CSD, a chain of intermediaries (including investor CSDs) and eventually the end investor. These actors are required to follow strict timetables to allow for specific sequential actions to be processed correctly.

Broadly speaking, corporate events can be categorised as (a) general meetings (b) distributions and (c) reorganisations. The actions required by participants are triggered by a set of three key reference dates: the record date, the election date and the payment date.

These three broad categories include other activities such as market claims and tax services relating to taxable corporate action events.

(a) General meetings

The process for general meetings starts with a notification from the issuer to all holders of its securities (shareholder or bondholder meetings). End investors are entitled to vote based on their holdings as of a predefined record date. Entitlements resulting from the positions recorded by intermediaries as of the record date are not themselves booked on securities accounts as in the case of all other types of distributions, but are used to validate instructions from end investors relating to the general meeting. Such instructions can include attendance as well as voting by correspondence, participation, and proxy voting.

(b) Distributions

The process for distributions is similar whether they are in cash (paid through the CSD) or in securities (distributed through the CSD). Both involve the same chain of participants as most asset servicing and a timetable starting with an announcement, continuing with an ex-date and a record date, and finishing with a payment date.

Distributions of cash or securities are booked by intermediaries on cash or securities accounts. Clearly the actions required for distributions must flow sequentially and the time elapsing between each is important – e.g. the announcement should be two business days before ex-date, and the ex-date should precede the record date by one settlement cycle minus one business day. The payment date should be as close as possible to the record date, preferably the next business day.

Some distributions may offer end investors an option and hence should be represented by an interim security. Such a distribution can be viewed as a distribution plus a mandatory reorganisation with options. Hence, a different timetable is required that starts like a normal distribution, then includes a payment date for the delivery of the interim security, a guaranteed participation date, and buyer protection and market deadlines, and ends with a payment date if the investor selects this option.

(c) Reorganisations

The process for reorganisations involves information flowing through the same chain of participants. The “original” security is redeemed and a new security is issued. For a mandatory reorganisation the sequence of events starts with an announcement by the issuer, the last trading date, the record date and finally a payment date. A price for fractions has to be set and each participant in the chain needs to process them accordingly.

Where the reorganisation is mandatory with options (i.e. a “voluntary” event), the corporate action is more akin to a conversion. The sequence of events starts with an announcement by the issuer, the start of an election period, a guaranteed participation date, a buyer protection deadline, a market deadline and a payment date. A tender process might be included.

9.2 Impact of potential DLT adoption

9.2.1 Impact on current processes

Following the logical sequence of the steps to be processed and the hierarchical structure of the asset holding chain, individual steps underlying asset servicing might be simplified by the use of a distributed ledger. For example, the following workflow could be used:

Event notification from issuer to issuer CSD

→ Event notification from issuer CSD to intermediary

→→ Event notification from intermediary to end investor

Advice of creation/distribution of outcome of the event (cash or new securities) from Issuer to issuer CSD

→ Advice of creation/distribution from issuer CSD to intermediary

→→ Advice of creation/distribution from intermediary to end investor

In the case of events with options or of voting instructions for general meetings, an additional reverse flow of information needs to be considered:

Information on election choice from end investor to intermediary

→ Information on election choice from intermediary to issuer CSD

→→ Information on election choice from issuer CSD to issuer

If all actors mentioned in the simple chains above are nodes participating in the DLT network, then the complexities around the processing of information up and down the holding chain (including all the required reconciliations and consistency checks) could be eliminated, simply by giving simultaneous, distributed access to the relevant information to all actors on the ledger. The design of the ledger would effectively be replacing the need for multiple sequential steps in receiving, verifying and passing on to the next level all the individual pieces of data in this flow of information.[56] It is worth stressing that such information flow can be bi-directional.

There would no longer be any need to collect and transfer such information along the holding chain, since the concept of a hierarchical chain of intermediaries would be replaced by direct interaction between all permissioned actors in the DLT.

The design of specific "smart contracts" could facilitate the implementation of various types of corporate action event, from simple income or rights distributions to more complex voluntary events. Smart contracts could be used to automate the sequential steps required in the information flow and in the processing of these events, and to take into account relevant inputs such as end investor elections, end investor tax status, historical trade data, etc.

Considerations to be further explored in the possible deployment of DLT solutions include the following:

- a DLT solution applied to securities holdings would imply that by construct all connected participants will have to adopt the same rules, procedures and deadlines;
- a DLT solution would need to be restricted to connected participants;
- market standards for corporate action processing could be implemented via ad hoc programming of the rules of the DLT network, using specific smart contracts for each type of corporate action event;
- in order to ensure adequate control over sensitive information regarding holdings, identities, etc., the DLT-based system would need to be designed with clearly defined permissions to each type of stakeholder in the ledger.

[56] Sample cases to be considered and to be further expanded in subsequent analyses are the following, as already identified for instance in the 2016 ISSA (International Securities Services Association) symposium: income payments, rights issues, elective corporate action and proxy voting.

Withholding tax procedures

Similarly to the more general discussion above, it would be imperative to ensure streamlining of processes in the area of WHT so that all relevant stakeholders have access to a common or to interoperable distributed ledgers. The real benefits of automation in the processing of income distributions, tax withholdings and DTT benefits can only be achieved if the system is preventively designed to incorporate all necessary actors and information.

Considerations to be further explored in the possible deployment of DLT solutions would include the following:

- a DLT solution applied to WHT procedures might make use of ad hoc smart contracts for the automatic collection of taxes at the correct applicable rate for each national jurisdiction, for each type of security, for each investor and for each applicable DTT;
- automated processing would imply that refund procedures would no longer be necessary.

Cross-border shareholder transparency and registration procedures

The design of a DLT-based solution that could be adopted for WHT processing purposes might similarly be used for the registration of investors to update corporate registers. It is conceivable that the information and communication flows between issuers and ultimate investors could be based to a large extent on the same registration data regarding the identities and holdings of each investor.

Registration processes are a method to achieve shareholder transparency, and may be triggered either by the settlement of a securities transaction, or by an asset servicing-related event.

Considerations to be further explored in the deployment of DLT solutions include the following:

- primary and secondary markets may potentially benefit from the adoption of a DLT solution, since the actual issuance and distribution activity would be performed in a single step (see Chapter 3, Issuance of securities);
- the notarising function and legislative tasks are subject to validation by means of adaptation of rules, which is key for issuer services.

Portfolio transfer

Although portfolio transfers are a type of settlement process, the principal challenge relating to portfolio transfers is the transmission of extensive information about the end investor, its tax status and its transaction history. The requirement for adequate

processing of the information flow has similarities to several asset servicing-related processes.

Depending on how DLTs might be adopted, the safekeeping account may need to be redefined as an “e-portfolio” that contains tokens or digital securities. The transfer of an “e-portfolio” would seem no longer to be a complicated operational process because the end investor would be directly “holding” its securities portfolio associated with a cryptographic key, without the need for the provision of traditional custody services by a third-party custodian. New roles would become necessary in financial markets, such as that of certification agent for the issuance of cryptographic keys to investors.

9.2.2 DLT network scenarios

Based on the scenario analysis performed by the Task Force on Distributed Ledger Technologies (DLT-TF) established by the T2S Harmonisation Steering Group (HSG), the key characteristics of DLT networks that are relevant to consider for impacts on the various services in the area of asset servicing are the service coverage and geographical reach of a network: in short, for the first characteristic the question is whether the network is used for information sharing only or whether it is also used in conjunction with the automated execution of payments and settlement; for the second characteristic, depending on the geographical scope of the DLT network, various technical and operational aspects need to be considered, for example in relation to the determination of end-of-day holdings and to the possibility of different dates and different calendars in the processing of corporate actions.

Information sharing only/single-region DLT network

In this scenario, a DLT solution is used only to streamline the simultaneous sharing of information and data along the holding chain, from issuers to end investors and, in reverse, from end investors to issuers and other relevant parties at the top of the custody chain. All accounting entries, securities transfers and cash payments are effected through existing “traditional” infrastructures based on information stored in a distributed ledger.

A single-region network would ensure that the complexities related to accessibility from multiple geographical locations, from multiple time zones and in significantly different scheduling and cycles, would be greatly minimised or completely avoided.

Information sharing only/global or multi-region DLT network

In this scenario, a DLT solution is used only to streamline the simultaneous sharing of information and data along the holding chain, from issuers to end investors and the reverse. All accounting entries, securities transfers and cash payments are

effected through existing “traditional” infrastructures, based on information stored in a distributed ledger.

Additional complexities need to be tackled, owing to the need to establish more sophisticated methods for multi-regional and multi-time-zone accessibility.

Information sharing and settlement processing/single-region DLT network

A more complex scenario to be analysed is the case of a DLT network that is used not only for simple information sharing but also for actual processing of accounting entries, settlements and payments. This additional range of activities may be accomplished by discrete interfaces with existing “traditional” infrastructures, or by more complex developments of additional features and functions within the DLT network itself that would allow the execution of all required transactions within the distributed ledger itself.

A single-region network would ensure that the complexities related to accessibility from multiple geographical locations, from multiple time zones and in significantly different scheduling and cycles would be greatly minimised or completely avoided.

Information sharing and settlement processing/global or multi-region DLT network

Additional complexities need to be tackled, due to the need to establish more sophisticated methods for multi-regional and multi-time-zone accessibility.

9.2.3 Challenges and opportunities

Any steps towards the adoption of DLT-based solutions, which could provide momentum to the definition of common standards and operational processes across all participants, could bring significant benefits in this area.

A distributed ledger solution for asset servicing could be the basis for simplifying the existing complex series of back-to-back contractual arrangements between data originators (mostly issuers), data providers and data users (intermediaries and end investors).

The adoption of DLT-based solutions in corporate actions processing has the potential to significantly reduce the existing practical and operational gaps that are faced by the relevant stakeholders (issuers, intermediaries and end investors). By storing all information related to the corporate events in a distributed ledger, the sharing of such information up and down the holding chain from issuers to investors would be greatly simplified. A crucial aspect to be addressed in the case of DLT adoption would be the ability to fully standardise all elements of these

communication flows, so as to allow their use in a shared environment. Another important key prerequisite would be to ensure in a harmonised and interoperable manner that the new technologies are equally adopted by all relevant stakeholders.

Potential benefits could include:

- streamlined process flow for all information flows and requirements from issuers to end investors, and vice-versa;
- simplification and full transparency of reporting to issuers about shareholder votes on voluntary events;
- possibility of significant reduction in the complexity of securities settlements related to corporate action processing;
- harmonisation ensured for all participants, subject to design specifications;
- elimination of the role of WHT collecting agents, reduced operational and credit risks;
- finally, a DLT solution applied to WHT procedures might make use of ad hoc smart contracts for the automatic collection of taxes at the correct applicable rate for each national jurisdiction, for each type of security, for each investor and for each applicable DTT. Automated processing would imply that refund procedures would no longer be necessary.

Potential challenges could include:

- disruption to the providers of registration, taxation, and ancillary asset services for the portion of their services that would be replaced by direct access to the DLT for authorised participants (service proposition of asset services providers remains substantially unchanged for clients who are not authorised to access the DLT network);
- interoperability issues between DLT flows and traditional flows;
- simplification and full transparency of reporting to tax authorities, immediate availability of funds;
- streamlined process flow for all information requirements from issuers to end investors, and vice versa;
- simplification and full transparency of reporting to issuers about shareholders votes on voluntary events;
- reduced or no need for ledger reconciliations among depositories, custodians and registrars;
- a simpler, more STP-driven process for portfolio transfers under a DLT scenario becoming more widely used by wholesale and institutional businesses, too;
- a DLT solution would seem adequate for connected participants. However the need for tax agents and tax procedures would remain for non-connected parties (e.g. retail business).

T2S harmonisation activity 20 – Withholding tax procedures

In order to ensure adequate control over sensitive information regarding holdings, identities, etc., the DLT-based system would need to be restricted and define permissions for each type of stakeholder in the ledger.

Potential challenges could include:

- WHT service providers would need to develop new interfaces and procedures for "traditional" services. There would be potentially increased operational risks for intermediaries and custodians that are connected to the DLT network for the institutional flows but also have retail clients;
- Legislation may need to be updated in most jurisdictions to allow for digital/virtual issuances;
- Privacy vs. transparency issues would require careful analysis of access rights (for issuers, market authorities, fiscal authorities, etc.);
- The DLT-based securities would be accessible only to connected participants, and a new restricted market could therefore be created for these securities.
- There could be disruption to the providers of custody services for the portion of their services that would be replaced by direct access to the DLT for participants (service proposition of custody service providers remains substantially unchanged for clients who are not authorised to access the DLT).
- The DLT solution of "e-portfolios" would be accessible only to connected participants. Interoperability issues arise for the portfolios held in traditional safekeeping accounts;
- Interoperability issues, with a continued need for complex and non-harmonised WHT procedures for non-connected parties.

Although the possible benefits are quite evident and very appealing on a theoretical basis, the complexity of how to actually achieve the transition to such a new DLT-based framework should not be underestimated, as very elaborate coordination of technical developments, business incentives and conversion timetables would need to be established and centrally managed in order to ensure a seamless, concurrent transition to the new framework by all actors.

10 Reporting, business and regulatory

10.1 Introduction

This chapter focuses on the possible use of DLTs in the field of trade and post-trade reporting. Recent regulations enforce timely reporting on a range of transactions. The EMIR requires the reporting of specific information about a range of derivatives transactions, along with counterparty data on the entities conducting the transaction and on collateral. Data reported are subject to change throughout the term of the derivatives transaction, and reporting updates need to take place when such changes occur. Reporting is required from both counterparties to the transaction, both financial and non-financial entities. Delegated reporting is possible, allowing entities to report on behalf of other entities.

