"THE USE OF DLT IN ISSUANCE AND POST-TRADE PROCESSES"

– Working draft report by the AMI-SeCo Fintech-TF –

DISCLAIMER: DRAFT VERSION (for comments/input only)

TABLE OF CONTENT

Executive summary

In the current fast-changing scenario, the adoption of Distributed-Ledger-Technology (DLT)-based solutions could bring opportunities and challenges to the financial ecosystem given its distinguishing features, such as its distributed nature and the use of cryptography for the functioning of its systems, including authentication and access.

Various institutional actors such as governments or central banks are actively undertaking initiatives in order to investigate and develop potential DLT-based use cases. In addition, a growing number of experimentations from different market players is taking place despite the current lack of common practices and standards. This could lead to an actual risk resulting in fragmentation in the market, with additional costs and missed opportunities to further progress in the Capital Market Union (CMU) Roadmap.

Market changes have prompted the Advisory Group on Market Infrastructures (AMIs) to launch an analysis by a community of stakeholder from the European post-trade industry in the form of this Fintech Task Force (Fintech-TF). The Fintech-TF made an initial assessment of the current DLT use in securities markets followed by an identification of possible use cases[1] with the objective of reviewing the conclusions from the former DLT/ Fintech Task Force (TF) common practices on DLT use while supporting the potential development of shared standards for interoperability in the post-trade area.

The Report focuses on current use cases for DLT-based equities and bonds given their market importance. It describes the different types of securities issuance in the market which are classified in 'Models' depending on how DLT can be used. It also covers the primary implications related to the use of DLT some or all those processes and extracts key features of operational models which leverage DLT to various degrees, based on some case studies.

It concludes that based on the evidence gathered, the adoption of DLT-based solutions could be driven by projected costs savings and efficiency gains. Similar to incumbent systems, interoperability remains critical, as it is needed to ensure both (i) migration from an incumbent system to a DLT-based system, and (ii) connection between DLT-based systems and incumbent systems on an ongoing basis.

However, DLT also may change the dynamics of current actors and their roles. Related life-cycle activities could be performed by different entities collectively for the network members and aggregated into smart contracts (e.g. a smart contact that issues a digital bond could be coded to interact with coded compliance/investor-country whitelists, as well as asset servicing activities that can be automated or human-triggered), which may require a discussion on the impact and compliance with the existing regulatory frameworks. For example, it is relevant to understand the relationship between smart contracts and the logic based on legal conditions.

It should be avoided that the adoption of DLT-based solutions could add new costs and barriers (e.g. legal validity of the token its transfer and settlement finality), to existing hurdles (e.g. fragmentation and interoperability issues), while benefiting from the use of innovative technologies and reducing or mitigating the related risks. For this to happen, a first step is

[1] https://www.ecb.europa.eu/paym/intro/publications/pdf/ecb.miptopical190111.en.pdf

the identification of a common technology neutral taxonomy to ensure clarity in terms of regulatory framework relative to different asset types.

The Report is structured as follows. **Chapter 1** outlines the regulatory, governance and interoperability issues which have been identified when using DLT. First it describes the key aspects in the regulatory framework that will be further identified in the analysis, highlights potential new roles in the DLT environment, as well as defines the concept of interoperability used in the Report. **Chapter 2** highlights the main identified practices by describing four fundamental models and their key implications. **Chapter 3** addresses key legal, technical and business implications resulting from the use of DLT at different stages of the securities life-cycle, starting from the issuance, custody and safekeeping and clearing and settlement

Examples identified in the market are presented in the Annexes: in particular, **Annex 1** completes the description of models and cases with concrete examples that are available in the market. **Annex 2** describes key examples of how interoperability can be ensured in DLT-based solutions.

Chapter 1: Regulatory, governance and interoperability considerations in a DLT environment

In light of previous work[2] of the AMI-SeCo and as follow-up deliverable in its monitoring of potential impact of financial innovation on securities post trade, this Report seeks to establish a common understanding from European stakeholders in the AMI-SeCo on how DLT can be used in the current regulatory system to issue new digital assets or represent existing ones (via tokens). It highlights the importance for DLT systems to be interoperable with non-DLT existing systems as well as across newly-established DLT-based solutions. The analysis has been conducted starting from practical examples that have already been developed and which allowed to identify two fundamental models of DLT adoption. This report includes a summary description of the most common current practices, as well as operational models observed during its monitoring exercise, and it is complemented by an overview of the regulatory obstacles identified.

Market standards are the critical connecting point between market needs and new technologies. Without market standards, and without compliance with the standards, the new technological solutions will fail, or lead to market fragmentation and barriers to entry for other market participants. In this vein, the majority of the initiatives focus on business rules and technical requirements (e.g. standards) of individual groups of market stakeholders. This could lead to a lack of interoperability between the different solutions and could hinder the opportunity and expected benefit of developments and improvements, as well as increase the risk of future fragmentation in the market.

Overall DLT could hold positive and negative aspects, as the use of new technologies, including DLT, could impact the existing systems and business cases, in terms of cost and opportunity and drivers of adoption (e.g. improving internal processes or reducing risks of single point of failure). Before joining or developing a new initiative based on DLT, companies should first address some preliminary issues, such as the business design and in some instances even the technical design of a solution, the articulation with the whole chain including final customers or legacy engines / tools which need to remain accessible.

The use of DLT would imply the same type of challenges the current environment endures (e.g. fragmentation and interoperability issues), and potentially add new ones (e.g. legal validity of tokens). DLT-based solutions should rely on strong governance where interests are aligned and well monitored, e.g. regarding settlement finality. In addition, the need for investments into internal IT applications and operational setup to support newly customized DLT-based products could reduce the ability of financial institutions to dedicate resources for R&D and new innovative products.

1.1 Regulatory framework

Key aspects related to issuance: taxonomy and nature of securities on DLT environment

The taxonomy of DLT based securities is a key component to understand the landscape of digital assets. However, the categorization of DLT based securities poses significant

[2] Please see the description of model 2c on page 14. In September 2017, the ECB published a Report of the Advisory Group on Market Infrastructures for Securities and Collateral (AMI-SeCo) which pointed out challenges and opportunities that using DLT could have for securities post-trading harmonization and to the wider EU financial market integration. The AMI-SeCo has continued monitoring the potential impacts of financial innovation on securities post-trade.

challenges for market regulators, and the regulatory framework should respect some key principles in order to ensure both legal certainty and efficiency in the issuance of securities on DLT environment.

The use of new technologies, including DLT, should not change the general principle that the identification of the category should refer to the intrinsic risks and characteristics of the activity and the reference market. Any definition adopted at international or European level should not refer to the use of a specific technology as a sole identifier of a new asset category. For instance, the relevant financial market regulation definition should consider the inherent financial and investment features of said asset in order to classify it as a financial instrument or, more broadly, as an investment product. Where initiatives leverage the DLT-based solutions, they should have a well-defined scope that provides clear guidance in order to reduce legal uncertainty.

It is also necessary to consider the intrinsic financial and investment characteristics of the product in order to analyse, understand and then classify it as a financial instrument or, more generally, as a financial or investment product. To this end, a classification should take into consideration elements of the asset model i.e if the asset at stake is referenced by a token referencing it on a distributed ledger and whether it confers any claims.[3] Another key feature for the identification of an asset at stake is the presence of an entity responsible for the issue and the intrinsic value represented by the token.[4]

The existence of a digital representation of value that can flow between independent systems (for instance an unspent transaction output - UTXO) does not preclude the development of other technologies able to form a digital asset which will exhibit similar properties but will not rely on DLT or what we deem modern cryptography.

In a previous work[5], AMI-SeCo clearly differentiated between the two concepts of i) security that is native to a distributed ledger (a native digital asset), and ii) reference to a security, which is already recorded outside a distributed ledger, by means of its representation (a token) via DLT. A “token” in a DLT environment represents a reference to an asset that originally has been issued and recorded in a conventional environment and is kept elsewhere (e.g. in registrar as it is done today). For this reason, in this report it is agreed that a “token” in the field of securities markets environment merely represents a security which has been issued and recorded in a CSD and remains kept in the legacy system or vault of the CSD. On the other side, a security that has been issued, recorded and kept solely on DLT as a “native digital asset” should be subject to the current regulatory framework in the very same way as security issued in the traditional environment.

To develop the use of DLTs and promote cross-border transactions in view of the realization of a European capital markets union, it is important to promote a harmonized approach to crypto-assets. At the national level[6], different jurisdictions have addressed this issue with new legislations, or with the aim of clarifying the existing regulatory framework (**Table 1**).

[3] Please see the description of model 2c on page 15.
[4] in line with the ECB's approach in its paper no. 230/2019, at https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op230~d57946be3b.en.pdf
[5] The potential impact of DLTs on securities post-trading harmonisation and on the wider EU financial market integration, available at https://www.ecb.europa.eu/paym/intro/governance/shared/pdf/201709_dlt_impact_on_harmonisation_and_integration.pdf
[6] For an overview, please see a recent article from ICMA, available at https://www.icmagroup.org/assets/documents/Regulatory/Quarterly_Reports/Articles/QR-article-DLT-related-legislation-and-regulatory-frameworks-130120.pdf

Table 1. Digital assets in national jurisdictions of some EU Member States[7].

France	With the ordinance 2017-1674[8], securities credited to the distributed ledger have the same legal effects as a book-entry form into securities accounts in terms of holding transfer.
Luxembourg	The law enables the use of secured distributed registers, electronic ledgers and databases for issuing, registration and circulation of securities without altering the regulatory framework and requirements for the security itself.[9]
Italy	A recent draft law[10] establishes that storing a document on DLT produces the legal effects of *"electronic time stamp"* as defined in article 41 eIDAS Regulation[11].

At European level, the recent proposal for a *Regulation on Markets in Crypto-Assets (MiCA)* as well as the proposal for a *Regulation on a Pilot Regime for market infrastructures based on distributed ledger technology* include functional definitions of crypto-assets and DLT-based securities. Therefore, the qualification of crypto-assets and DLT securities from a legal perspective would remain subject to national laws and may vary across different jurisdictions, taking into account that MiFID II does not provide for a harmonized definition of financial instrument.

Custody: the importance of the safekeeping of private keys

The concept of private keys is not new to the financial system as it is common to several solutions which do not rely on DLT. However, there is no common understanding of what the implications of DLT for custody services are in relation to crypto assets[12] and its custody. Some argue that it is primarily a matter of safekeeping private keys, others consider private keys only as a technical feature to produce digital signatures, as keys do not constitute either a means of safekeeping nor proof of ownership or provide for the validation of a transaction. This would mean that a custodian of private keys would not have the same ability as a custodian of traditional securities, on the basis of the specific design (e.g. regarding the setup of the transfer instruction). A key point for discussion is whether custody of tokens representing securities is limited to the safekeeping of private keys, which would change the current service model and related responsibilities. Rules for the safekeeping of private keys designed for individual custody of securities certificates could be designed with reference to know-your-customer (KYC), anti-money laundering and combating the financing of terrorism (AML/CFT), as well as consumer protection.

---

[7] In most of the EU countries, the legal basis for native digital assets does not yet exists, For example, in the case of Austria, the key laws applicable to securities offerings are i) Capital Markets Act (KMG); ii) Stock Exchange Act 2018 (BörseG 2018); and iii) Securities Supervision Act 2018 (WAG 2018).

[8] https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000036171908&categorieLien=id

[9] Luxemburg's Bill of Law 7363, available at https://www.chd.lu/wps/portal/public/Accueil/TravailALaChambre/Recherche/RoleDesAffaires?action=doDocpaDetails&backto=/wps/portal/public/Accueil/Actualite&id=7363 .

[10] Law No. 12/2019 of 11 February 2019 and Decree Law No. 135, (Decreto Semplificazioni) of 14 December 2018, available at https://www.gazzettaufficiale.it/eli/id/2019/02/12/19G00017/sg and at https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legge:2018-12-14;135!vig

[11] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN

[12] [WIP] Currently there is a lack of clear definition of crypto-assets, in addition to the one of custody although new initiatives by legislators at EU and national level aims to ensure a common understanding of this new type of asset recorded in digital form. At national level, the German government announced a draft law with a focus on the concept of electronic securities. In particular, BaFin has developed an approach that aims to provide for the issuance of securities on a distributed ledger without the application of laws on custody of paper certificates or centrally registered securities, as set out in the German Custody Act (DepotG) or the CSDR. Such issuance is possible with the concept of the so-called "Wertpapier sui generis" or "security of its own kind". A prerequisite of this approach is that the crypto-asset is "content wise" structured as a so-called "asset investment" (Vermögensanlage) . As regarding tokens, BaFin defines them as 'securities' available on DLT

Settlement: using DLT and its implications

The lack of recognition by each Member State of the equivalence between the digital form and the dematerialisation of the financial instrument may generate uncertainty for market participants and hinder cross-border transfer of digital securities. A harmonized approach with equivalence recognition between all Member States is essential for the development of DLT securities at EU level.

In general, rules on transfer of ownership and enforceability of rights are based on systems for holding "intermediated securities" and implies the existence of bilateral relationships (usually qualified as deposit/custody, depending on the applicable law) between the account holder and intermediaries along the custody chain. Rights on intermediated securities are usually constituted as sequence of crediting securities on the account of the holder / beneficial owner with the intermediary having a deposit relationship with the latter and the account holder / beneficial owner can transfer ownership rights only through intermediaries. The compatibility of such rules in a DLT context whereby usually ownership is supposed to be directly transferred peer-to-peer shall be tested and clarified, considering that these areas of law are largely based on local not harmonized legislation. For example, it may be difficult to locate an investor's entitlement in a bond which is held in a distributed network according to the widely established Place of the Relevant Intermediary Approach (PRIMA) approach[13]. This does not mean that ownership of securities on DLT cannot be intermediated: the difference to traditional custody chains would be that the intermediation in that case is expected to happen outside DLT network used for other parts of the settlement.

Finally, a DLT network requires different coordination and synchronisation processes for ensuring consistency and transparency on information that is provided. The production of information data as result of, for example, the consensus mechanism may result in the system itself to be the owner of the data produced in the forms of encrypted information, and, as consequence, to be responsible for the use of the data in compliance with the current regulatory framework (which may vary according to the jurisdiction(s) involved or even multiple jurisdictions at the same time). In this context, it remains to understand to what extent the GDPR would apply to network which may have nodes linked to participants from different jurisdictions.[14]

[13] See https://www.icmagroup.org/assets/documents/Regulatory/Quarterly_Reports/Articles/ICMA-QR-Q2-2019-Where-is-my-blockchain-bond-170220.pdf

[14] In particular, the data that is shared within the network may be subject to GDPR (e.g. article 4(1) in case, for example in blockchain, the public key is shared to the network and it is possible to link it to its identifiable owner. On the topic of relationship and compatibility of Blockchain and GDPR, please see https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445(ANN1)_EN.pdf

1.2 Governance of the DLT-based systems: Identified roles and functions

The transition from a legacy system to a DLT environment will imply a new model of communication, where a shared communication model enabled by DLT will replace the current sequential way of communicating and exchanging information; the new model will require the identification of new functions in the financial markets. Some of the relevant roles will depend on the specific configuration, key features and nature of the DLT network, as well as the status and jurisdiction of the providers. In this context, in addition to existing functions and roles, most of which are likely to 'survive' in DLT frameworks, additional ones are expected to emerge. This may have an impact on the services provided by incumbent and new entrants, as well as increase the overall complexity of their activities, as knowledge and adoption of DLT-based solutions matures. However, the expectation of benefits and efficiency gains can spur the provision of new services, which may require new skills and resources. It is very important to note that not all these roles and functions are likely to correspond to different legal entities: it seems realistic that one legal entity might incorporate two or more of these roles at the same time, which may also necessitate that regulators clarify which roles, if any, need to be separated, as well as how to apply conduct of business rules and manage conflicts of interest in this environment, and to whom they should apply. A high level description of functions in a DLT environment is provided below.

Issuer of digital assets

Compared to 'traditional' issuers, issuers of digital assets will need to adopt new technological structures and develop advanced competencies to fulfill their role of both issuers of digital securities and nodes of the DLT network. In order to ensure efficiency, issuers of digital assets could outsource this function and rely on a dealer or on a third party provider, especially for the issuance of native digital assets.