Looking beyond EMIR to the wider scope of reporting under other regulations (MiFID II; the Markets in Financial Instruments Regulation (MiFIR[57]); and the Securities Financing Transactions Regulation (SFTR[58])), it is worth noting that there is not a complete overlap in terms of data fields, timing, reporting parties and authorised regulators.

The current post-trade environment relies heavily on relational database structures for transaction data and account balances, as well as ancillary business data from systems such as enterprise resource planning, customer relationship management, data warehouses, and ultimately the various business intelligence tools which generate useful management information from these various sources.

For example, the Liquidity Coverage Ratio (LCR) was created to ensure that banks have an adequate level of high-quality liquid assets (HQLAs) in order to absorb financial and economic stress that can arise in the market. In the current reporting process, data are pulled from various databases inside a financial entity and calculated under the ratio components. Figures may be manually reconciled, verified and approved. The gathering, analysis and reporting of data from various different databases is time-consuming, requires a substantial amount of resources and bears the risk of manipulated data reports.

The implementation and maintenance of interfaces between the transactional systems of a CSD and custodian bank transactional systems, and of the range of business systems and business intelligence tools, are tasks that require considerable resources and are replicated across all market participants in a highly fragmented and non-standard way. Data necessary for reporting is usually

[57] Regulation (EU) No 600/2014 of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Regulation (EU) No 648/2012 (OJ L 173, 12.6.2014, p. 84–148).

[58] Regulation (EU) 2015/2365 of the European Parliament and of the Council of 25 November 2015 on transparency of securities financing transactions and of reuse and amending Regulation (EU) No 648/2012 (OJ L 337, 23.12.2015, p. 1–34).

distributed across different systems which do not communicate with each other and where different access controls may hinder smooth dataflow.

10.2 Impact of potential DLT adoption

DLTs could potentially be used for the collection, consolidation and sharing of data for reporting purposes, either by providing a new tool for what is currently a separate process from trade settlement (Scenario 1 in Section 10.2.1) or by enabling the introduction of a new reporting process embedded into the rest of the trade lifecycle (Scenario 2 in Section 10.2.2).

In any case, DLT implementation would not remove the need to aggregate information from a number of distinct DLT and off-DLT locations in a diverse range of formats. As such, the potential benefits of DLT implementation to reporting and reconciliation may take considerable time and effort to achieve.

10.2.1 Impact on current processes

In the first scenario under consideration, where the distributed ledger is essentially used to collect and communicate data collected from other databases, interfacing and possibly reconciliation would still be required to verify that the data reported corresponds to data recorded elsewhere in the post-trade process. That would still be a challenge to market participants that are dealing with the increasing volume of transactions to be reported on a daily basis and need to manage reporting timing issues also to make data available to trade repositories and regulators.

DLT could solve certain issues in the area of cost and especially reconciliation across different systems – many of which are upstream of regulatory reporting but are nevertheless part of an overall process. Cost-savings might be achieved, both *intra*operationally within one firm and *inter*operationally across multiple firms. At the same time other costs might have to be counted against the savings in the form of computational resources necessitated to operate some DLTs (such as data storage capacity, network capacity), as well as the costs of necessary technical adaptations with potentially widespread effects within financial markets.

Looking at the process of business reporting, the adoption of DLT would be likely to trigger a large scale re-engineering of many reporting processes. While the use of DLTs could reduce the cost of maintaining interfaces, banks will face a challenge to standardise the output from the DLT into reporting systems, as the remainder of the tools and processes will remain highly custom-made and reserved for the internal use of the firms involved.

On a macro level, efficiency gains would depend on the grade of application of DLTs within the industry, as even the smaller market participants would ideally be in the position to use a DLT application once it was set up. The running of multiple different reporting processes/systems in parallel – one based on DLTs and one following

conventional reporting methods – could otherwise initially make a transitional period more inefficient.

Regulators could also be affected by higher costs during a transitional phase. In particular, different technical requirements/systems would have to be catered for to enable the regulators to cross-analyse the data submitted to them via two different technology solutions.

10.2.2 DLT-enabled processes

In a second scenario, where information recorded in a distributed ledger is used both for reporting and for settlement, some of the reconciliation issues involved in current business reporting would be mitigated, since the DLT records would represent accurately not just the instruction history but also the actual transaction/ownership/settlement history.

For regulatory reporting however, the situation remains broadly similar to that of Scenario 1. This is because not all information collected under the various reporting regimes can be sourced from a record of settlements (an obvious example of this being EMIR trade reporting, where the only element sourceable from settlement history is the collateral reporting, as the derivative trade itself does not result in a settlement of an underlying asset). DLT participation, validation and information sharing would therefore be broadly similar in this respect to Scenario 1, with the need for an operational process for the submission of relevant information to the DLT that is different from the process for the settlement of assets.

10.2.3 Challenges and opportunities

The recent regulatory reporting requirements have led to a gradual harmonisation and adoption of standardised formats, processes, identifiers and delivery times of reports, to mention just a few achievements. Those achievements should be fostered further as sensible standards, and will remain a prerequisite of smoothly functioning markets even – or especially – in the event that DLT is applied in this space.

Use of a DLT to facilitate transaction reporting required under regulations would entail the ability to collate, validate and aggregate transactional information from a number of distinct off-DLT locations in a diverse range of formats. Participation in a DLT implementation designed to meet these requirements would therefore have to be broad. Validation would have to take place both on the level of the counterparties agreeing to the trade details (bilateral validation) and on the level of the network to ensure compliance with the reporting standards required for the specific class of derivatives transaction being reported (network/consensus validation).

Authorisation levels would require distinct, defined roles, including reporting participants, entities to whom reporting on behalf of other participants has been delegated, regulators and trade repositories. Reporting participants should only be

able to access and edit details of trades to which they are party. Delegated third-party reporters should only be able to access the details of those entities that have delegated reporting to such entities, and only for the time for which they are authorised to do so. If there is direct regulator access to the platform, regulators should only be able to view transactions of those entities which they are responsible for regulating (this normally being a question of geographical location).

Depending on the DLT model, reporting from a distributed ledger can involve either querying database table entries or analysing transactions recorded in a blockchain. In addition, modern transactional systems such as T2S are based on the double-entry system of bookkeeping, whereas blockchain ledgers structured as UTXOs are of the single-entry type and track single assets as they change beneficiary over time. Raw data from a DLT environment adds an additional source of complexity when such data needs to be processed, for instance in the above-mentioned example of the LCR. Therefore, reporting logic might need to be re-engineered to a considerable extent to cope with a single-entry ledger, or else the reporting output would need to be transformed into its corresponding double-entry view for use in business systems.

Currently, reporting is generally conducted on a batch basis to reduce the operational burden on end participants. If a DLT were envisaged to conduct real-time gross reporting without integration with data sources from which information is collected, the increased operational requirements on the reporting participants would be considerable.

In the course of implementation of DLT, it will be essential to have a solid concept around data protection and alignment with existing confidentiality requirements of different participants involved. It is crucial that the high level of transparency provided by DLT does not conflict with the high confidentiality levels required by financial market participants, as explained further in Chapter 13 on data privacy. This is especially true in the context of MiFIR, where market participants also have to report personal data.

DLTs used for reporting may have to be interoperable with other DLTs (potentially across different processes) to gain the biggest efficiencies. This would require agreements on data interoperability and policy interoperability, possibly along with adherence to international standards. As discussed in Chapter 14 on interoperability, this is a common feature that has emerged across a range of business cases considered in this report.

Benefits would be undermined if only some aspects of the lifecycle of securities were in the DLT environment, since there would be less certainty and more gaps in the history of the transactions. It is therefore necessary to consider the above in the system design, including the standardisation of reportable elements.

PART III – DLTS BEYOND TRANSACTION PROCESSING

11 Cyber resilience

11.1 Introduction

Cyber risk is defined in the "Guidance on cyber resilience for financial market infrastructures" published by the CPMI and IOSCO in 2016 (CPMI-IOSCO, 2016) as "the combination of the probability of an event occurring within the realm of an organisation's information assets, computer and communication resources and the consequences of that event for an organisation." The increasing reliance of financial markets on information and communication technologies in recent years has driven financial market participants and regulators to develop a proper understanding of cyber risk and the tools able to improve the resilience of their IT infrastructure.[59]

Market participants have been investing to protect customers and their businesses from cyber risk by engaging in a range of individual and collective actions. That has been substantiated in active monitoring of incidents and emerging threats, information sharing across the industry, establishment and maintenance of best practices related to the technology used, staff and customer education, control processes and governance, and self-assessment and third-party assessment to identify vulnerabilities of internal IT systems. This chapter focuses on the analysis of what changes DLT adoption could bring or require in comparison with mainstream database technology.

European public authorities have sought to encourage strong cyber security in financial markets by acting both in the role of catalyst and supervisor or overseer in order to protect consumers, ensure financial stability and maintain national security. Recent examples include the Network Information Security (NIS) Directive[60], which has brought major financial services organisations into the scope of thorough reporting requirements previously applied only to the telecommunications industry; the General Data Protection Regulation (GDPR[61]); certain aspects of the Second Payment Services Directive (PSD2[62]); the ECB cyber incident pilot; and the establishment of the European Cybercrime Centre. As part of its Digital Single Market Strategy, the European Commission has established the NIS platform in conjunction with the European Union Agency for Network and Information Security (ENISA) to exchange views about network and information security matters with a

59 CPMI-IOSCO (2016) defines a cyber resilience framework as the "policies, procedures and controls an FMI has established to identify, protect, detect, respond to and recover from the plausible sources of cyber risks it faces".

60 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19.7.2016, p. 1–30).

61 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).

62 Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (OJ L 337, 23.12.2015, p. 35–127).

number of financial services firms. Individual Member States have also taken action by setting specific frameworks for controlled intelligence-led cyber security tests, or advocating for legislation on provision of cyber-enabled services to be applied not only at the location of production but also at the location of delivery. A harmonised European approach is lacking in this respect.

At the global level, the CPMI and IOSCO issued their first guidance on cyber resilience for FMIs in 2016 (CPMI-IOSCO, 2016). Market participants are aware that cyber resilience needs to extend beyond the internal system of a service provider and its interface with the outside to additionally encompass the network of users and the technology they employ to interface with the infrastructure used for service provision. SWIFT, a provider of financial messaging services to 11,000 financial institutions in more than 200 countries, has initiated a global initiative under its customer security program to raise awareness of cyber risks and implement stricter cyber security standards and monitoring on its network and the wider infrastructure of its clients.

DLTs have been indicated as possible tools to improve the cyber resilience of the centrally managed database systems that financial market participants use to process transactions and to update asset holdings of their clients. Section 11.2.1 focuses on the possible impact of DLTs on the resilience of financial institutions and market infrastructures to cyber risk. Rather than describing out of context the intrinsic features of DLTs – which have been extensively highlighted in other discussions and publications on the same topic – this analysis focuses on the likely additional protection and risks brought by DLTs against a background where financial institutions, market infrastructures, and public authorities have acquired substantial awareness and developed a resilience framework against cyber threats.

A separate issue is that of possible specificities of DLT networks with regard to the definition of a cyber resilience framework. Any DLT platform for financial markets would indeed be part of the cyberspace and subject to cyber risk, but the possibility that a number of different institutions would jointly operate such a platform may require a bespoke approach to cyber resilience that starts with the definition of a proper governance structure and responsibilities across the different organisations involved. The fact that transaction processing in DLT networks involves a number of different separated entities adds a level of complexity to the governance of cyber risks. Section 11.2.2 addresses this issue and highlights the necessity for a cyber strategy in a DLT environment to encompass a multi-entity approach to the choice and ongoing upgrade path of hardware and software, configuration control, software development, testing, support and incident response processes, resilience and business continuity, and user access control.

11.2 Impact of potential DLT adoption

11.2.1 Impact on current processes

Database systems used in financial markets are designed to be resilient to cyber threats.[63] The guidance provided by CPMI-IOSCO (2016) in the field of financial market infrastructures suggests that design and implementation of a cyber resilience framework should be coordinated with other relevant stakeholders, with a view to: identifying critical assets and processes; setting up layers of technological protection to cyber threats; and detecting threats and responding to them in a way that allows service provision to be recovered. Whereas the broader issue of designing such a cyber resilience framework for DLT applications is touched upon in the following section, the focus here is on what features of a DLT network could change the capability of a FMI to contain and recover from an event that disrupts its ability to keep digital records of financial transaction and/or holdings.[64]

DLTs are often described as being able to resolve the issue of single point of failure – i.e. the possibility that the failure of a specific piece of hardware or software might prevent the provision of a service. However, this issue has been acknowledged for years and is already addressed in the mainstream database systems currently used by financial institutions and market infrastructures.

A key standard in this respect is set by CPMI-IOSCO (2012), which recommends that an FMI should be able to resume operation of its critical information systems within two hours of any disruptive events and to complete settlement by the end of the day of the disruption, even in extreme circumstances, including by using a secondary site (and a third site in exceptional situations). The reality is that FMIs often replicate data and processing capabilities in three or four data centres, at least one of which is located hundreds of kilometres away to increase the likelihood that it remains unaffected in the case of a regional disaster. Data recorded in the mainstream database system of an FMI are usually replicated between two (but possibly among several) data centres in the same region synchronously, allowing a redundant secondary infrastructure to remain constantly updated and to seamlessly recover service provision if the primary data centre is unavailable.[65] At least one other data centre, in a geographically distant site, is used to meet the provisions of PFMIs on operational risk by receiving data asynchronously from the primary site, so that core services can be resumed in the second region if large-scale issues make all sites in the first region unavailable.