Asset Tokenizer

The function of the Asset Tokenizer could integrate the possibility of performing activities such as corporate actions and executing of dividend payments in the smart contract code. In a scenario where the security is issued in a legacy system and then it is transferred on a DLT environment with the issuance of a token, the Asset Tokenizer plays a fundamental role in the management of corporate actions with smart contracts and in the issuance of tokens, which represent the security, and it ensures the regulatory compliance of the process according to the applicable law.

Provider of custody services for digital assets and tokens

In a DLT network, the deposit of assets and tokens should ensure asset protection, handling of positions, accurate records in case of continuity issues, cyber-attacks, system disruptions, bankruptcy and should facilitate consensus on transactions. As digital assets emerge, existing tools for custody may require the deployment of new technical solutions while adapting its offering to address the risk of misappropriation of those digital assets. One of these activities could be the safeguarding of private keys, which are used to conduct transactions or access digital assets. In this setting, there would be a private key which is used by the custodian to operate the wallet; however, it could not / should not be allowed to operate the digital assets contained therein (which will require another private key). However custodians may choose to use the keys of their own wallets and provide similar services with the aim of conducting transactions and controlling the use and transfer of those specific assets. The actual investor/asset-protection roles of a digital asset custodian are likely to

differ depending on the type of digital assets and DLT used. Furthermore, access methods and points can change over time, with clients potentially connecting directly into such P2P systems, and the role custodians play in the market may evolve from custody of financial instruments to ‘data and information custody’. Network participants would have to be established who controls input into and access to the information, namely how dual instructions, by non-authorised parties, information leakage and theft can be avoided.

Trading and settlement of digital assets and tokens

The price discovery remains a key function of a trading venue even in a DLT environment, although how this is performed may deeply change. In addition to the trading functions, settling for trade “on chain” may have different features and may require additional skills and authorisations.

1.3 Interoperability of DLT-based solutions

The uptake of a DLT-based solution will be influenced by the possibility to interact with the legacy environment, in the entire life-cycle of assets. The current lack of interoperability in the majority of the DLT-based solutions may give rise to market fragmentation or fragmented liquid pools. This report covers two types of Interoperability, one that relates to the level of interaction with legacy system and another one that refers to interactions between different DLT networks.

In general, standardisation and common rules on a broader set of features and technical aspects is needed for the different systems to interact one with the other in a smooth manner. Specialised technology firms have developed tailored DLT-based solutions, which however may vary significantly in terms of scope, connection speed, scalability or fault tolerance.[15]

1.3.1 Types of interoperability

1.3.1.1 Interoperability between conventional and DLT systems (integration)

The challenge of integrating newly established DLT-based solutions with legacy systems persists but new solutions appear to be gaining traction.[16]

In this exploratory phase, a major challenge for a DLT-based solution is to accomodate for manual processes and transactions. If a process is not automated, the DLT may be not able to move it into a distributed ledger. Besides the data sources must be interacted with secure mechanisms like oracles, which act as an interface between on-chain and off-chain and all interactions are digitally signed to provide a basic level of accountability.

Another critical challenge for integration of DLT in legacy systems could be the costs and the limited pool of qualified human capital to lead DLT-based projects.[17] Another issues are inherently limited data sources, as the DLT can only access data stored that are available on the chain. In addition, a key challenge of integration is to overcome the complexity of allowing smart contracts to accept off-chain data sources with respect to security models.

Regardless of the technology, integrating in existing architecture is necessary to assure smooth transition and preventing the creation of another separate technology stack. Besides, it is important to gain efficiency via rationalizing duplicated infrastructure (legacy system) with DLT adoption and reducing costly reconciliation processes. For example, a single data version instead of duplicated data (DLT and legacy system), could reduce costs.[18]

Interoperability between DLT networks and legacy/existing infrastructure can be achieved through, among others, the use of smart contracts in order to transfer financial data on-chain and underpin automated workflows (if X off-chain, then Y on-chain). There are different solutions that can be undertaken for ensuring interoperability of DLT-based solutions with conventional system, such as via APIs i.e. for digital data to flow bi-directionally between the

[15] For example, technology firms such as Microsoft and TCS have also developed proprietary application programming interfaces (APIs) to facilitate interoperability between their respective DLT networks and the existing infrastructure, for example, TCS's Quartz Gateway or Microsoft's Azure Blockchain Workbench API. See https://www.tcs.com/content/dam/tcs-bancs/pdf/bancsprotected/Quartz-Blockchain-Aug-2018.pdf and https://docs.microsoft.com/en-us/rest/api/azure-blockchain-workbench/

[16] https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/risk/deloitte-nl-risk-blockchain-control-principles-in-fsi.pdf

[17] https://www.ifc.org/wps/wcm/connect/2106d1c6-5361-41cd-86c2-f7d16c510e9f/201901-IFC-EMCompass-Blockchain-Report.pdf?MOD=AJPERES&CVID=mxYj-sA

[18] https://www2.deloitte.com/content/dam/Deloitte/us/Documents/financial-services/future-of-post-trade.pdf

DLT network and existing infrastructure. For interoperability to work, the different networks can also operate on a set of commonly accepted data definitions, transaction formats and processing logic. New technological intermediators between existing and infrastructures based on DLT can be required to ensure integrity related to double spend and authorisation / digital identity. In any case, introducing "message broker" type of intermediators may add costs, latency times and inefficiencies.

1.3.1.2 Interoperability between different DLT-based systems

A fundamental challenge lies in the diversity of DLT networks, many of which have been developed in isolation for specific use cases. In particular, key differences encompass i) data records, on-chain v. off-chain; ii) data structure and transaction protocols; iii) consensus algorithms and data distribution; iv) distributed applications (i.e. smart contracts). In the course of the Report, interoperability between DLT networks is divided into two broad sub-categories according to its purpose.

First, trusted third-party authorities can be used to validate transactions or information. In particular three examples that can be highlighted are i) centralised or notary schemes; ii) sidechains or relay schemes; iii) Hash locking.[19]

Second, interoperability can be ensured via the creation of a direct link between DLT networks through other systems or smart contracts.[20] Today, one of key obstacles to the broader adoption of DLT-based solutions is the lack of standards which prevents a multitude of fragmented systems to reach scalability and efficiency gains, with positive network effects.[21].

From an operational perspective, two main categories can be distinguished: i) trusted bridging (with the involvement or an intermediary and ii) trustless bridging, where there is no need for any third party involvement for the successful use of the solution.[22]

As the industry participants are presently building their own DLT-based systems, there is a risk of incompatibility between the different systems, potentially leading to fragmentation. For example, if each market participant develops its own solution that is not compatible with other systems, instead of reducing operational risks, these risks are likely to increase them. Standardized rules for such security tokens (e.g. transferability) are needed and can be ensured in two main ways.

In a more direct manner, standards and common rules (e.g. for messaging) that are the same for the two systems can contribute to a smooth interactions during the issuance processes. In a more indirect, intermediated manner, an interface can be provided (also by third party providers) and standards are ensured. For example, in the context of a consortium for specific use cases, and in which new entrants (with DLT-based business) and incumbents (that might be more hesitant regarding investing in the technology) have to

[19] For more details on these three types, please see the Glossary.
[20] European Blockchain Observatory and Forum: Scalability, interoperability and sustainability of blockchains, available at: https://www.eublockchainforum.eu/sites/default/files/reports/report_scalaibility_06_03_2019.pdf
[21] In this regard, two concept of interoperability are relevant in the presentation of these examples, namely semantic vis-á-vis syntactic interoperability. For more details on the differences, please see the Glossary.
[22] In this regard, please see the difference between i) Trusted bridging: takes places with the involvement of an intermediating third party fulfilling the role of a bridge. It requires participants to trust the intermediary during the entire process; ii) Trustless bridging: takes place without the involvement of any intermediary. It requires more complex arrangements and significantly higher development effort from than trusted bridging. For concrete examples on both trusted and trustless bridging, please see Annex II.

cooperate as participants. This can be the case when one participant developed only one of the two systems and must nevertheless interact with other participants which base their business on both systems (such in case of Model 2b).

1.3.2 The evaluation of interoperability solutions: key properties

For the evaluation of interoperability solutions, there are several key properties which help to distinguish between solutions and related impacts:[23]

- Functionalities in form of: i) token and asset portability[24]; ii) Delivery versus Payment (DvP) or Payment versus Payments (PvP)[25] via smart contracts; iii) cross-chain oracles accessing data from other ledgers via smart contracts; iv) cross-chain asset encumbrance.[26]
- Reach, i.e. the direction, in which the ledgers can interoperate, because some ledgers only enable one-way interoperability.
- Scope, which relates to the state that is stored in case of interoperability. A permissioned ledger only stores state at a limited number of participants, while unrestricted ledgers enable wide and open access to the information from the ledger.
- Scalability: the term refers to the number of transactions that a network can process in a defined period of time (e.g. a second). This depends on the interoperability solution or the ledger, which connects to the solution.
- The update function (consensus mechanism), which defines how the network on which the ledger operates achieves consensus[27].
- Costs: set-up and maintenance of infrastructures require investment for ensuring interoperability among systems, potentially affecting the concrete adoption of DLT for future solutions. At the same time, the execution of transactions could incur fees which may differ depending on the specific DLT-based system and commercial arrangements.
- Development: As the research and development of DLT is in progress, there could be many changes in the future that could affect the interoperability between ledgers, e.g. if ledger X is upgraded, it may need to wait for ledger Y to reach consensus.

[23] https://www.ingwb.com/media/2667864/assessing-interoperability-solutions-for-distributed-ledgers.pdf
[24] Cross chain oracles and Cross chain asset encumbrance can be performed by notary and in relay schemes (one- and two-way). Atomic swaps can fulfil notary, relay (two-way) schemes and hash-locking (three-way).
[25] The automatic transfer of assets when specific conditions are fulfilled via the use of smart contracts is defined Atomic Swap. One the topic, please see ECB-BoJ joint report on Cross-border Payments, https://www.ecb.europa.eu/paym/intro/publications/pdf/ecb.miptopical170101.en.pdf
[26] In this case, the assets are stored and locked on the ledger until certain conditions are fulfilled
[27] There are two main categories: deterministic consensus and probabilistic consensus. See in the Glossary.

Chapter 2: Identified practices of securities issuance or recording and post-trade handling in a DLT environment and key implications

On the basis of market initiatives and practices included in the Fintech-TF monitoring exercise, the report identifies two main models to enable securities in a DLT environment and providing interoperability with conventional systems:

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

A summary description of the initiatives is provided in the Annex, based on the information publicly available or collected by Fintech-TF members

Model 1 – Securities issued as native digital assets

Under this scenario, securities do not have any other representation outside the DLT network: the ledger where the native digital assets are recorded would constitute the only and the relevant book-keeping system itself.

From a purely operational perspective, the native digital assets could be **publicly** traded on conventional execution venues; however, to date Model 1 has been used mainly for the purpose of bespoke Over The Counter (OTC) transactions or in the form of private placements.

The implementation of this model is reliant on the applicable regulatory framework which should enable issuance of securities through DLT. Examples from different market initiatives are included in **Annex 1**.

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

Under this scenario, securities were initially issued within traditional system and afterwards enabled in a DLT environment. Many examples of this model already exist. Some of these initiatives are led by incumbent players or consortia. Others originate from new entrants (e.g. start-ups) that might currently be not regulated.

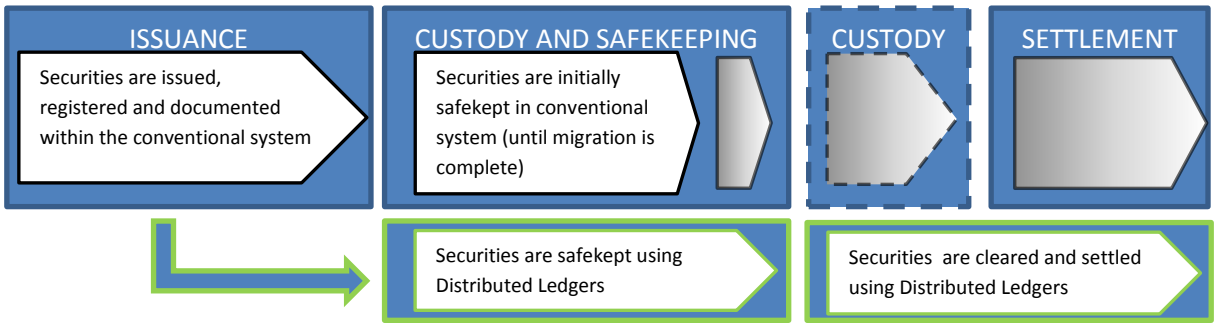
The identified use cases can be broken down into the following three different solutions for enabling securities on a DLT under Model 2:

- **Model 2a**: Securities recorded in a legacy system and fully migrated to a DLT (without the issuance of a token);
- **Model 2b**: Bridging legacy and DLT systems to issue and record tradeable securities; and
- **Model 2c**: Securities recorded in the conventional system, but referenced by a token in DLT environment.

Model 2a – One way: securities recorded in a conventional system and migrated to a DLT-based solution

This scenario combines both elements of already existing systems and opportunities provided by the use of DLT. The securities are initially issued and recorded in the legacy system (which then remains responsible for the processing of relevant events of the securities lifecycle) while custody activities and settlement are arranged with the use of DLT.

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



Model 2b – Two ways: bridging conventional and DLT-based systems to issue and record digital financial assets

This model assumes that assets are made available either in conventional system or in the DLT environment. In particular, securities are issued and recorded using the incumbent system and custody and settlement performed on both conventional and distributed ledger. As a result, a parallel system is provided in order to settle trades in the securities both in the incumbent and the DLT-based systems. It is also possible that one of the two systems is used for performing the main phases of the securities lifecycle such as the issuance, custody, clearing and settlement take place in the incumbent system, while specific parts of the process are performed in the other. For this to happen, tools for ensuring the synchronisation between the two systems are needed. Additional complexities can be expected from the coexistence and the simultaneous availability of the securities in the traditional and DLT-based system. In order to avoid any arbitrage opportunity and ensure fungibility between securities recorded conventionally and on-ledger, the systems should be able to ensure a continuous, efficient and rapid synchronization (reconciliation) for the update and record-keeping of assets.

Model 2c - Securities recorded in conventional environment and referenced by tokens in a DLT environment.

Under this model, securities are initially issued and recorded in the conventional system, where they are stored in a traditional book-keeping system. Afterwards, securities are tokenised, creating their representation on a distributed ledger. In Model 2c, tokens can be used on DLT-based solutions in order to perform transfer of value and (all or part of the) rights that are embedded in the security that the token represents. To date, this model appears to be mainly used for back office, collateral transfer or lending facilities.

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

In this context, the transfer of a token, may be, but does not have to be, reflected in the conventional ledger. In this regard, consideration should be given to risk stemming from exchanging tokens and not the assets which they represent. Appropriate operational safeguards preventing the parallel use of the securities behind the tokens and the tokens themselves should be ensured in order to prevent double spending and integrity issues and abuses This practice can have an impact on market liquidity and overall stability of the market and financial ecosystem, as well as risks for regulatory arbitrages. In addition, the question arises as to 'what' will be transferred via the token (e.g. only record of the assets belonging to an asset available in DLT environment, rights of underlying securities).

Chapter 3: Key Features of the use of DLT for issuance, custody and settlement

3.1 Issuance, recording and redemption of securities on DLT environment

This section takes a deeper look at the issuance processes behind the different possibilities sketched above. It outlines the possible added value of issuance via distributed ledger and clarifies how certain functions (e.g. accountability, legal validity) are performed in legacy systems and systems relying on DLT. These findings together with a legal analysis of key aspects will allow for the derivation of key implications and requirements.

3.1.1 Description of related business and operational processes

The issuance in existing systems is currently pursuant to the national laws where the related assets are issued.