---

63 CPMI-IOSCO (2016) defines a cyber threat as “a circumstance or event with the potential to intentionally or unintentionally exploit one or more vulnerabilities in an FMI’s systems, resulting in a loss of confidentiality, integrity or availability”.

64 This report is of a non-technical nature and describes the differences between DLTs on the one hand and mainstream technology on the other from a functional point of view. Any measurement of the ability of DLTs in general to contain and recover from disruptive events is unwarranted, and penetration tests should be performed on a specific DLT application across a broad range of set ups before drawing conclusions that could not in any case be applied generally to the wider DLT space.

65 Additional data centres could be updated synchronously if the relative expected gain in terms of availability of the system justified the associated cost.

The asynchronous nature of data replication among data centres across distinct regions means that some transactions accounted for in the primary centre (and in synchronised centres) have generally not been broadcast to other centres by the time the primary centre stops working. The delay between the moment when the latest snapshot of data recorded in the primary centre is sent to another region and the time when the primary centre stops working implies that, in the extreme case of a regional disruption, service provision is restored on the basis of information that does not take all transactions processed in the primary site into account.

The ability of an FMI database system to limit the gap between transactions processed in the primary site and transactions acknowledged by a backup site defines its recovery point objective (RPO). In the case of asynchronous replication, there will always be an RPO greater than zero.[66] If validation of record updates were to be based on a distributed consensus, as is the case in DLT applications, RPO could be reduced to zero in all nodes that have participated to validation of the latest transaction. The reason for this is that validation of record updates in a distributed ledger occurs among a set of nodes seeking consensus cooperatively, with a level of message and infrastructure redundancy that departs form the simpler master-slave replication of centralised database systems.

Recovery time objective (RTO) is a distinct measure of a database ability to recover its service, and its threshold is set at two hours by the PFMIs.[67] In the case of DLTs, validation of new transactions remains unaffected as long as the number of faulty validating nodes is low and the surviving ones that are aware of the latest update reach the necessary quorum. This means that a greater network of validating nodes is more resilient, and consensus algorithms requiring a lower quorum ensure availability of the service against failure of a higher number of nodes. However, a balance is required given that a) a high number of validating nodes increases latency and b) a low quorum increases the possibility that control over just a few validators will allow the ledger to be tampered with.[68]

Consensus algorithms used in DLT applications could potentially achieve synchronous replication of an FMI database on a larger number of data centres and regions. In fact, current database systems had the possibility of adopting synchronous replication across regions even before DLTs came into play. The overheads in terms of performances and costs – especially due to network traffic and redundancy of the infrastructure – have encouraged industry players to strike a balance between resources involved and the ensuing performance in terms of RPO and RTO. It remains to be seen whether DLTs under development are able to change the decisions made over this trade-off.

---

66 T2S has an RPO of less than two minutes in the event of a regional disaster.

67 T2S has a RTO of less than one hour in the event of primary site failure and less than two hours for business critical services in the event of a regional disaster.

68 Whereas a DLT network with strong governance should be able to deter or at least correct any data-tampering by a rogue validator, the systemic importance of FMIs and the legal consequences of book entry records act as a deterrent to even the temporary misrepresentation of asset holdings.

An aspect of DLTs that may sometime be overlooked is that they do not provide additional protection over mainstream technology in the case non-independent failures – i.e. failures affecting the operation of a large number of validating nodes at the same time. This is especially relevant in DLT models where a single network participant (a single point of failure in the network) provides a core service such as issuance of certificates or rubber-stamping of the latest agreed ledger. In that case, the same tools and procedures that are used in mainstream database technology – such as the above-mentioned master-slave replication in synchronous or asynchronous mode – still have a role to play.

11.2.2 DLT-enabled processes

One major innovation driving DLT adoption in financial markets is that this set of technologies allows different entities to collectively provide services related with financial data stored in the ledger even in the presence of untrusted parties. Notwithstanding the chance that a (limited) number of participants may misbehave, the rest of the network can continue processing transactions. Such a feature is useful not only when users of different participants deliberately breach the rules of the system but also, more importantly in the area of regulated financial markets, in the case of malfunctioning due to software, hardware or connectivity issues – so improving resilience to cyber threat. The guarantee that participants who behave correctly and are not affected by malfunctioning can collectively deliver their service despite issues coming from some network peers is called Byzantine fault tolerance.

DLTs cannot be adopted in the securities market unless they achieve levels of resilience that are demonstrably comparable with the technology and market infrastructure used within the industry today. Although a distributed architecture may improve resilience against localised breaches or infrastructure failures affecting specific nodes in the network, DLTs remain largely untested against the cyber threats faced by the securities industry and the added complexity of a shared IT infrastructure, and the issue of their cost-efficiency relative to mainstream technologies has not been given the consideration it deserves.[69]

Adoption of distributed consensus algorithms used in the updating of distributed ledgers within the securities market is predicated on the establishment of an overall enterprise grade architecture that can match existing security and resilience standards within the industry, and comply with all relevant internal bank policies, regulations and guidelines. In addition, the architecture would need to be based on clear data standards and a governance model to which all participants are willing to adhere.

In particular, given the distributed nature of a DLT network in which each node may be independently owned and managed by network participants, it must be ensured

[69] It shall be noted that, where we have seen breaches of DLT enabled networks, these appear to have occurred because of vulnerabilities in the wider DLT ecosystem and configuration control environment of unrestricted systems, rather than because of the underlying DLT technology and encryption techniques employed.

not only that each node is resilient to cyber risk, but also that the overall network architecture adopts technology, management and control standards that ensure the security of the network as a whole. While the use of distributed consensus should protect a DLT network from failures of (a limited number of) individual validating nodes, it brings no additional resilience against non-independent failures. Besides the above-mentioned possibility of a single point of failure in a DLT network, examples of non-independent failures may originate inter alia at the level of hardware, software, configuration and contagion.

The correct functioning of FMIs is essential in order to ultimately ensure economic growth and financial stability, since they are major channels through which liquidity and credit risks can be transferred to the financial markets, with potentially disastrous consequences for an entire economy. As cyber incidents affecting the information systems of FMIs can be a source of financial shocks and market disruptions, the guidance on cyber resilience issued with CPMI-IOSCO (2016) sets out preparation steps and other measures that FMIs should undertake in order to improve their cyber resilience capabilities and diminish escalating cyber threats that could put financial stability at risk.

Governance

Any network-wide cyber resilience framework above all needs clear governance to coordinate the efforts of the different actors involved. In the context of DLTs, this is particularly challenging, as it requires developers, validators, certificate authorities and gatekeepers to cooperate on a set of standards and appropriate governance arrangements. That would be hard to achieve in an unrestricted network, whereas accountable legal entities can work on a clear governance structure and allocate responsibilities for different functions such as the choice and ongoing upgrade path of hardware, operating systems and software, configuration control, software development, testing, support and incident response processes, resilience and business continuity, and user access control.

While existing market practices and processes are prescriptive about the way that market participants interact throughout the trade lifecycle, a governance model for DLT applications would need to reach more deeply and intrusively into the use and management of technology by participants in the system. The governance model would need to ensure clear change management and would have to establish mechanisms for:

- vetting and approving network participants: define a cyber resilience framework, establish an accredited evaluation capability, and establish an approval process that engages other network participants and relevant supervisors;
- monitoring compliance: establish an accredited capability for the ongoing review of network participant compliance with the cyber resilience framework and for the oversight of any agreed remediation actions;
- enforcing agreed standards: establish a compliance review board comprising network participant appointees, put in place a tiered regime of sanctions that

can be deployed against non-compliant network participants (e.g. fines, suspension from network), and ensure that network participants maintain their assets within the jurisdictional reach of the governance model as a condition of membership;

- managing conflict or disputes on a cross-border basis: establish an independent arbitration panel and process to oversee disputes between network participants, and enshrine the legal enforceability of its decisions within the rules of membership for each network participant;
- establishing liability in the event of cyber breach: define, develop, and maintain a cyber resilience framework aimed at addressing current and emerging cyber threats, establish a cyber risk management capability, and establish a cyber risk management board from among network participants;
- regulatory accountability: engage relevant supervisors to agree on a framework through which regulators will ensure accountability for the management of the central enabling functions of a DLT network.

Identification of critical assets and processes

To achieve a balance between the benefits and costs of distributed consensus, thus justifying the adoption of DLTs by market participants, it will be necessary to identify new and old risks.

The possible centralisation of some key processes, such as user authentication and upgrade of the infrastructure and protocol, introduces traditional types of risk that show the danger of focusing on distributed validation as an oversimplified solution to cyber risk.[70] A trade-off will need to be achieved between decentralisation of processes and loss of performance, as well as with the features of deterministic and probabilistic consensus algorithms.

The reliance on messaging among DLT network nodes may also create room for contagion of malicious software. The risk of contagion may be exacerbated in a DLT network where smart contracts are agreed in the form of executable code, which could be used to introduce malicious software that disrupts the operation of multiple nodes of a DLT network[71]. The intrinsically higher degree of record validation may become a double-edged sword in unrestricted DLT networks, where any participant can exploit a bug in a smart contract and thus take advantage at the expense of other users which, in the absence of proper governance and accountability, have no possibility of resolving the issue or punishing the malicious user.[72]

Resolution of issues related to bugs in the code could be achieved in a restricted network based on a governance model enshrining thorough and enforceable standards for security.

---

[70] The higher level of complication of DLT protocols constitutes an additional layer of risk. This could be resolved by having DLT applications more thoroughly tested.

[71] Besides cyber security concerns, smart contracts are also subject to the legal risk related to their enforcement.

[72] See for instance the DAO heist.

Protection of confidentiality, integrity and availability

At a time of widespread cyber awareness, adoption of DLTs in financial markets would represent an unprecedented opportunity for market actors to redesign IT systems that have been developed over the years from the ground up. DLT models under development should be designed to find the right balance between a set of possibly conflicting features such as confidentiality (see also Chapter 11), integrity and availability. For example, the integrity of data would certainly be maximised by storing full copies of a ledger in as many nodes as possible, whereas confidentiality of data would probably be better served by replication across a smaller number of fully trusted nodes. Unless a DLT solution is found that provides maximal protection to data confidentiality, data integrity and the availability of the system, it will be necessary to design a cyber resilience framework that sets the right balance along all these dimensions.

The management of risk stemming from interconnections among users of a DLT network is of key relevance. In order to ensure that all interested parties support the cyber resilience framework, it may be necessary to opt for a restricted network.

Detection

The potential use of DLTs in financial markets would be likely to expand the outermost layer of threat detection beyond a single institution. Without a central database manager that authorises users, receives and validates transaction requests, and updates records, DLT networks may need cooperation among different parties in the detection process while avoiding the moral hazard phenomenon whereby each participant may have an incentive to shift onto others the responsibility for reinforcing the system by means of costly investment in their local infrastructures.

Response and recovery

As explained in Section 11.2.1 above, DLT adoption could improve the RPO and RTO performance of information systems used by market participants. However, the potential benefits of distributed processing must not be reversed by the centralisation of some of its key functions.

Testing

Testing of a cyber resilience framework in DLT networks requires collaboration of all actors involved in the operation of the service. This would be a cross-entity task and would require agreement on what scenarios should be considered, with a high level of replicability of tests across the hardware and operating systems of all entities involved in management of data in the ledger.

11.2.3 Challenges and opportunities

Byzantine fault tolerance has hitherto been used in the provision of highly critical services in industries where the consequences of any breakdown of the IT system would be catastrophic, such as air traffic control. DLTs have the potential to introduce this additional level of resilience in the realm of securities post-trading. However, establishing standards that are acceptable to all existing market participants presents some challenges as it will require adaptation by participant firms to align their existing technology and risk management standards to those set out in the governance framework. An appropriately designed governance framework aimed at ensuring security and resilience of both the nodes and overall architecture of the DLT network is critical for preventing cyber attacks and can be effective in ensuring that a localised breach does not expose the entire network.

DLT adoption is currently limited to niche solutions. Regulators may recognise and endorse the governance framework within their regimes of oversight to ensure that financial stability objectives are maintained if and when DLT adoption expands.

One particular challenge for DLT deployment on a cross-border basis may arise from divergent cyber regulations that may make it difficult to maintain and enforce a cyber resilience framework within the governance structure of the network when different actors are based in different jurisdictions.

12 Digital identity in DLT networks

12.1 Introduction

A digital identity is information used by computer systems to represent an entity that can be a person, organisation, application or device. International Standard ISO/IEC 24760-1 defines identity[73] as a "set of attributes related to an entity" where the primary function of the concept of an attribute[74] is to be a "particular, well-defined aspect of the description of an entity in an identity management system".

The Electronic Identification and Authentication Services Regulation[75] defines the applicable interoperability framework for the recognition of electronic identities within the EU. The European Commission has published technical specifications and reference implementations of the interoperability nodes for the electronic identification[76] (eID) mechanisms for the technological infrastructure under the Connecting European Facility programme. Any EU Member State may notify its national eID means and will be bound to recognise those notified by others.

In the financial sector, digital identity is a key element to many current processes such as initial enrolment (or on-boarding), confirmation of investors' eligibility attributes, authentication and access to systems, signature and traceability. Due diligence and transparency obligations are provided for in the EU framework on KYC and AML,[77] which establishes procedures and transaction monitoring, as well as in MiFIR, which specifies the scope of transparency obligations.

Financial institutions carry out a number of identity processes covering the following aspects.

- Identity verification: for an individual this is based on confirmation of attributes such as name, date of birth and address using government-

[73] Identity is used to determine the transactions in which the entity can rightfully participate. Identities can be assigned to three main types of entity: individuals (e.g. customers or operators); legal entities (e.g. financial institutions, companies); and assets: items that are tangible or intangible (e.g. datasets, a security or any object whose characteristics can be confirmed, approved by a third party and managed).

[74] Identity attributes fall into three categories: (1) inherent attributes are intrinsic items such as an individual's date of birth and fingerprints; (2) accumulated attributes are items developed over time, such as health records and sports preferences; and (3) assigned attributes are items that can change and reflect relationships held with other bodies, such as email address and passport number.

[75] 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, pp. 73-114).

[76] eID is one of the tools used to ensure secure access to online services and to carry out electronic transactions with enhanced security protection.

[77] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (OJ L 141, 5.6.2015, pp. 73-117) and Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006 (OJ L 141, 5.6.2015, pp. 1-18).

issued, paper based credentials (increasingly these attributes can be verified via online mechanisms).

- Identity authentication: after identity verification, the individual receives credentials they can use to prove that they are the right person when attempting to access a service. These credentials usually include a user name and password plus a token or e-certificate for additional security (e.g. used to carry out a transaction).
- Regular KYC updates and AML controls/transaction processing (notably on transactions and global functioning of customer account).
- Risk management (e.g. use of identity data for measuring the credit risk of a given customer; also risk profile of a customer to ensure compliance with MiFIR regulation).

These current identity processes lead to a number of issues. Buy-side clients respond to multiple requests from bank partners for reference data and associated documents during initial on-boarding and updating. Banks have various standards and requirements for on-boarding new relationships, products and regions, and this leads to different document requirements for each bank updating and validating client information. Clients lack transparency on how their documents are used and how they are stored. Processes around identification, distribution, and secure management of reference data are complex and difficult to maintain. Specifically in the case of non-listed securities, registration and traceability are ensured by the issuing company and organised by its statutes. However, this process is not standardised and rests upon market participants for which client identification is not the core business and which may lack sufficient reliability. Anecdotal evidence shows that existing offers enabling issuing companies to subcontract the management of issued securities are not financially viable for relatively smaller companies, and this may be due in part to the high costs of identifying prospective investors.

Besides the above-mentioned KYC obligations, financial institutions and market infrastructures are also interested in the digital identity of their clients with a view to facilitating the provision of their services, for instance in the case of client credit ratings). In addition, ongoing developments in the realm of fintech are shifting the focus on the digital social identity of end clients to allow further improvement of service provision on the basis of their public interaction via the internet.

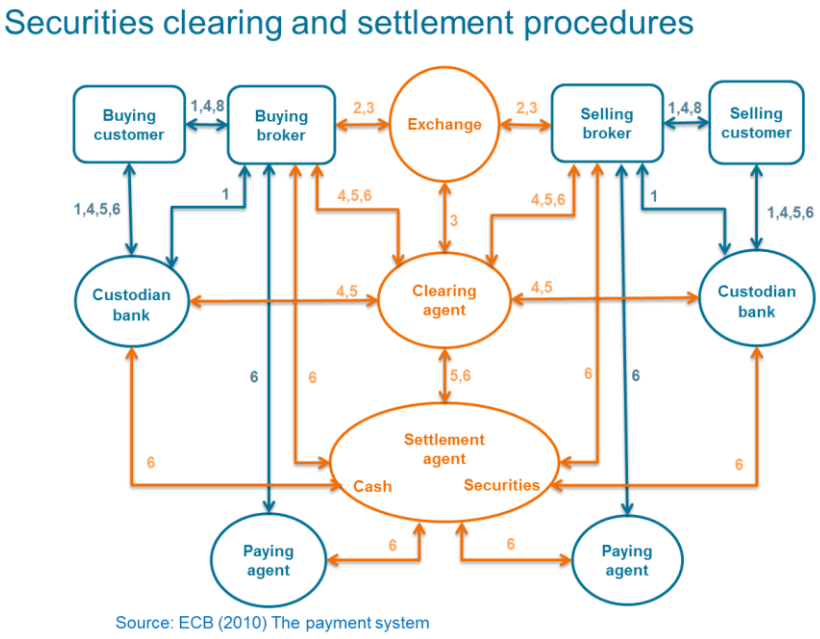
12.2 Impact of potential DLT adoption

12.2.1 Impact on current processes

Traceability of securities holdings is currently complicated by the multiplicity of intermediaries involved in a transaction process. The fragmentation of relevant information across intermediaries limits the traceability of securities holdings and makes it difficult to link them to their end beneficiaries. DLT solutions have been proposed to manage digital identities and to provide a single source of information

linking asset holdings at any level of the chain of intermediaries to the identities of market participants.

Figure 12
Entities involved in securities post-trade



Source: ECB (2010) The payment system

Step 1: the buyer and the seller place their orders with their respective brokers and/or custodian banks. Step 2: the brokers execute their clients' orders in the exchange. Step 3: the exchange sends the clearing agent and the brokers details of the transactions executed. Step 4: the brokers (both the buyer's and the seller's) send details of the trade to the clearing agent. Step 5: the clearing agent sends the brokers, custodians and settlement agent the securities balances and the fund balances. Step 6, the securities are delivered in exchange for funds.

12.2.2 DLT-enabled processes

The hash of investors' identity documents could be stored and validated in a distributed ledger. The purpose of such a solution is for customers to register their data on the blockchain. Once these data have been certified/checked, the corresponding digital identity can be shared among several financial intermediaries and market infrastructures.[78] These could then choose to accept certain validated subsets from each other, potentially speeding up KYC processing and reducing its cost.

[78] Without using DLTs, SWIFT proposed back in 2014 a customer identification service based on a common register where participating institutions input the data they collected on their customers or correspondents based on a harmonised format developed by SWIFT. Each institution is free to share these data with the institutions they choose. They can also ask for access to the data of their correspondents.

Some fintechs may also provide “connected services” that add data to a customer’s core identity. These fintechs could also provide the trusted identity to existing services (e.g. social media via APIs), and every transaction in such services could also reaffirm the identity and push metadata back into the core identity (e.g. employment, marital status).

Financial institutions do not own the information related to their clients, and the latter need to agree before such information is shared with other parties. DLT applications are being developed to facilitate information sharing with the consent of the clients by tokenising attributes of a digital identity and giving the possibility to the corresponding owner to send the information to different institutions once it has been validated in the distributed ledger. To avoid data privacy issues, some solutions are being developed that enable the DLT network to be used as a medium for sending the credentials to access documents stored in a secured non-DLT database or a hash that is stored by a trusted institution and that can be used by any entity to verify the authenticity of documents provided in an identification process, with no need to process them again.

12.2.3 Challenges and opportunities

It remains to be seen whether a distributed ledger is the best way to control access to data which may be held elsewhere. It could be argued that existing databases meeting high level security and access rights control requirements might indeed be more appropriate. However, as discussed in the paragraph below outlining the opportunities identified, a DLT may be particularly suitable for processes bringing together different stakeholders.

An identity system generally includes four key roles: users with identities; identity providers to verify users; so-called relying parties that require a user’s verified identity before allowing access to a service; and governance bodies to oversee the system.

Since multiple institutions may be involved in the validation of transactions related to a user, each of them could theoretically be responsible for identity checks. Some institutions could act as gatekeepers, but those that act only as validators might still be responsible for checking eligibility for a given transaction. One way to allow identity checks on a DLT network is to use a common digital identity scheme. This requires clear governance and allocation of roles and responsibilities.

Depending on the DLT model under consideration, market participants at different levels of the securities transaction value chain would need some level of portability of users’ identities.[79]

[79] The identity of beneficiary owners is known to their points of entry to financial markets but cannot be easily reused either by other institutions providing a similar service or at higher levels of the securities transactions value chain to allow know-your-customer’s-customer (KYCC) identity checks.

There is a risk of fragmentation due to the lack of established standards and agreed form of governance. Although open source codes may provide standards, there are many different open source codes, and making them available is not sufficient to ensure interoperability.

Business issues

The MADRE project,[80] where every participant holds a validating node, highlighted a relevant constraint for smaller institutions in terms of technological and, to a lesser extent, financial barriers, since participants would need to have the competences and resources to set up a node to participate in the blockchain, even if they carried out only a very limited number of transactions per year. This is an argument in favour of tiered networks, where some institutions are connected to the distributed ledger but do not validate.

Technical challenges

Currently, the deployment of a DLT application is more complex than in the case of a centralised architecture and requires that each participant installs and changes the settings of the software. Costs for participants may be higher, although the situation may change as a standardised and thoroughly tested DLT application becomes available.

Opportunities identified

For processes bringing together different stakeholders who wish to preserve their control over their internal processes but are ready to share data, or where such processes bring a distinct added value on shared data, then a distributed ledger seems to have more potential to connect these actors than a portal for example.

In general for identity management, blockchain has the potential for some useful applications (e.g. creating evidence for identity verification such as for individuals with no or limited evidence as well as for personal data stores) as well as some strong inherent characteristics such as chronology features.

By way of cryptography, it may also be possible to hold a small piece of data known to be confidential (or private key) and use it to demonstrate that an institution has explicitly sanctioned a particular piece of information (e.g. an ID document, an authorisation to trade in a given type of securities or the actual existence of the given security) without uncovering that information to another party. To this end, the confidential information is combined with the document in question (using a special mathematical function) to produce a signature. This may be freely distributed (usually, but not necessarily, with the document).

[80] This project brings together the Banque de France (BdF), Labo Blockchain and various banks. As part of their KYC obligation, each account holder institution examines the opportunity to grant its customer a SEPA creditor identifier (ICS). The BdF alone is competent to allocate the ICS. It carries out a number of manual controls based on evidence provided by the account holder institutions on behalf of their customers. The project aims to replace the current ICS management application with a blockchain by enabling the direct input of ICS requests by banks.

13 Data protection and professional secrecy

13.1 Introduction

Besides contractual obligations to protect clients' data, financial institutions and market infrastructures are subject to regulatory obligations on data privacy and professional secrecy aimed at both protecting the confidentiality of personal data and maintaining fair and competitive markets. Data privacy and professional secrecy are requirements laid down in a large regulatory corpus of EU and national provisions.

With regard to EU data protection law, the General Data Protection Regulation (GDPR) [81] refers to the protection of the personal data of natural persons.[82] Data processing[83] is allowed with the data subject's consent or under other circumstances (see Article 6 of the GDPR). No reference is made to data protection of legal persons, such as corporations and credit institutions. However, some Member States have extended the personal scope of the data protection rules to legal persons. Member States also have data protection rules as a result of the transposition of earlier directives on data protection into national law back in the 1990s, which creates a patchwork of rules on data protection across Europe.

Under the GDPR, not only must the private data of EU entities be protected and used only for legitimate data processing purposes, but any entity may also exercise a "right to be forgotten" by any data processor by having their private data deleted. These obligations apply to all data processors, irrespective of global location, that are processing the personal data of EU entities.

With regard to professional secrecy, no harmonised rule exists at EU level. EU law only provides for some cases where the identity of a person needs be disclosed and the national secrecy rules do not apply.[84]

---

81 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, pp. 1-88).

82 The same holds for Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119 4.5.2016, pp. 89-131).

83 Article 4(2) of the GDPR defines data processing as any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

84 See for instance Article 7(9) of the CSDR on settlement fails: "CSDs, CCPs and trading venues shall establish procedures that enable them to suspend in consultation with their respective competent authorities, any participant that fails consistently and systematically to deliver the financial instruments referred to in Article 5(1) on the intended settlement date and to disclose to the public its identity only after giving that participant the opportunity to submit its observations."

13.2 Impact of potential DLT adoption

13.2.1 Impact on current processes

Every market participant is currently responsible for the treatment of data pertaining to its clients' digital identity (see Chapter 12 for details on digital identity), holdings and transactions. The adoption of DLTs may require a different approach to data privacy if different legal entities acting as validators need to access such information to update records. Distributed validation often implies a level of transparency that is at odds with the data privacy obligations that financial institutions must observe to protect the confidentiality of their clients' personal and financial data.

Whereas initial DLT applications relied on the transparency of a fully public ledger to avoid the phenomenon of double-spending, a number of solutions have been developed over time to introduce some degree of data privacy in DLTs.

Within its governance framework, a DLT arrangement to be used in financial markets would require logical partitions that allowed only authorised access to encrypted personal and transaction data by market participants and regulators. However, encryption can only protect data to the extent permitted by state-of-the art technology at a particular point in time. With no need to consider the extreme scenario of quantum computing, it cannot be excluded that technological development might allow users who hold copies of an encrypted ledger to read its content at a later stage. This argument rules out the possibility of full replication of confidential data across different nodes.

The approach of using a restricted network can limit participants to known entities with whom there may be no data privacy concern. This approach restricts the number of participants allowed to read the record of transactions, while little compromise is made as to their processing time. However, the limited number of parties with which a financial institution may be willing to share its data limits the usability of even restricted DLT networks for the management of sensitive data – at least until a way is found to connect such narrow ledgers and to ensure their coherence without breaching their confidentiality.

Ensuring coherence of information held across private restricted ledgers is the objective of synchronised bilateral ledgers, which have been developed to allow a set of counterparties (usually two) to agree on transactional data and update them without sharing details with third parties. Validators in the DLT network only intervene to make sure that every UTXO is spent once, with no need to know the details of the corresponding transaction. Sidechains allow for some holdings to be frozen in the main, possibly public, distributed ledger, so that they can be transferred among trusted participants in a parallel restricted distributed ledger.

Other solutions would allow some degree of data privacy to be introduced by disguising information on a transaction or the accounts involved. The mixing approach allows multiple participants to jointly sign a transaction so that it should be impossible to track who sent what amount to whom. The ring signature approach

allows a participant's information to be hidden among a larger set of fictitious transactions. The stealth address approach allows for both parties to a transaction to agree on a destination address, without broadcasting trade information to the entire network, by opening a new address for the purpose of receiving that specific transaction.