With respect to the two models presented in the previous section, Model 2 assumes that the issuance of a security is performed in conventional system, while the other post-trade processes could be harmonised and treated also on DLT-based systems by making available the securities directly on distributed ledgers (2a and 2b), and via referencing tokens (model 2c). In particular:

- Securities in model 2a are issued in conventional systems but then post-processing is performed within DLT environment after a full migration from legacy system.
- In Model 2b the operations subsequent to the issuance are either performed on DLT or in the legacy systems. In this regard, two ways of hybrid treatment can be distinguished:
  - i) A certain, defined fraction of conventional securities is treated on distributed ledgers and another certain, defined fraction of conventional securities is treated in conventional systems (i.e. the fractions are not mixed).
  - ii) A 'functional' split is performed: Certain post-processing is administered on distributed ledgers, while some post-processing is administered in the conventional systems.
- Finally, in model 2c the initial issuance is performed in legacy systems, but then the assets are partially or fully tokenised in order to ensure the transferability of the embedded rights in DLT systems and for operational purposes.

When referring to native digital assets which are issued directly on distributed ledgers, the processes performed in case of Model 1 warrant further investigation, in particular where the initial recording of a security would be done directly on the DLT. The issuance processes could benefit from distinctive features of DLT. A positive driver for DLT adoption can be the streamlined and uniform documentation such as the operating manual of the system (all elements are digitized immutably within DLT network) compared to conventional processes which may involve different intermediaries and processes. In addition, DLT can enable for higher transparency of the issuance process via nodes, depending on the information that is actually shown to stakeholders on the network.

Initial experimentations[28] with DLT and smart contracts favoured the discussion on possible revision of porting traditional assets into new technology environment swiftly, but it has

[28] See examples please in Annex I.

identified few issues related to asset creation and distribution: in model 2a and 2b, the use of DLT for creating and/or maintaining two systems that runs in parallel may imply new and different issues of interoperability and record-keeping.

3.1.2. Key implications and requirements

3.1.2.1 Legal perspective

3.1.2.1.1 Legal value of securities on DLT environment

All legal and regulatory requirements which are applicable to current assets are also adaptable to newly created assets via DLT-based solutions.

In case securities that are available in DLT networks are tradable financial assets, they must be in conformity with the financial laws of the country in which they are issued (and then traded).

Regarding model 1, challenges may arise due to different legal frameworks in Member States regarding the possibility of purely native digital assets.

The impact might be mitigated when running the on- and off-chain procedures in parallel (as in case of Model 2b).

In model 2c, it is conceptually intertwined with the process of tokenisation, with tokens being crucial for the functioning of the system. The relation between the conventional securities and their representations in DLT environment currently lack clarification from a legal and regulatory perspective. The concept of “issuance” should be used carefully and not be confused with the issuance of securities and any related legal implications, as the process of using tokens merely representing securities is rather a technical matter which may not be relevant to parties who are not directly involved in operating the system.

Tokenisation can conceptually be perceived in a very broad sense. On one hand, it can constitute merely generating a claim to ownership of an underlying security in the form of a token. On the other, tokenisation can end up in a complete ‘replication’ of the asset, where all associated rights are represented by the digital instance.

One question emanating is about the nature of tokens in the context of Security Token Offerings (STO), which in principle, claim to be a way of raising capital by creating either native digital assets or tokens referencing to existing assets by leveraging on DLT. Only in the latter case we speak about tokenisation. Despite certain conceptual similarities with traditional forms of funding such as Initial Public Offering (IPO), STOs do not resemble traditional securities and issuance.

3.1.2.1.2 Governance of issuance in DLT networks

A successful execution of issuance, recording and redemption of securities on DLT will depend on the presence of an authorised entity that assures the interconnection of the off-chain world with the system. If this is not regulated, market participants will not have the necessary reliance to engage with DLT-based securities. As already highlighted in previous work of this group[29], proper governance of any market infrastructure is important to ensure its safety and efficiency also in a DLT environment. In this regard, the question of how DLT

[29] https://www.ecb.europa.eu/paym/intro/publications/pdf/ecb.miptopical190111.en.pdf

solutions shall be governed may need to be considered as a matter of platform governance, application governance, as well as governance of intellectual property (IP) rights associated with the design of the solution used to provide a service through the platform and with the data recorded/shared through it. In any case, any arrangement should aim to enhance the integrity and resilience of information recorded.

3.1.2.1.3 Representation of assets in DLT networks

When moving towards a sole representation of processes on DLT, the question around the precise rights the token confers, actually becomes central. Tokens on a DLT can either represent ownership or legal entitlement to the underlying asset. In this document, out of an issuance perspective, we shall distinguish between three potential cases: i) the tokens refer to assets in a 1:1 relationship (e.g. one token - one 'underlying' security), targeting representation of the securities themselves on distributed ledger; ii) they refer to securities in a 1:n relationship (e.g. a token represents a legal claim to a basket of securities); iii) the tokens represent fractions of rights embedded in the asset they represent (1:1/n). All these cases can be captured in Model 2c, where the emphasis is both on facilitating post-processing and on direct replication of existing assets.

Tokens are not considered 'transferable securities' and therefore are not regulated by the competent authority according to existing regulatory framework, and cannot be transferred on regulated exchanges either. However, transfer of those tokens can be conducted on non-regulated platforms with risks of fragmentation and regulatory arbitrage in trading and post-trading processes. In the current regulatory framework, securities issued on conventional systems can receive an International Securities Identification Number (ISIN), allowing for information retrieval about the security and its issuer via conventional sources. Regarding accounts outside the conventional platforms, receipts from third-party wallets may require a prior whitelisting by the Issuer depending on the way the security tokens are set up. For example, Issuer and Arranger currently determine together whether a secondary market investor will need to be whitelisted or if the security tokens can be freely transferred.

Such procedures have found some prominent applications, and its main aspects can be seen in the description of Model 2c.[30] However, as pointed out above, the token only represents a claim to the underlying security, but not all features of the security may be represented on DLT environment. They may allow for simple fractionalization of equities via tokens and near-time settlement. The owner of the token effectively holds a claim for receipt of the underlying security towards the Token Issuer[31] (thus generating issuer and settlement risk). In any case, if an underlying security separate from the tokens exists the action of 'migrating' (Model 2a) or 'tokenising' (Model 2c) the issuance in a DLT environment cannot *per se* create a security. The token itself would not be seen as financial instrument, as this process would not reflect an issuance process per se, but a tokenisation. Also in case of a 'complete' representation of an existing security on a distributed ledger, targeting effective transfer of ownership in the security leads to a tokenisation and not an issuance or creation of digital native assets (such as in Model 1).

[30] For examples see Annex I.
[31] This is true generally speaking, but might be different in concrete cases depending on the overall legal setup and documentation.

3.1.2.2 Technical and business perspective

3.1.2.2.1 Connection to the Platform/DLT-System

The Issuer (or the Issuer Agent) would directly connect to the DLT system via its digital asset custody wallet for the Issuance of security tokens and the processing of payments throughout the lifecycle of the security. From an operational perspective, some processes are triggered by the Arranger on behalf of the Issuer (e.g. triggering of order allocation and token creation) or conducted automatically by the Platform (e.g. coupon payouts).

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

In model 2c, some form of tracking and comparability between tokens and underlying securities should be considered, in order to avoid any intentionally or unintentionally (ab)use of rights related to the security or securities represented by the token available in DLT environment.

3.1.2.2.2 Network architecture in DLT environment

In this regard and as highlighted above, securities can be issued on DLT network to introduce them to the conventional world after the issuance process (such in Model 1). At the same time, a logical step in evolution of securities towards DLT-based solutions can see first securities issuance being digitised and only at later (more developed) stage the full post-processing is also performed by leveraging on distributed ledgers (cf. Model 2a). On the other hand, it shows the lack of clarity for post-processing setup (especially towards CSD questions, local security laws, collateral eligibility rules, etc.) which forces innovative companies to re-enter the conventional world and to run in parallel both DLT-based solutions and conventional systems (cf. Model 2b).

As highlighted by a Focus Group on DLT under the International Telecommunication Union (ITU)[32], the high-level architecture can constrain the highly abstract hierarchical architecture of distributed ledgers. In particular, nodes in a DLT network work with typical distributed system solutions (including cloud solutions), which require key components such as i) safe hardware; ii) extendable protocol communication; iii) Network (including P2P network) management; iv) Consensus mechanism; v) Smart contract mechanism.