Research is ongoing in the field of zero-knowledge proof to allow encrypted transaction data to be validated without decrypting their content.

In the absence of a suitable governance framework, accountability for data breaches may become unclear. A governance framework is therefore required that will be strong enough to maintain trust between the node owners, market participants, regulators and data owners by both upholding and enforcing measures able to ensure data privacy.

13.2.2 DLT-enabled processes

Public DLTs could be used as a public notary registry to time-stamp documents and ensure their authenticity when they are exchanged privately among parties who do not fully trust each other. The way this can happen is by storing in a distributed ledger the hash of those documents verified by a trusted party.

13.2.3 Challenges and opportunities

If it becomes possible to protect data stored in distributed ledgers, DLTs may present an opportunity to provide public notary services with no need for a central trusted institution.

However, data privacy in DLT arrangements is challenging both in terms of technology, since some DLT models are ruled out by issues concerning confidentiality and ability to delete past records, and governance, which is required to define clear responsibilities that can only be enforced in restricted networks.

A major concern related to the use of DLTs is how an operator will comply with the national provisions on professional secrecy. This is particularly true in cases where there is no proper governance arrangement ensuring that responsibilities over the operation of a DLT network are clear.

14 Interoperability in a DLT environment

14.1 Introduction

DLT and other fintech innovations provide opportunities to make financial market infrastructures more efficient. The capital markets union (CMU) project is a vision for post-trade services to be based on competition, transparency and choice.

In recent years, European market participants and public authorities have successfully made financial market infrastructures more efficient through post-trade harmonisation, integration and introduction of the T2S platform.

With the possibility of future DLT adoption, interoperability between the different generations of technology, providing choice and competition, may be a challenge. New DLT-based services that do not interoperate with the financial infrastructure we use today may lead to fragmentation. The fundamental consequences of using a distributed technology for the provision of post-trading services in securities markets are illustrated in the other chapters of this report. Existing and coming legislation – on non-discriminatory "access and interoperability" for trading, clearing and settlement, and continued harmonisation and standardisation – can mitigate fragmentation among today's infrastructures. The same concepts of access and interoperability must be applied to mitigate fragmentation among services based on DLT and those based on existing technology. Access and interoperability are essential to accelerate the integration of new and existing infrastructures.

It is useful to distinguish between different types of interoperability. The first type relates to connections between upstream and downstream services in a value chain, such as trading and clearing. The second type relates to arrangements between different suppliers that allow their respective customers to transact with each other laterally in the same part of the value chain, such as linkages between CSDs. Both *value chain* and *lateral* interoperability require non-discriminatory access to ensure a level playing field for a range of services offering a choice to consumers.

A practical example of a framework supporting interoperability in both directions is the European Commission's European Interoperability Framework[85] (EIF), which is part of the Digital Single Market[86]. It is aimed at improving the quality of European public services and create an environment where public administrations can collaborate digitally. The EIF is an enterprise-level interoperability framework covering the legal, organisational, semantic and technical aspects of public administration. It does not create competition and choice between different public administrations. The *enterprise* interoperability of the EIF facilitates the administrations' selection among competing vendors and provides the vendors with

[85] https://ec.europa.eu/isa2/eif

[86] https://ec.europa.eu/digital-single-market/en/policies/shaping-digital-single-market

"open access" to the different administrations across Europe so that vendors can compete on a level playing field.

Further details and examples of enterprise interoperability frameworks can be found in Appendix 2.

In financial markets, relevant regulations on non-discriminatory "access and interoperability" include:

MiFIR; Commission Delegated Regulation C(2016)3807[87]; and the CSDR, and specifically:

- Article 35 of MiFIR, Non-discriminatory access to a CCP;
- Article 36 of MiFIR, Non-discriminatory access to a trading venue;
- Article 38 of MiFIR, Access for third-country CCPs and trading venues;
- Articles 50-52 of the CSDR, Access between CSDs;
- Article 53, Access between a CSD and another market infrastructure.

14.2 Challenges and opportunities

With new DLT-based services running in parallel with traditional services for the same or interconnected asset classes, there will be a need for right of access and interoperability that in turn creates pressure to find integrated or federated solutions to minimise fragmentation and increase efficiency and choice. Access and interoperability require non-discriminatory access, technical standards and consistent regulations.

If sound applications of DLTs to mainstream securities markets become part of existing value chains through non-discriminatory access to existing financial infrastructure, they could make financial market infrastructures more efficient by means of better sharing of information and STP, and ultimately strengthen the CMU.

The European Commission communication entitled "A Digital Single Market Strategy for Europe"[88] has a specific section on interoperability and standardisation stating that "in the digital economy, interoperability means ensuring effective communication between digital components like devices, networks or data repositories. It also means connecting better along the supply chain or between industry and services sectors. It means more efficient connections across borders, between communities and between public services and authorities". That strategy is supported and made tangible through the EIF. This type of framework can be helpful in structuring challenges and solutions to interoperability between new DLT-based services and traditional services.

[87] Supplementing Regulation (EU) No 600/2014 of the European Parliament and of the Council with regard to regulatory technical standards on clearing access in respect of trading venues and central counterparties

[88] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192&from=EN

15 Potential impact of DLTs on T2S harmonisation and broader EU financial market integration

This concluding chapter draws on the analysis provided in the previous chapters of the report to assess the impact of potential DLT adoption on the integration of financial markets in Europe. As a general note, AMI-SeCo members agree that the adoption of DLT technologies cannot bring substantial benefits without common standards that are necessary to allow interoperability of business processes across distributed ledgers, as well as between DLT and non-DLT systems.

The importance of market integration is recognised by market participants and public authorities in Europe. On the regulatory side, harmonisation across Member States recently received new momentum in the form of the European Commission's CMU action plan[89]. With regard to business processes, the T2S project has brought considerable standardisation around the settlement layer.

The T2S platform allows participant CSDs to seamlessly update their respective records and that has made settlement of cross-border transactions as efficient as in the case of domestic ones. However, the T2S harmonisation work stream has been a key factor in this process by enabling T2S stakeholders (inter alia NCBs, CSDs and CSD participants) to agree on standards which facilitate safe and efficient cross-border settlement.[90] When discussing DLTs it is clear that, similarly to the T2S experience, besides the obvious requirement that technical solutions adopted to connect different participants must be interoperable from an IT perspective, harmonisation will be a necessary condition for the adoption of the new technologies across financial market participants in the post-trade area.

15.1 Impact of DLT adoption on T2S harmonisation activities

The analysis in the preceding chapters has shown that use of DLTs in the post-trade processing of securities transactions would introduce a number of innovations in the way market participants interact. This is true both in the case of technical standards and in the case of business interaction between legacy and newly enabled processes. This section focuses on the possibility that DLTs may affect the standards agreed by the T2S stakeholder community in the past. These standards have been the subject of ongoing harmonisation activities.

89 See https://ec.europa.eu/info/business-economy-euro/growth-and-investment/capital-markets-union/capital-markets-union-action-plan_en

90 In addition, the T2S harmonisation standards have become the de facto benchmark in the European post-trade ecosystem, also influencing developments in non-T2S markets.

Distributed ledgers are a type of database and can therefore store asset balances for a range of investors and intermediaries, either directly or indirectly, by keeping a historical log of transactions. DLTs can thus be used to manage investor accounts, at least from a functional point of view. The legal definition of a securities account, however, is not harmonised at the European level. The same is true with regard to the legal effects of records in a distributed ledger (e.g. whether a record creates, represents or evidences rights or other forms of entitlements in relation to securities) and to the legal nature of the securities recorded via DLTs (tokenised and digitised assets), which may differ across DLT models and jurisdictions. Lack of harmonisation in this respect may constitute an obstacle to DLT adoption in T2S markets, but the remainder of this section focuses on the impact of DLTs on the T2S harmonisation agenda, assuming that these can in fact be used by market participants and FMIs.

DLTs can in principle accommodate omnibus account structures (T2S harmonisation activity 13 – **Availability of omnibus accounts**) by means of sidechains, including for the provision of appropriate services on those accounts (T2S harmonisation activity 14 – **Restrictions on omnibus accounts**), possibly using smart contracts. Such technical feasibility means that agreed T2S standards could in principle be kept in the case of DLT adoption, but it does not ensure that developers and adopters of new technologies will take a unanimous decision in that respect. T2S has achieved market consensus for harmonised processes around settlement, and this achievement should be preserved by potential DLT solutions without reintroducing market fragmentation. It is of primary importance for market participants to join forces to ensure that new technological solutions are developed that recognise business needs, and that the fruitful collaboration that led to the successful launch of T2S is leveraged to foster integration as an enabler of safer and more efficient markets.

An example where DLT solutions currently under development appear to be diverging from standards agreed in the T2S community is that of securities and cash account numbering (T2S harmonisation activities 15 and 16 – **Securities accounts numbering and Dedicated cash account numbering**). Harmonised numbering facilitates identification of account holders and providers, and the same T2S standard could be used in a DLT environment. However, the use of public keys to identify DLT users may diverge from T2S standards. The concept of a settlement account number is indeed generally replaced, in a DLT environment, by that of public cryptographic keys, and the numbering based on public key cryptography is more complex than human-readable account structures. The necessity to share both protocols and data consistently across all DLT system nodes could make the use of the DLT public keys incompatible with T2S account numbering conventions.[91]

If DLT and non-DLT solutions are to coexist, as seems reasonable at least for some time in the case of DLT adoption, it will be necessary to ensure interoperability

[91] While human-readable account identifiers would still be desirable for various processes, these could be hidden from external parties either by keeping them off the DLT or using DLT system encryptions and permissions to hide them from third parties.

between the two approaches. There may be a need to provide different settlement instructions depending on the technology used, which may also require the use of ad hoc matching fields (T2S harmonisation activity 2 – **T2S mandatory matching fields**) when a market participant holds both DLT and non-DLT accounts. Whereas the agreement over a single and exhaustive list of matching fields allows T2S actors to access all T2S markets without managing divergent and mandatory specificities in the settlement transaction flow, coexistence of DLT- and non-DLT-enabled systems could reintroduce such specificities.

Without agreed standards, market integration could be further impacted by the need to interface platforms based on possibly incompatible technologies and adoption models.[92] In some cases, standardisation will be necessary only at the level of individual asset classes (T2S harmonisation activity 23 – **Securities amount data**).[93] However, the distributed nature of DLTs also requires a standardised way to allow instructions to be exchanged and validated via network communication, which may become a hurdle to interoperability with existing non-DLT systems if DLT systems adopt different standards. The use of a set of ISO 20022-compliant messages is part of the technical requirements for T2S actors' interaction with the T2S services (T2S harmonisation activity 1 – **T2S ISO 20022 messages**) and a possible DLT adoption by non-T2S systems that may wish to interoperate with T2S would probably require revision of the standards to include specificities such as execution of smart contracts. Timing of standardisation is a key strategic issue, and the process should be general and descriptive until a technology reaches maturity. On the one hand, if standards are set too early and without involving all interested parties then they may soon become obsolete, as the technological capabilities are still not fully understood. On the other hand, a lack of standards can create barriers to integration that may be difficult to overcome thereafter.

Some DLT implementations are of the single-entry type, looking more like a share registry than a set of accounts. A DLT application could replace and ultimately improve the process of registering holders of securities if the participants worked at the same level of beneficial ownership as the registry of investors requires. In cases where DLT participants held wallets that were equivalent to omnibus accounts, interaction with either existing registration systems or with DLT sidechains storing information at end-investor level could be envisaged. In the former case, each registration system would have to deal with the complexity of interfacing to a DLT network but could keep its national or functional specificities, with no need to introduce additional data in settlement instructions (T2S harmonisation activity 3 – **Interaction with T2S (registration procedures)**). The latter case would instead require standardisation of the DLT protocols used by omnibus account holders. In both cases, definition of appropriate standards is hindered by the presence of different models for shareholder transparency (e.g. regarding the owner of a

[92] For instance, DvP between two DLT models (or between DLT and non-DLT) would require each system to wait for the other to confirm booking of the relevant transaction that is subject to a possible withdrawal in the case of probabilistic consensus (see Chapter 1).

[93] The non-standardisation of amount data has no impact on settlement as long as only one rule is used for each ISIN in T2S (either nominal amount (FAMT) or quantity/units (UNIT)). In a DLT environment, the same would hold true.

registered instrument or investors' rights over the same asset) across European markets. Registration processes, and the mechanisms used to transmit registration information, vary considerably across Europe.[94]

The analysis carried out in preparation for this report has shown that settlement finality, a cornerstone of both financial stability and investor protection, is open to different interpretations among DLT developers and practitioners in the financial services industry. Whereas some define settlement finality from a technical point of view and attach its meaning to the technical immutability of an update of the relevant database[95], public authorities, financial institutions and market infrastructures are aware that different levels of finality can be attached at different legally defined moments. Finality is defined by the system operator under the applicable national law.

In T2S, all participants adhere to a harmonised definition of the moment of entry of transfer orders into the system (T2S harmonisation activity 7 – **Settlement finality I**), the moment of irrevocability of transfer orders (T2S harmonisation activity 8 – **Settlement finality II**), and the moment when the transfer of assets (i.e. record updates) becomes irrevocable and enforceable (T2S harmonisation activity 9 – **Settlement finality III**). A clear governance structure and an agreed set of legally binding rules, hence a restricted network of participants, are necessary in order to define such milestones in a DLT environment, too.