[32] https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d31.pdf

3.2 Custody and Safekeeping in a DLT environment

This section outlines the custody and safekeeping of respective securities models which are based on DLT solutions *vis-à-vis* conventional systems. It presents to what extent the established system of custody and safekeeping is relied on by presented securities models as well as how the same processes are conducted in terms of fully DLT-based assets. It then discusses the aspects related to account structure, asset servicing, including, investor protection and their functioning in the DLT reality. Lastly, it describes key implications related to the custody and safekeeping of securities in DLT-based system for market stakeholders and financial market infrastructures.

3.2.1 Description of related business and operational processes

As described earlier in this report some of the identified models, which leverage DLT, rely also on the existing system. In Model 2, the initial issuance of assets takes place in the incumbent system. Only once this process is done the assets are either:

- fully migrated to the DLT-based system, terminating custody and safekeeping in the conventional system as it takes place under Model 2a;
- kept parallel in both systems, and made available in traditional or digital way, depending on the need of a particular transaction or specific arrangements for safekeeping and custody, as provided by Model 2b;
- tokenised and later managed through a referencing token on a DLT network according to Model 2c, keeping at the same time the actual asset in custody of the conventional system.

A decentralised system could be considered compatible with the potential latency in post trade processing which uses rich business logic to support multiple customised events (e.g. corporate actions), while centralised platforms are being used mainly for pre-trade and trade execution activities, where the need is to ensure a unified process flow. Regardless the specific technology used for those services, the compliance with the current regulatory framework is still *conditio sine qua non* for the development and wide adoption of those solutions, and this should be the case also when using DLT. In addition, the possibility to use DLT-based solutions could require the existence or the development of different rules, different infrastructures and on the basis of specific recordkeeping techniques depending on the protocol used and the validation process. In this regard, the identification and definition of ledgers' structure and the overall governance which is ensured throughout the post-trade processes remain of key importance.

Furthermore the peculiarity of specific design of DLT protocols could raise concerns regarding the use of these technologies in a Peer-to-Peer (P2P) context, in terms of compliance e.g. with current AML/CFT rules and security purposes.

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

It remains to be discussed how exactly the custody and safekeeping processes would be shaped and organised in DLT environment and whether the asset available on DLT impacts

the rules and requirements to be compliant. In particular, in case the asset available only on DLT network would be a security (such in some cases of Model 1 and Model 2a after the migration period of securities issued via traditional systems), it should require the application of same rules as if it was available on traditional systems. In this context, the use of wallets and private keys may result in more difficulties in keeping track of the securities' movements and additional risks as the ledger would be the only source of information. At the same time, the potential benefits (i.e. wider overview of information and movements among nodes) could be used as main driver for adoption of those technologies. In Model 2b, for example, the possibility to check for changes in the clients' accounts and of rights on his/her behalf (e.g. Corporate Actions) requires a communication between the two systems on continuous basis and transfer of ownership rights might be more complex. In Model 2c tokens are merely representing the securities which remain in the conventional environment. However, tokens may represent some of the rights that are relevant in the asset servicing and might require some form of synchronisation among the systems.

3.2.2 Key implications and requirements

3.2.2.1 Legal perspective

3.2.2.1.1 Governance of custody in DLT environment

A question to address is to what extent the use of DLT could change the process of custody and safekeeping from a legal perspective, and in particular on the governance of the processes and to automated components of the system (e.g. smart contracts).

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

As different forms of governance and consensus protocols provide specific safeguards against manipulation of DLT networks, such as double spending, it remains to be determined which aspects should be subject to regulation and whether the architecture of the network (e.g. restricted v. unrestricted) may change the existing and well-established rules to be applied to it for custody and safekeeping. On the topic, ECB AMI-SeCo's previous work highlighted that the DLT-based consensus algorithms can have the potential of improving how the current post-trading processes are conducted, but also that can bring threats and negatively affect processes and machines. In any case, the need for a proper governance framework goes beyond any specific network and key features, especially taking into consideration the novelties in the custody and safekeeping which see the use of token, cryptography-based tools and 'trustless' trust (ensured via IT techniques).

Regardless of the technology used, custodians of assets have to provide sufficient safe custody of assets from misuse and/or malicious activities. This can result in additional burden and risk considering that the custody of client's assets is performed via the transfer of assets into a custodian's wallet and held on behalf of the investor. In order to mitigate this risk, one option could be to require a license that is tailored to the specific business and risk profile of a custodian.

3.2.2.2 Technical and business perspective

3.2.2.2.1 Safekeeping of digital assets in DLT environment

Custody of assets stored on distributed ledger would be different from custody of securities in the current setting, as technical design of a DLT storing a security or token that can be exchanged in a distributed network can require different steps *vis-à-vis* storing dematerialised asset in a centralised database as well as private keys that allow moving the assets. Currently, there are several approaches to safekeeping of private keys[33] in DLT environment.

A first question should be whether having control of private keys on behalf of clients (which may be the preferred option of the clients) should be regarded as safekeeping services and rules to ensure the safekeeping and segregation of client assets should apply to the providers of those services.[34] In particular, this would mean that, from a technology perspective, a custodian of a digital asset does not hold a client's private keys to the digital assets, but safekeeps its own private key that operate the client's digital assets.

Another key question is whether recording securities holdings on a distributed ledger would not be the same service as CSD notary and registration functions, which are essential to maintain the integrity of securities issues. However, a differentiation seems to be needed between key storage and safekeeping of the "booked" assets, especially in case of Model 2c where the keys refer to a token and not a security.

3.2.2.2.2 Requirements for custody of digital assets v. custody of private keys

The safekeeping of securities is currently regulated by national laws. Irrespective of whether assets are issued conventionally or as native digital assets directly in a DLT environment, , as well as the specific design and governance structure, the same requirements should apply. Securities accounts which are used for settlement and safekeeping need to be enabled to hold all type of assets including those natively issued in a DLT-based system. The same set of data for both securities in traditional form and digital need to be applied. In this context, rules such as on reconciliation are in place with the aim of addressing the risks that ledgers organised in hierarchy (e.g. custody chain) may imply. In a DLT context, the effectiveness of these rules should be assessed according to the purpose, specific organisation, governance of the specific DLT-based solution. Normally securities accounts held by intermediaries need to be reconciled. As long as the intermediary runs own and third party accounts, there is need for reconciliation. The reconciliation in the DLT set up would not be required as long as the ledger itself is displayed and reported to the client. However, a question is whether this is performed by any internal reconciliation due to the nature of distributed ledger.

As preliminary consideration, it must be highlighted that the holding of a digital token is referenced by holding of its private key, which are kept in wallets which function as repository. The risk of losing the ownership of digital assets by losing the related private key depends on how the custody of the key is performed, as well as the role of custodian and the existence of conventional environment. The specific case could entail a highly adverse impact and must be managed through appropriate models and procedures. There are however also important concerns regarding a definition of digital assets for custody

[33] See https://www.deutsche-boerse.com/resource/blob/1738116/946044d7f949f27cb373e6c7a7e32749/data/20200123-dlt-buba.pdf, p. 7.
[34] https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf.

purposes, which could be limited to back-up of private key or end-to-end protection of private keys and the assets themselves. This can take place by the transfer of assets to the digital wallet address of the custodian along with the ability to directly access, safekeep and transfer the assets via different types of wallets such as hot, warm and cold wallets[35].

Among others, custody chains are theoretically an option but, in any case, hardly compatible with the concept of DLT-based or any peer-to-peer system, which does not mean however that ownership of digital assets cannot be intermediated. The difference to traditional custody chains would be that the intermediation happens outside, partially or *in toto* the DLT-based network.