For most transactions, there will always need to be a designated system recognised by the EU public authorities to ensure that counterparties are protected against insolvency procedures. Unique settlement finality moments could be defined by the operator of a securities settlement system even in a DLT environment – taking into account technical and operational requirements that could introduce fragmentation among the settlement finality rules of different systems and that would hamper their ability to interoperate. For instance, in some DLT models an instruction cannot be cancelled unilaterally or bilaterally as soon as it is submitted for validation – which implies a stricter settlement finality rule than currently envisaged in the SFD – while at the same time its successful validation cannot ensure a subsequent cancellation in all DLT solutions (especially in the near future). In such cases, it seems to be a challenge to define irrevocability of the transfer of securities from a functional perspective. In other DLT models, an instruction that is sent to the network cannot be cancelled unilaterally before validation, and as soon as a sufficient number of nodes have validated it, the corresponding transfer of assets is irrevocable. This means that the three levels of settlement finality, as per current T2S terminology, are simultaneous. It is clear that interoperability among systems characterised by such different concepts of finality will be a challenge that it is impossible to resolve without further work.

---

94 Harmonisation would probably be even more challenging if the scope reached beyond Europe, as in the case of a global or multi-region DLT network.

95 As explained in Chapter 1, no distributed ledger is truly immutable. Immutability of each DLT application is only ensured under specific assumptions that cannot be applied generally to real-life situations.

Clear and common definitions of the different settlement finality moments are necessary to allow interoperability among systems and to promote market integration. This in turn restricts the range of DLT models that could be adopted by market participants. In the case of a CSD-operated DLT, the CSD cannot delegate responsibility and control over its core functions to third parties. A solution proposed by some developers is therefore that the licensed CSD operates a single node validating each update of the distributed ledger to define its irrevocability and enforceability. However, the necessity for a single institution to perfect the validation of a settlement instruction would thwart the potential benefits of DLTs and does not encourage their adoption. DLTs can at the same time ensure finality of settlement and interoperability among systems only if market participants, FMIs and public authorities can find a way to ensure the accountability and responsibilities of institutions involved in the operation of a DLT platform around a common agreed technical and governance framework, possibly by finding an appropriate design for restricted networks that use a type of consensus algorithm able to define clear moments for settlement finality. It may be necessary to harmonise some design and operational aspects of the DLT implementation, also considering how a combination of DLT systems and a non-DLT system such as T2S could interact.

Validating nodes need to be connected to the DLT network in order for the latter to function properly and provide its post-trade services. This suggests that harmonisation of the settlement day and a single calendar (T2S harmonisation activity 5 – **T2S schedule of the settlement day and calendar**) would remain necessary in the case of DLT adoption. On the one hand, institutions with validation responsibilities in a DLT network would need to align their schedule, or the system in which they participate may stop working. On the other hand, similarly to what happened in the past, lack of coordination among the opening times of different systems would make any link among different systems inefficient and risky[96] – an issue that is particularly important for two-leg transactions such as DvP. The T2S AG, predecessor of the AMI-SeCo with respect to T2S-related responsibilities, agreed at the outset of the T2S project that the full compliance of T2S markets with the T2S schedule and calendar would be a prerequisite for an efficient cross-CSD environment. If DLT solutions were to be used in a single geographical region such as Europe, defining a commonly shared standard among DLT network participants and market infrastructures adopting mainstream technologies would not seem a daunting task. Nevertheless, different operators may have different preferences, possibly driven by the business needs of their users. Furthermore, in a global or multi-region network, the only viable option to achieve true interoperability would be opening 24/7/365. It remains to be seen whether the industry will find a business case to support such a model, and the issue of agreeing on the cut-off for a business day would remain.

[96] The CSDR implementing technical standards, published by the European Securities and Markets Authority (ESMA) on 28 September 2015 and adopted in November 2016 by the European Commission, include the legal requirement that linked CSDs (in an interoperable link arrangement) "shall agree on equivalent standards concerning reconciliation, opening hours for the processing of the settlement and of the corporate actions and cut-off times".

In EU markets, the settlement cycle timeline for transferable securities executed on trading venues and settled in a securities settlement system is up to two days after the trading day, or T+2 (T2S harmonisation activity 12 – **Settlement cycles**).[97] The possibility of instantaneous settlement is often mentioned in debates over the features of a DLT-enabled securities market. Whereas instantaneous settlement is already available in T2S, the main reasons why the recent shortening of settlement cycles was limited to T+2 seem to be: (i) the lack of STP capabilities among the intermediaries involved in a transaction; and (ii) the liquidity benefits, i.e. the possibility for market participants to net their trades over a prolonged cycle and to only deliver on their netted obligations at the end of it. It is true that adoption of DLT solutions, if *fully interoperable* across all institutions involved, could allow STP and "settlement at trade". However, the costs borne by market participants in terms of additional liquidity would need to be considered.

A potential new market standard on settlement cycles should ideally be defined by the securities industry in advance, rather than new standards being accepted that may be technologically possible but could be problematic from a market perspective. A further point of concern from a market integration perspective is that, in the case of different STP technologies coexisting, such as a harmonised DLT model and legacy solutions involving lengthy manual reconciliation, there may be a need for such systems to interoperate, at least over a provisional period.

The establishment of a single settlement cycle in the EU was deemed crucial for T2S participants' technical infrastructures in terms of rationalising back-office activities as well as managing cross-border corporate actions. The harmonisation of settlement cycles has an impact on the processing of corporate actions since the deadlines for instructing relevant messages laid down in the market, as well as the T2S corporate actions standards, are based on the notion of the settlement cycle timeline. Encoding of automated procedures for corporate actions requires a high level of standardisation. To date, standardisation has been slowly implemented using mainstream technology (T2S harmonisation activities 6 and 18 – **T2S corporate actions standards and Corporate actions market standards**). In future, standards are likely to need even further detailed definition to allow the use of smart contract capabilities – e.g. taking a number of parameters into account for the taxation of dividend payments.

Lack of harmonisation with regard to tax withholding responsibilities across European markets (T2S harmonisation activity 20 – **Withholding tax procedures**) implies that tax relief at source can often be granted only with the involvement of a local intermediary, which would hinder the benefits brought by use of DLT in the field of corporate actions.[98] A preliminary analysis of tax processing has highlighted that complex procedures, such as pro rata temporis, could benefit from DLT implementation if considered in the system design. Native DLT assets, as well as

[97] The existence of different settlement cycles has no impact on the core settlement process in T2S since T2S is neutral in this respect and can accommodate different settlement cycles. However, in order to facilitate efficient cross-border settlement of entitlements (corporate actions on flows), the T2S community has strongly supported the harmonisation of settlement cycle rules in the EU.

[98] On this topic, see the CMU action on establishing a WHT Code of Conduct.

digitised/tokenised assets, can be tracked per individual unit or even fraction over time if they have been on the DLT for the entire period of history relevant to the tax calculation. This may support DLT implementations at end beneficial ownership level, or drive the development of tiered wallets capable of tracking transactions for tax reporting purposes without necessarily passing information via settlement messages (T2S harmonisation activity 4 – **Interaction with T2S (tax information requirements)**) but instead referring to the information relative to the account of the beneficial owner. A similar outcome can be expected in the case of portfolio transfers (T2S harmonisation activity 24 – **Portfolio transfer**), where the use of digital wallets holding the keys to all assets held by an investor would be likely to simplify the transfer of such assets among custodians only if the latter had access to the same distributed ledger or to interoperable ledgers.

The CSDR will provide for a fully harmonised **SDR** approach for Europe, complemented by a specific standard in T2S markets (T2S harmonisation activity 11). There is a risk that DLT settlement solutions could create different approaches to the settlement model and to the issue of settlement fails. DLT-enabled systems with potentially instantaneous settlement would require prefunding prior to the moment of trading (either with own assets or via lending agreements) to ensure that settlement fails were not possible. For any other settlement cycle, it should be noted that the CSDR approach to settlement discipline is heavily influenced by the current settlement models. If the functioning of new technologies affects settlement models to the point that DLT-enabled and non-DLT-enabled settlement systems are subject to different constraints even though they provide the same services under a common regulatory framework, amendments to regulations may eventually need to be considered to deal with those differences.

Potential solutions to allow T2S CSDs to interface DLT-enabled securities settlement systems with the T2S platform based on mainstream technology, possibly allowing DvP via standard RTGS dedicated cash accounts, may require the definition of new harmonisation activities to allow such connectivity. Such harmonisation activities could also concern the possible protocol used to interface the traditional system with non-DLT ones. The possible introduction of a variety of DLT-based payment systems might introduce the need to ensure technical interoperability between old and new systems dealing with commercial bank money. No negative impact on financial integration is foreseen in the realm of central bank money in the euro area, since a common DLT model would be developed if DLTs were to be deemed viable for Eurosystem market infrastructures in the future.

It is of primary importance for market participants to join forces to ensure that new technological solutions are developed in recognition of business needs, and that the fruitful collaboration that led to the successful launch of T2S is leveraged to foster integration as an enabler of safer and more efficient markets.

15.2 Impact on the wider EU financial integration agenda

Beyond its impact on T2S harmonisation activities, the potential use of DLTs would have implications for EU financial market integration and may require some adaptations.

The market may want to consider **ISO 20022** extension into smart contract initiation and coding, as well as DLT-specific concepts. Adoption of DLTs across markets would also require the adoption of a single standard identifier (e.g. product, legal entity and class) for each asset transacted using the network. To encourage future interoperability between a DLT network and existing market infrastructures, where the use of an identifier may vary according to the market, trading venue, geographical area and asset type, it is recommended that the ISIN standard be adopted by any DLT initiative.[99]

The use of an interoperable DLT by different market participants may bring efficiency gains for some services around the issuance process, such as information exchange, reporting and potentially auctioning.[100] The possibility to mobilise capital in Europe and to channel market-based financing to all companies, including SMEs, is part of the CMU action plan defined by the European Commission and supported by the Eurosystem. The use of DLT solutions, both by issuers and by financial intermediaries and market infrastructures, may reduce costs associated with the **issuance process** and ease access to capital markets. As a result, the flow of capital between investors and European companies could be facilitated, including for SMEs.

DLT adoption might also facilitate **shareholder identification** and reduce the costs of keeping a **shareholder register**, in particular cross-border. As a result, issuing companies could save on costs and might be encouraged to access capital markets. However, if this phenomenon reaches a large scale and its administration is left to the initiative of individual issuers, a number of diverse issuer-run DLT platforms might emerge that are also based on national legal specificities – possibly to the detriment of overall market efficiency.

All possible scenarios for DLT networks discussed above are possible. They are not mutually exclusive. This is also true for the multiple options for validation available in a DLT network designated as a settlement system for tradeable securities. For issuers and investors to have improved access to the capital markets, it is necessary for these models to be **interoperable** and for the same securities to be available through different mechanisms. Creating a post-trade environment where the accounts of different DLT networks would only coexist without interoperating is not an optimal outcome, as this would create a re-fragmented post-trade landscape requiring harmonisation.

[99] Unlike several other standards, ISINs decouple the concept of settlement location from the asset identifier.

[100] The collective safekeeping of securities in digital form (e.g. immobilisation or dematerialisation) is governed by different national legislations in Europe. It is necessary to review whether current legislation of different markets can already accommodate “tokenisation” and recording of asset holdings in the non-traditional database structures used in some DLT applications.

If DLTs were to be used in financial markets, the absence of a harmonised **digital identity** could hamper the development of pan-European solutions and could lead to fragmentation. The portability of any digital identity scheme fit for use in DLT applications across Member States needs to be ensured to promote the adoption of integrated DLT solutions. The identification of DLT network participants is necessary to allow processing of their transactions and could improve shareholder transparency, but the performance of KYC by all validators in a DLT network for each user would be highly inefficient, and it may be necessary to define who holds such responsibility – e.g. validator or operator – particularly in the case of interoperable DLT-enabled systems.

The use of DLT networks for the streamlining and standardisation of all communications on **corporate events** originating from issuers may be a powerful tool to ensure that a single "golden copy" of all corporate events is easily produced by the originators of such information and accessible to all interested parties and users.

Proper **governance** of any market infrastructure is important to ensure its safety and efficiency. It is even more important in the case of a DLT network, where different legal entities share the responsibility for at least some processes and data. The potential adoption of DLTs will require the development of appropriate governance to ensure that responsibilities for data handling are clear and that a cyber resilience framework can be adopted in a way that ensures full commitment by all network participants to the common good of data integrity and protection from external threats. Key stakeholders from public authorities, financial institutions and market infrastructures would need to develop a governance framework for restricted DLT networks. Ultimately it would be desirable to achieve industry-wide international agreement on the approach via the CPMI and IOSCO, as this would facilitate long-term interoperability and integration between securities markets globally.

Protecting currently achieved standards or even introducing further standards will be essential in order to keep markets efficient and avoid friction. Thought should be given to any interfacing systems, as DLT might not be applied as a solution on its own. Data uploading, processing and analysis are some examples where interfaces to different technology could still be required. For instance, both counterparties to a trade (these could be a financial or non-financial institution) that are subject to a reporting obligation would need to adopt the DLT in order to confirm the trade and to allow the reporting of such a trade.

It is important to note that a number of elements of a theoretically DLT-enabled financial market have to be properly designed and put together before DLT adoption can be considered a realistic possibility in the securities settlement space.

References

CPMI, *The role of central bank money in payment systems*, 2003.
http://www.bis.org/cpmi/publ/d55.pdf

CPMI, *Distributed ledger technology in payment, clearing and settlement. An analytical framework*, 2017.
http://www.bis.org/cpmi/publ/d157.pdf

CPMI-IOSCO, *Principles for financial market infrastructures*, 2012.
http://www.bis.org/cpmi/publ/d101a.pdf

CPMI-IOSCO, *Guidance on cyber resilience for financial market infrastructures*, 2016.
http://www.bis.org/cpmi/publ/d146.pdf

ESMA, Discussion Paper – The Distributed Ledger Technology Applied to Securities Markets, 2016.
https://www.esma.europa.eu/sites/default/files/library/dlt_report_-_esma50-1121423017-285.pdf

Euroclear and Slaughter and May, *Blockchain settlement – Regulation, innovation and application – Regulatory and legal aspects related to the use of distributed ledger technology in post-trade settlement*, 2016.
http://www.euroclear.com/en/campaigns/Blockchain-settlement-Regulation-innovation-and-application.html

European Commission, *Action Plan on Building a Capital Markets Union*, 2015.
http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52015DC0468

Godeffroy, J.-M., *T2S: in Europe and beyond*, 2012.
http://www.ecb.europa.eu/paym/t2s/pdf/T2S_beyond_Europe.pdf

Government Institutes, *Telecommunications: Glossary of Telecommunication Terms*, Ed. Rowman & Littlefield, 1997

Mersch, Y., *Distributed ledger technology – panacea or flash in the pan?*, 2016.
https://www.ecb.europa.eu/press/key/date/2016/html/sp160425_2.en.html

Mersch, Y., *Distributed Ledger Technology: role and relevance of the ECB*, 2016.
https://www.ecb.europa.eu/press/key/date/2016/html/sp161206.en.html

Nakamoto, S., *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008.
https://bitcoin.org/bitcoin.pdf

Pinna, A., *Distributed ledger technologies in financial markets?: An introduction and some points of interest for legal analysis*, in ESCB Legal Conference 2016, 2017.
https://www.ecb.europa.eu/pub/pdf/other/escblegalconference2016_201702.en.pdf?e2dea3a78485afe4c70d5d5010f368be

Appendix 1: Adoption scenarios

A number of **scenarios** have been defined so as to capture in the best way possible the different DLT adoption models' characteristics and their impact on the harmonisation and efficiency of securities markets. The following characteristics have been deemed useful for defining the applicability of each scenario to the different topics of interest:

- Scope: will a DLT be used for the whole securities market or only for some subsets? In the latter case, the focus moves onto the following "sub-characteristics":
  - Regulation: is the DLT used for securities subject to the main pieces of EU financial market regulation (tradeable securities) or is it used for less regulated niches of the market (non-tradeable securities)?
  - Asset classes: is the DLT network used for bonds and/or equities, for instance?
  - DLT asset: does the distributed ledger record native digital assets or a tokenised representation of securities that exist off-ledger?
- Service coverage: are all functions of a securities market provided by means of the DLT or is the latter applied to specific services only (e.g. issuance, settlement or asset servicing)?
- Geographical reach of the network: is the set of DLT securities and participants (e.g. operator and/or validators) limited to the EU or does it extend to the rest of the world?
- Responsibility: is governance and/or the validation in the DLT network provided by financial market infrastructures, financial intermediaries or non-financial entities?

The next section outlines the scenarios that DLT-TF members have agreed to use in the preparation of the report to capture relevant results in an efficient way and to provide a basis for the assessment of the impact of DLTs on harmonisation. The table at the end of this appendix provides a summary of all scenarios and characteristics that are deemed useful to be considered in the detailed analyses of each topic.

Scenarios used in this report

Chapter 2 on accounts

The legal entity with responsibility for maintaining information on securities holdings is deemed relevant for the analysis of securities accounts. Regulation is also important, as it defines which legal entities can provide such a service. This leads to five possible cases. Additional considerations may be relevant with regard to different asset classes.

Chapter 3 on issuance

The scope of application of a DLT network certainly matters with regard to the regulation applied to the set of assets to be recorded in the ledger of holdings. The governance and validation responsibilities might also be relevant owing to the application of different requirements, especially under national legislation. This leads to a total of five scenarios. Further consideration should be given to the differences between DLT asset types (tokenised vs. native). Other notes could make a reference to these differences where it is necessary to mention the nature of the assets transferred via the DLT network.

Chapter 4 on cash and delivery versus payment

Among the characteristics that have been identified in this chapter, geographical reach seems to apply in the case of both central bank money and commercial bank money, as it is possible that different types of money will be used in the ledger. This leads to two scenarios.

Chapter 5 on settlement finality

The scope of application of a DLT network certainly matters with regard to the regulations applied to the set of assets recorded in the ledger of holdings, since these regulations determine the range of entities that can be involved in the settlement of securities transactions. Governance and validation responsibilities are of interest owing to the different types of finality in the case of FMI vs. financial intermediaries (both tradeable and non-tradeable securities) as well as in cases where non-financial institutions are involved (e.g. the case of non-tradeable securities). This leads to a total of three scenarios to be analysed in the chapter for this topic.

Chapter 6 on settlement discipline

Responsibility for governance and validation matters, since applicability is limited to FMIs. This leads to two scenarios (FMI/non-FMI, including both financial intermediaries and non-financial entities). Non-financial entities would not be allowed to levy disciplinary fines as per current regulations (e.g. CSDR).

Chapter 7 on settlement day schedules and calendars

The geographical reach of the DLT network would be relevant since different regions have different time zones and bank holidays. This leads to two scenarios.

Chapter 8 on collateral management

The service coverage of a DLT network is relevant, since the latter could be used either exclusively to register collateral movements (for information/accounting purposes only) in the accounts of a collateral management service provider or additionally for settlement of collateral transactions among all market participants. This leads to two scenarios. It may be necessary to give further consideration to defining the scope of collateral management (in terms of asset classes) in a DLT network – including looking at DLT assets as a tokenised representation of physical assets.

Chapter 9 on asset servicing

The service coverage of a DLT network matters because the network could be used either as an information platform or in conjunction with the automated execution of payments and settlement. Additional considerations may be relevant with regard to the geographical reach and settlement cycle owing to the relevance of close-of-day holdings and different dates in the processing of corporate actions. Four scenarios in total need to be considered.

Chapter 10 on reporting

The service coverage of a DLT network is relevant since the latter could be used either to transmit information sourced from the non-DLT accounts or as a way to report transaction data directly as it is generated during settlement. This leads to two scenarios.

Chapter 11 on cyber resilience

The responsibility for governance and validation matters since different entities are subject to different assessment frameworks. That leads to two scenarios.

Chapter 12 on identity management

Scenarios are not deemed useful for this topic. Geographical reach might deserve a mention given the specificity of EU regulation.

Chapter 13 on data privacy

Scenarios are not deemed useful for this topic. Geographical reach might deserve a mention given to the specificity of EU regulation.

Chapter 14 on interoperability

Scenarios are not deemed useful for this topic.

	Topic	Characteristic 1: - Scope/regulation /asset class	Characteristic 2: - Service coverage	Characteristic 3: - Geographical reach of network	Characteristic 4: - Responsibility for validation	Scenarios to be analysed:
2	**Accounts**	Tradeable/non-tradeable; bonds/shares/ others	Characteristic not relevant	Characteristic not relevant	FMIs Fin. intermediaries Non-financial entities	1. Tradeable/FMI 2. Tradeable/fin. interm. 3. Non-tradeable/FMI 4. Non-tradeable/fin. interm. 5. Non-tradeable/non-fin. entity + considerations on asset classes
3	**Issuance**	Tradeable/non-tradeable	Primary issuance only Issuance & settlement/servici ng	Characteristic not relevant	FMIs Fin. intermediaries Non-financial entities	1. Tradeable/FMI 2. Tradeable/fin. interm. 3. Non-tradeable/FMI (not explicitly covered) 4. Non-tradeable/fin. interm. 5. Non-tradeable/non-fin. entity + considerations on service coverage
4	**Cash and delivery versus payment**	Characteristic not relevant	Assumption: DLT provides settlement services	EU only Global	Characteristic not relevant	1. EU only 2. Global
5	**Settlement finality**	Characteristic only relevant to determine possible role played by non-financial institution	Assumption: DLT provides settlement services	Characteristic not relevant	FMIs Fin. intermediaries Non-financial entities	1. FMI (tradeable and non-tradeable) 2. Fin. interm. (tradeable and non-tradeable) 3. Non-fin. entity (non-tradeable)
6	**Settlement discipline**	Characteristic not relevant	Characteristic not relevant	Characteristic not relevant	FMIs Fin. intermediaries Non-financial entities	1. FMI 2. Fin. interm. and non-fin. entity
7	**Schedule of day & calendar**	Characteristic not relevant	Characteristic not relevant	EU only Global	Characteristic not relevant	1. EU only 2. Global
8	**Collateral management**	Characteristic not relevant	DLT only for information sharing DLT used for info sharing and execution of settlements	Characteristic not relevant	Characteristic not relevant	1. Info only 2. Info & settlement + considerations on asset classes + considerations on DLT assets (tokenisation vs. native)
9	**Asset servicing**	Characteristic not relevant	DLT only for information sharing & comms DLT used for info	EU only Global	Characteristic not relevant	1. EU/info only 2. EU/info & settlement 3. Global/info only 4. Global/info &

	Topic	Characteristic 1: - Scope/regulation /asset class	Characteristic 2: - Service coverage	Characteristic 3: - Geographical reach of network	Characteristic 4: - Responsibility for validation	Scenarios to be analysed:
			sharing and execution of settlements			settlement
10	**Reporting**	Characteristic not relevant	DLT only for information sharing DLT used for info sharing and execution of settlements	Characteristic not relevant	Characteristic not relevant	1. Info only 2. Info & settlement
11	**Cyber resilience**	Characteristic not relevant	Characteristic not relevant	Characteristic not relevant	FMIs Fin. interm. Non-financial entities	3. FMI 4. Fin. interm. and non-fin. entity
12	**Identity management**	Characteristic not relevant	Characteristic not relevant	Characteristic not relevant	Characteristic not relevant	None + mention of geographical reach/jurisdictions
13	**Data privacy**	Characteristic not relevant	Characteristic not relevant	Characteristic not relevant	Characteristic not relevant	None + mention of geographical reach/jurisdictions
14	**Interopera-bility**	Characteristic not relevant	Characteristic not relevant	Characteristic not relevant	Characteristic not relevant	Characteristic not relevant

Appendix 2: Enterprise interoperability frameworks

In Chapter 14 on interoperability in a DLT environment, two types of interoperability are discussed. The first type describes connections between upstream and downstream services in a value chain, such as trading and clearing. The second type describes arrangements between different suppliers that allow their respective customers to transact with each other laterally in the same part of the value chain, such as linkages between CSDs.

In this appendix, two examples of interoperability frameworks are described. These can serve as templates for assessing the interoperability of fintech innovations with new business models on the one hand, and incumbent systems and business models on the other. The templates could also be used to assess interoperability between new competing fintech innovations. Where there is a low degree of interoperability, market fragmentation can be expected to increase, and vice-versa. An important aspect of an enterprise interoperability framework is its broader scope, encompassing not only technical interoperability but also business concerns, processes and concepts.

Introducing an interoperability framework

The enterprise interoperability of the European Interoperability Framework (EIF) is tailored to drive harmonisation in three types of interaction: administration to administration, administration to business and administration to citizen. The EIF may not be the ideal reference point for future DLT applications, which are not as clearly defined and are therefore uncertain.

An enterprise interoperability framework which caters for uncertainty is the international standard ISO 11354-2:2015[101] – "Advanced automation technologies and their applications — Requirements for establishing manufacturing enterprise process interoperability — Part 2: Maturity model for assessing enterprise interoperability". The model has three dimensions, namely concerns, barriers and approaches to interoperability.

Concerns over enterprise interoperability can be at:

- business level with vision, strategy, policy and legal aspects;
- process level with process models, tools and platforms;
- service level with service definitions and offerings;
- data level with data models and mapping.

[101] https://www.iso.org/obp/ui/fr/#iso:std:iso:11354:-2:ed-1:v1:en

Within those areas of concern, there can be barriers at:

- conceptual level with the use of different descriptive models;
- technological level with the use of different incompatible technological solutions;
- organisational level with the use of different organisational structures, responsibilities, rules and methods.

A fourth barrier that is not part of the ISO model could be considered, namely at **commercial** level with the use of various mechanisms to preserve market share and even possibly to create monopoly situations.

For each of the ISO model's 12 combinations of concerns and barriers, there are defined maturity levels available on the usual maturity scale of 0 ("unprepared") to 4 ("adaptive").

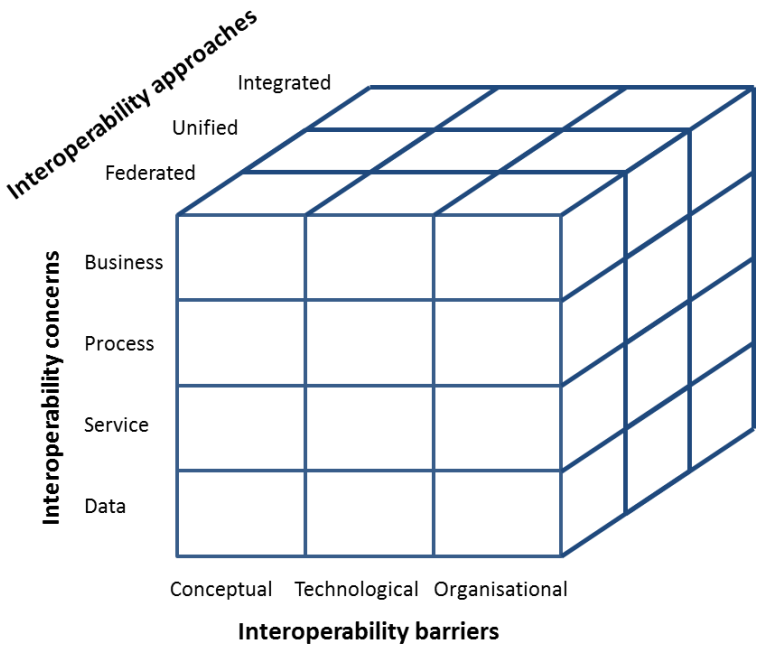
The model suggests summarising the maturity of an enterprise as in the table below, thus providing a single score:

	Conceptual	Technological	Organisational	Concern average
Business	0 - 4	0 - 4	0 - 4	= (C + T + O) / 3
Process	0 - 4	0 - 4	0 - 4	= (C + T + O) / 3
Service	0 - 4	0 - 4	0 - 4	= (C + T + O) / 3
Data	0 - 4	0 - 4	0 - 4	= (C + T + O) / 3
			Summary score	**= minimum of the above**

The approach to achieving enterprise interoperability can then be:

- federated, with nothing predefined but with dynamic adjustment – maturity level 4, more interoperability;
- unified, with common high level definitions – maturity level 3;
- integrated, with common formats, models and systems – maturity level 2, more integration.