3.2.2.2.3 The identification of assets in DLT-based system

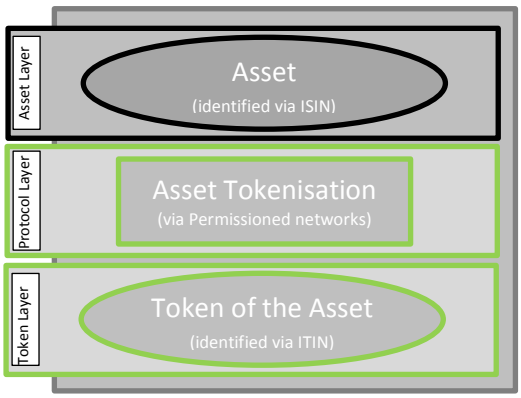
Unique identifiers for commodities, securities, or other assets, have been used on international markets for a long time. Typically, assets are represented as books and records, tracked via certain identifiers (e.g. ISIN) harmonising core processing across related asset types (e. g. equities, bonds etc.). At the same time, currencies are identified through internationally recognized ISO currency codes (e.g. EUR for Euro). While the current approach clearly requires ensuring scalability, it may come at the expense of penalising customised assets that have a special logic, as this approach puts limits for processing most assets just as an "asset item" effectively ignoring any features and conditions. This limited creation of assets variety on its own as well as product development and asset servicing activities. In simpler words: how can the market ensure the above while catering for innovation? Is there a need to balance scalability and changes in the current infrastructure and standards? Are those standards 'technology neutral'?

In the case of tokens, a key question is whether there is a need for specific identifier, i.e. whether there should be an additional domestic identifier (such as WKN in Germany, or SEDOL[36] in the UK) used alongside ISINs or CUSIPs[37], or whether, for example, ISIN should be the only identifier (which then raises questions, *inter alia*, on listing and transfer of such tokens)[38]. A need for token identification arises from the 'natural' consequence that a digital asset or a digital representation of a referenced traditional asset, in order to run on a distributed ledger, still needs to be defined by a code. This code does not only capture details of the token such as the current holdings by participants but defines as well a token's logic, such as the transfer of tokens from one participant to another. This characteristic of a digital asset recorded on a distributed ledger may be different from traditional assets within the existing market infrastructures, where securities are administered by central agents who record current holdings as well as transfers in their proprietary systems.

The implications of such difference for appropriate identification can imply that, in the case of traditional financial instruments or securities, a unique identification code or name, respectively, is sufficient in order to administer and update securities holdings by participants through central agents in their proprietary systems. In case of tokens however, it is of utmost importance to unambiguously locate the respective token address with respect to i) the

[35] The difference mainly relates to the use of internet connection. Please see the definitions in the Glossary under 'wallet'.
[36] Stock Exchange Daily Official List.
[37] 9-character alphanumeric code that identifies a security (like a stock or bond, debt or equity) for the purposes of facilitating clearing and settlement of trades in the US and Canada.
[38] For example, the World Bank's bond-i has an ISIN just as any other conventional debt instrument. For more details on the initiative, please see the Glossary.

distributed ledger it is deployed on as well as ii) the implementation mechanism and address used for deployment.
This difference can be best showcased by the following illustration, demonstrating the different layers that traditional identifiers and digital asset identifiers, like the International Token Identification Number (ITIN) provided by the International Token Standardization Association (ITSA) apply to[39]. While ISIN or FIGI are working on the Asset Layer, identifiers like ITIN are designed to capture the Token Layer, yet referencing the Asset Layer wherever possible. As a consequence, assets being 'tokenised' on different ledgers (or even by functionally distinct token contracts on the same ledger) may result in distinct stock tokens that will each receive a different ITIN, while still referencing the same stock ISIN.



At market level, also worth mentioning is the work of the Organisation for International Standards (ISO) on a Digital Token Identifier (DTI)[40], which aims to ensure interoperability, transparency end efficiency between different parties, by creating a 1:1 relationship between a digital token and its identifier.

3.2.2.2.4 Connectivity and standards in DLT environment

In order to ensure clarity, a preliminary distinction should be made between connectivity and standardisation of messaging. In the former case, connectivity ('the pipes') can currently be ensured via Swift, FIX, API, MQ or bespoke links. At the same time, messaging (the syntax and 'the content') should be standardized in order to allow straight-through processing (STP) in the participants and the participant's clients systems. No bespoke formats or free format fields should be considered or implemented. Whatever the connectivity method is, the messaging/reporting should adhere to existing or widely-used standards (such as ISO 15022 or ISO 20022). With the final objective of further contributing to the wide and efficient use of DLT network for custody and safekeeping purposes, (new) common rules and standards should be developed and/or applied by ISO/SMPG, in order to avoid that each system develop their own bespoke messages, which increases fragmentation and reduces the benefits for the whole ecosystem.[41] At the same time, it is worth considering is a possibility to overcome the concept of standards and messaging and ask whether they are needed also in a DLT environment. In the current ecosystem, with initiatives leverage different protocols, and technologies, common rules still seem to be indispensable, in particular when taking into account the risks of fragmentation in the market and the technological transition it is experiencing. However, in the (not foreseeable) future, it may be the case that new ways to

[39] For more information, please see https://itsa.global/
[40] For more information, please see https://www.iso.org/standard/77972.html

interact and perform transactions on the basis of DLT or other technologies in a fully decentralized ecosystem will require the establishment of new standards or new ways of defining the concept of standardisation.

Different network purposes and project scopes may require different connectivity solutions. DLT adoptions in FMIs so far seems to be developed into three use cases: i) Data and account structure standardization, ii) Mutualizing multi-party workflows on DLT and iii) Building applications on top of rich data sets that FMIs would eventually sit on.

As in case of Model 2a, migration of standards will take time and be determined by a number of factors, including harmonization processes (e.g. ISO 15022 to ISO 20022), in which many stakeholders are involved, it will be undertaken in waves and take time to become widespread. Costs and other priorities are also a consideration regarding timing. At the same time it needs to be stressed that standard modes of connectivity are needed in FMI initiatives and will remain mainly to ensure that isolated pockets are not created. Furthermore, they are important to avoid that users will need to redesign/redevelop their own mid/back office platforms, and/or have a separate workflow for legacy and for DLT based systems. Currently, different types of connectivity already exist in the market: they aim to ensure the standardisation of processes, actions and events, such as in the T2S environment. FMIs/projects adopting DLT are offering API based connectivity as an alternative, not as the only option. However, the content of the messaging needs to be standardized. For example, market wide initiatives and programming languages such as DAML would need to create a correspondence with market messaging schemes (e.g. ISO 15022, ISO 20022 or any other messaging scheme used).

Moreover, FMIs which would like to use DLT to synchronise multi-party workflows in order to achieve efficiencies in post trade services will have to make sure to provide multiple connectivity methods to ensure no participants are excluded from the new-infrastructure.

Certain specific message types of content fields might not be able to make efficient use of a DLT network. In order to overcome this problem there is a need of ISO/SMPG community work on new/expanded standards, rather than have each system to develop their own bespoke messages. Some initiatives have been developed by market participants with this goal. This means that in terms of communicating into/out of matching/asset servicing/Mid Office and other necessary systems, there could be a time where clients (or their service providers) may want to connect directly into such systems so everyone can see or match results at the same time without having to go through chains of intermediary messaging flows. This would need to be accommodated for and considered when designing the system.

DLT could also be used as infrastructure for tokenization, value-exchange or for fund raising. Native tokens would be issued, traded and exchanged on digital marketplaces (which can include tokenizing existing securities). There are market projects in which FMIs offer web portals/API based connectivity, which however will continue to persist with standard connectivity models. There are other projects developed within narrower contexts, as asset tokenization allows P2P marketplaces to be set up among a closed loop of players. The messaging standard here may be driven by the needs and requirements of the members participating in that project so the group supports connectivity options that work for each stakeholder within that group.

3.2.2.2.5 Potential changes in assets servicing (including Corporate Actions)

The life cycle of corporate actions starts with the company announcing to the market details of its impeding action. The following example, a capital increase with issuance of rights, is used for illustrating purposes. Every shareholder gets a specific number of rights allocated, based on the holdings on a given record date. The rights have their own specific ISIN. In many cases, the rights can be traded on a stock exchange or official market. The corporate action conditions normally state that, in order to complete the transfer of the new shares, the shareholder will have to pay the pre-determined price plus has to deliver the necessary number of rights to an agent, who is dealing with the capital increase on behalf of the issuer. Depending on the model, there are different solutions to ensure that these (basic) corporate events can be supported. It may lead to greater automation, earlier distribution of information and be less error prone than today's process.