The model is summarised by the following illustration:



The ISO enterprise interoperability model, although designed primarily for manufacturing processes, can nevertheless be useful as a framework in financial services. For example, it can be used to illustrate the implementation of T2S as a shared platform for CSDs. Here, many concerns have been raised, and barriers have been identified. Ultimately, these have been managed by means of an integrated approach, i.e. a common system platform, common legislation and international standards. T2S can be seen as having an interoperability maturity of "2 – aligned", providing an environment that is "integrated: the interoperation environment has a commonly agreed format (or standard) to which all other enterprises can build their system".

In trading, clearing and non-T2S settlement services where there is no common platform, the ISO model can likewise be used to illustrate value chain and lateral interoperability. MiFID II, MiFIR, EMIR and CSDR mandating interoperability and access, or clients demanding them, could be considered as a federal approach. It would require enterprises involved to have an interoperability maturity of at least 3 meaning "the enterprise is capable of using meta modelling to achieve the mapping needed to interoperate with other compatible enterprises".

The ISO enterprise interoperability framework can be refined and adapted for a range of uses. For example, a version of an enterprise interoperability framework has been applied for public administration with the EIF.

To have a fully functional tool, the mode needs to be further tailored to the purpose. The advantage of using a common model, such as the ISO standard, as a basis is that knowledge and expertise are available in the market, even outside the post-trade community. For example, the Digital Single Market Strategy leverages

enterprise architecture with ISA[2] [102], the EIF and the 30-minute interoperability assessment[103].

[102] https://ec.europa.eu/isa2/home_en

[103] https://ec.europa.eu/isa2/news/assess-interoperability-your-public-service-just-30-minutes_en

Appendix 3: Glossary

Address: A string of characters identifying a specific *node* or asset in the DLT network. The *public key* held by a *participant* can also be used as the participant's address.

Arrangement: "A generic term for any DLT-based application or implementation. An arrangement can be described in terms of its technical design and institutional structure. There is limited standardisation of terminology in the industry: emerging arrangements include systems, platforms and layers. Without seeking to establish specific definitions, a system is designed to stand alone and to fulfil its functions without interacting with any other arrangement. Another type of arrangement might be a platform, with applications being built on top of a common foundation to leverage functionality across multiple arrangements. Still other implementations of the technology might seek to act as a layer, with the emphasis on providing interconnectivity between arrangements." (From *Distributed ledger technology in payment, clearing and settlement – An analytical framework*, CPMI, 2017. http://www.bis.org/cpmi/publ/d157.pdf)

Block: The term used to define a batch of ledger updates in a *blockchain* environment.

Blockchain: A DLT model (and a type of data structure) where batches (*blocks*) of individual updates are linked sequentially together by means of cryptographic tools.

Consensus algorithm: A set of rules used in a *distributed ledger* environment – as well as in a network of decentralised traditional databases – to find agreement on what is the current status of the ledger at a specific point in time.

Consensus ledger: A DLT model where updated snapshots of participants' holding balances are agreed by *validators* by means of a *consensus algorithm*.

Currency: The specific form of *money* that is in general use within a country or monetary union.

Data centre: "Department in an enterprise that houses and maintains back-end information technology systems and data stores – its mainframes, servers and databases." (From the Gartner Information Technology glossary.)

Delegated consensus algorithm: A type of *consensus algorithm* where users of the DLT network delegate a set of *nodes* both to validate updates and to agree on what is the latest information.

Deterministic consensus algorithm: A type of *consensus algorithm* where at each round of validation a (possibly interchangeable) leader selects the update requests to be considered and asks the other validators in the network to agree on their validity. Such algorithms are called "deterministic" because a validated record update does not risk being declared void and overwritten by subsequent validation.

Digital financial asset: A *financial asset* that exists only in digital form.

Digitised (also **tokenised**) **financial asset**: A *financial asset* that exists outside the distributed ledger and that is represented in digital form in the *distributed ledger*.

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.

Distributed database: A type of database that allows users in different locations to access data stored and managed by a single central institution, often offering some or all users the possibility to propose updates.

DLT model: An implementation of DLTs that differs from others with regard to data structures, *consensus algorithms*, data transparency and roles played by its *participants*. A DLT model can be adopted by an *arrangement* to provide its services by means of a DLT.

DLT network: A set of *nodes* that share the management of a common set of information, which is recorded in a *distributed ledger.*

Double-spending transaction: A transaction attempting to transfer from a given sender assets that had already been transferred to another beneficiary.

End user: A *participant* that uses the DLT to keep its own data – i.e. to read information and submit updates.

Executable code: Software typically referring to machine language that is run by a computer in order to perform indicated tasks according to encoded instructions.

Financial asset: A contractual claim on an asset, the value of which is derived from the value attached to such underlying asset.

Fork: When two or more different *record updates* are agreed upon within distinct subsets of *nodes* connected to a *DLT network***.** A fork is said to emerge on the ledger when, starting from a common root or path of the ledger updates, some validators agree on a set of new transactions whereas others agree on a different one. Such a situation can only emerge if a *DLT model* is adopted that uses a *probabilistic consensus algorithm*.

Gatekeeper: A participant responsible for providing access to the network to end users. This involves for instance identifying the end user and providing access keys.

Hashing: In general, a hash is a mathematical function that processes input data of any size and returns output data of fixed length (the “hash”) by means of cryptographic techniques. Any new version of a *distributed ledger* includes the hash of its previous version. This makes it possible to validate the new version by checking that the fixed-length output corresponds to the hash included in the updated version.

Licit transaction: A transaction that complies with the rules of the DLT network managing the relative ledger, e.g. where the *participants* involved are correctly authenticated and hold the assets they are exchanging.

Money: Anything that is used widely to exchange value in transactions. See also *currency*.

Mainstream technology: Current technology that is widespread and generally used among participants in the financial market.

Native DLT asset: An asset that has value only in the DLT network and can be exchanged only among its *participants*, e.g. Bitcoin, Ether, Gas, etc.

Node: Any machine 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. A participant can be an *end user*, *validator* or *gatekeeper*.

Practical Byzantine fault tolerance (PBFT) algorithms: A set of *deterministic consensus algorithms* able to achieve consensus even if some limited components of a *distributed database* system (e.g. users, *nodes*, code, hardware) fail to follow the agreed protocol. Depending on the specific implementation of PBFT, a DLT model can withstand different failures. For instance, it may ensure the validation of all licit transactions or prevent validation of all non-licit transactions if the percentage of network *nodes* failing does not exceed a specified upper limit.

Private distributed ledger: A *distributed ledger* whose content is visible only to its participants or where specific parts of the data content are only visible to subsets of *participants*. See also *public distributed ledger.*

Private key (also secret key): One of two keys (the other being the *public key*) used in asymmetric cryptography and held privately by its owner. It is used by its owner either to digitally sign a message proving his/her authorship or to decrypt any message that was encrypted by another party using the relative public key.

Probabilistic consensus algorithm: A specific type of *consensus algorithm* where all validators work in parallel to process ledger update requests and then reach an agreement on whose validated set of updates should be accepted by all other users. They are called “probabilistic” since, typically, different validators will temporarily rely on different sets of information, causing conflicting versions of the ledger (*forks*), which are then reconciled at a later stage.

Proof of identity: A *consensus algorithm* that leverages the reputation of a *validator* to encourage it to update the ledger only with *licit transactions*. It is only applicable to *restricted networks* and can be scheduled via round robin (*round-robin scheduling)*.

Proof of stake (with collateral): A *probabilistic consensus algorithm* that uses economic incentives to encourage *validators* to update the ledger only with *licit transactions*. In practice, *participants* receive voting rights after posting some collateral either inside or outside the DLT network. Such collateral is forfeited if a validated transaction is found to be illicit ex post. See also *proof of stake* (*with native assets*).

Proof of stake (with native assets): A *probabilistic consensus algorithm* that uses economic incentives to encourage *validators* to update the ledger only with *licit transactions*. In practice, *participants* receive voting rights over the validity of new transactions in proportion to their holding of *native assets* in the network. If non-licit transactions are validated, or if licit transactions are not validated, the consequent loss of trust in the network should affect the validator via a drop in the value of its native asset holding. See also *proof of stake* (*with collateral*).

Proof of work: A *probabilistic consensus algorithm* that uses economic incentives to encourage *validators* to update the ledger only with *licit* transactions. In practice, it requires *participants* to bear the cost of electricity and hardware to validate transactions. It remunerates such effort only if validated transactions are confirmed as *licit* by other *participants* ex post.

Public distributed ledger: A distributed ledger whose content is publicly visible. See also *private distributed ledger*.

Public key: One of two keys used in public key cryptography (the other being the "*private key*") used in asymmetric cryptography and disclosed publicly by its owner. It is used by anyone either to encrypt messages that can then be decrypted only by the owner, or to verify that a message was signed by the owner. It can also be used as an *address* in the network and gives its owner access to the assets owned.

Record update: New information, or updates to information that already exists in a database.

Repudiation: Claim that a transaction that updated a record in a bookkeeping database did not happen.

Restricted network (also closed network): A DLT network is restricted when it can be accessed only by a specified set of *participants*, who can then be assigned different roles (hence also the use of the colloquial term "permissioned network"). See also *unrestricted network*.

Round-robin scheduling: A scheduling rule that allows individual *participants* to take turns when proposing updates for *validation*, with a view to avoiding working in parallel on concurrent and possibly incompatible updates.

Sidechain: An ancillary blockchain that interacts with a main reference blockchain. Participants have the opportunity to immobilise assets in the main blockchain (by sending them to an escrow service) and to have the corresponding amount of assets issued in the sidechain. This operation can usually be reversed to redeem assets from the sidechain and have them available in the main blockchain again.

Smart contracts: Algorithms that are coded in the ledger to update records when a set of conditions are met. It is unclear whether and how smart contracts might reflect legally binding contractual arrangements.

Sybil attack: Attempt to take over the management of a peer-to-peer system by generating a number of fictitious identities, especially in cases where each identity connected to the system can cast a vote.

Synchronised bilateral ledgers: A *DLT model* where counterparties can update the subset of information that refers directly to their bilateral activity (possibly with other elected parties also accessing these records) and make some of that information available to a broader set of *users*. *Validators* in the *DLT network* only intervene to make sure that every *unspent transaction output* is spent once, with no need for them to know the details of the corresponding transaction.

Unrestricted network (also open network): A *DLT network* that has no restrictions on participation (see also *restricted network*). Any entity has the possibility to become a *participant* without having to link its identity to its network *address* or *public key* in the network.

Unspent transaction output (UTXO): A transaction that is unspent by the participant to which it has been sent. It can be used as an input of a transaction, leading to new UTXOs becoming available to its recipients.

Validator: A *participant* that takes part in the consensus process adopted in a DLT network to confirm the validity of an update and to synchronise the information held by its *participants*.

Virtual currency: A digital representation of value which is not issued by a central bank, credit institution or e-money institution but which in some circumstances can be used as an alternative to money[104]. For instance, Bitcoin is a *digital financial asset* that is *native* and is used as a *virtual currency*.

Wallet: Software that stores private keys used to initiate transactions and provides additional customisable services, e.g. an overview of the asset balance and transaction history.

[104] See *Virtual currency schemes – a further analysis,* European Central Bank, 2015. https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf

Appendix 4: List of contributors

Composition of the Task Force on Distributed Ledger Technologies (DLT-TF) that prepared the AMI-SeCo report.

Participant's organisation	**Name of participant**	
Deutsche Bank	Mr. Stephen Lomas	(Chairperson)
European Central Bank	Mr. Andrea Pinna	(Rapporteur)

Members

AFME	Mr. Emmanuel Le Marois, Mr. Rob Morgan
Banque de France	Ms. Cécile Becuwe
BNP Paribas securities services	Mr. Alan Cameron
BNY Mellon	Mr. James Cunningham, Mr. James Higgins
Citi	Mr. Marcello Topa
Clearstream Banking	Mr. Robert Somogyi
European Central Bank	Mr. George Kalogeropoulos
European Central Counterparty	Mr. Björn Svensson
Euroclear	Mr. Luc Vantomme
Iberclear	Ms. Berta Ares Lomban, Ms. Yolanda Graña
JP Morgan	Mr. Alex Dockx
KBC	Mr. Dirk Hermans
Monte Titoli	Ms. Chiara Rossetti
Northern Trust	Mr. Michael Buzza
Société Générale	Mr. Alain Rocher
State Street Bank	Ms. Ines Cieslok, Mr. Swen Werner

Observers

ESMA	Ms. Anne Choné
European Commission	Mr. Lars Tomas Thorsén

Significant contributions were also made by Ms. Oana-Andreea Cristian and Ms. Georgia Koutsoukou (European Central Bank).