Like in the above example, the processing mechanism of some important services under asset servicing may require additional consideration when leveraging DLT. Looking at another example, in terms of securities lending DLT could be applied in the stages of i) identification of potential fail, ii) collateral availability and position updates, iii) communication and agreement, and/or iv) instruction generation to off-chain platforms, with the aim of solving the challenges of strict market time pressure through process efficiency and ensuring faster operational risk management. Additionally, DLT can deliver concurrent communication of real-time information to multiple concerned parties so that these parties can be aware faster and to prepare earlier on what they need to do, as this aspect can help removing the time pressures from present sequential steps between parties. The immutability of information provided via DLT ensured via cryptographic tools could, technically, bring benefits in terms of asset protection, certainty and transparency in the market and costs savings. Furthermore, in terms of asset servicing instructions of securities lending could benefit from smart contract driven execution, although the code complexities can require additional steps to be processed before execution via smart contracts.

On this topic the DLT-TF provided an insightful analysis regarding how DLT can be used and what could be the key implications on post-trade processes.[42] In particular, it recognises that new technologies (including DLT), can ensure greater automation of contracts, for example in the area of corporate actions announcements. Furthermore, the use of information extraction and machine learning techniques could be relevant to improve efficiency and streamline processes. One of the key issues in this field is the ability to ensure a trusted, and ideally a golden copy to be used as the single source of legally binding information on corporate actions for information purposes. The ideal situation for the market would be one where every issuer (or its agent) is responsible for announcing all its corporate events by means of standardised, electronically readable, consistently formatted messages, and assumes liability for their accuracy and correctness. In a distributed environment, this could require more effort in terms of validation process and in the clear identification of roles, especially in unrestricted networks. In this regard, the use of smart contracts in DLT can provide a unique source of accessible information to all participants. Based on the role of the participants in the DLT network, the smart contract information could also be enriched, and again increase the value of the trusted copy. Reference data on Corporate Actions as

[42] https://www.ecb.europa.eu/paym/intro/publications/pdf/ecb.miptopical190111.en.pdf ; https://www.ecb.europa.eu/paym/initiatives/shared/docs/e4063-ami-seco-2017-12-07-item-1.6_2-dlt-tf-follow-up-work-on-corporate-actions.pdf.

records on DLT would be first created at securities setup for predictable events documented in the prospectus of the issue, while additional corporate actions throughout the lifecycle of a security would form updates to this original record. This would be the case in Models 2a and 2b, where the issuance is performed in legacy systems.

This process could be seamlessly conducted regarding ‘conventional’ Corporate Actions event such as in case of coupon payment, redemption of a bond as well as in case of default. However, it remains to be clarified how unpredictable events can be flagged and monitored in a decentralised environment, and what rules to enforce in order to ensure the consistency of the information and the efficiency of the flows of data among network participants and external parties.

3.3 Clearing and settlement in a DLT environment

3.3.1 Description of related business and operational processes

Clearing and settlement of assets, especially of securities in regulated systems such as exchanges, ensure the liquidity of the market and the stability of the financial ecosystem as a whole, which see the direct involvement of players and in the future potential other actors accessing the market with new and different solutions.

- In Model 2a, the system to be able to process and ensure clearing and settlement in the conventional system until the migration to the DLT-based system is completed.
- In Model 2b, clearing and settlement happen either within conventional or DLT-based system, and may increase the overall complexity.
- In Model 2c, clearing and settlement processes are performed for securities that are safekept e.g. by custodian banks in traditional securities accounts and in compliance with current regulatory framework.

The DLT can take the role of storing the information regarding who is the owner of which part and transfer of the ownership. However, it will not be able to prove automatically i.e. whether the rights can be enforced by the owners of the assets; whether the asset on DLT (cf Models 1 and 2a and 2b) or in case of token, the underlying asset even exists (cf. Model c). Such confirmation would require additional features on the top of the DLT at stake.

In case a party wants to sell or buy securities, settlement requires simultaneous exchange of cash and securities. In principle, same rules should apply when using DLT, although additional or different processes may apply.

In Model 1, clearing and settlement processes are performed within a DLT-based solution. As these native digital assets would be securities, same rules applied to conventional environment should apply. In case of private placement issuance without the aim to trade it on a regulated market the use of private and closed system may facilitate the transfer of securities without the need of settlement to happen and would be closer to an update of the ledger. DLT-based solutions are used after the fully migration from the conventional environment (in Model 2a) or depending on the need of the specific model (cf. Model 2b).

Model 2c would allow tokens to be transferred on DLT-based solution which, in any case, needs to ensure that the information are verified and the embedded rights can be enforced by the entity that receive the token from an entity that was entitled to transfer those rights. In this context, settlement finality links to the concept of immutability of the transfer of rights. In addition, the synchronization between the conventional system (in which the underlying assets are traded) and the DLT-based one (in which tokens partially or fully represent the underlying assets) is needed to perform clearing and settlement while ensuring integrity of the assets and enforceability of the transfers among (also external) parties.

3.3.2 Key implications and requirements

3.3.2.1 Legal perspective

3.3.2.1.1 Settlement finality in DLT environment

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

In traditional systems settlement finality is a well-defined point in time, backed by a unambiguous legal basis. For DLT arrangements, settlement finality may not be as clear. The settlement finality directive (SFD)[43] adopted in 1998 regulates designated systems used by participants (e.g. banks, CSDs and CCPs) to transfer financial instruments and payments in case of traditional systems. It guarantees that transfer orders which enter into such systems are also finally settled, regardless of whether the sending participant has become insolvent or transfer orders have been revoked in the meantime.

DLT-based arrangements rely on a consensus mechanism to ensure the settlement finality, but must comply with the current regulation (e.g. SFD). However, the specific protocol used by the networks may imply different and/or additional steps and processes to its participants for the purpose of achieving the finality in a point in time that is agreed by the network and enforceable to externals.

In addition, DLT-based solutions can be used for synchronising value date and trading date via 'real'- or 'near-time'-settlement according to the consensus mechanism, with the aim of reducing settlement risk and potentially providing capital relief thanks to the immediate availability of funds to be reused for other transactions. At the same time, DLT may reduce the hurdles of complex reconciliation due to its distributed data structures. 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).Finally, the role of operator is needed in case of a system failure, especially in ensuring the latest positions are correct. In this context, the value of a golden record can be twofold. First, it will ensure certainty, as synchronization between systems will be performed, which may require time. Secondly, it would reduce the risk of arbitrage between two systems (i.e. the traditional and DLT-based systems) which need to interface one with both for clearing and settlement purpose.

3.3.2.2 Technical and business perspective

3.3.2.2.1 Digital Asset: Delivery v. Payment in DLT environment

Securities could be settled and traded on one platform such that delivery-versus-payment can be ensured and reconciliation efforts could be efficiently conducted, operational transaction finality can be achieved within seconds such that settlement time can be considerably reduced. A joint research of the ECB and Bank of Japan (BoJ) considered DvP to be conceptually and technically designed in a DLT environment with cash and securities on the same ledger (single-ledger DvP) or on separate ones (cross-ledger DvP). The concrete design of DvP, however, depends on the characteristics of the DLT platforms (e.g. range of information shared among participants, data structure and locking of delivered assets). In addition, depending on the use case, DvP design can be influenced by a number of factors including the interaction of the DvP arrangement with other post-trade infrastructures.[44] Finally, the expected gains of tokenising securities and by creating 'cash on Ledger' to settle the transactions, compared to settling the transactions on existing systems, and the rationale and business case for such an investment are still to be explored.

[43] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A01998L0026-20190627
[44] ECB and BoJ, Securities settlement systems: delivery-versus-payment in a distributed ledger environment, at https://www.ecb.europa.eu/pub/pdf/other/stella_project_report_march_2018.pdf

3.3.2.2.1.1 Delivery: Asset on Ledger

The ownership of a digital token can be represented by possession of its private key, which can be stored in a wallet. As this can be owned directly by the investor, therefore no custodian is required. A broker may also not be necessary as the transaction can be executed directly via the DLT. Nevertheless, it remains important to distinguish the operational processes, from the business drivers, as it may technically be feasible to execute a transactions peer-to-peer, but it may practically be challenging in light of lack of price discovery and an intermediary may well be required. In comparison to legacy systems, two or more intermediaries are involved. For this to happen, the investor would need to connect directly to the counterparty on the DLT or become a node itself.

Real-time processing of assets with liquidity savings mechanisms could be possible as there is no longer a need to close incoming/outgoing feeds for maintenance or strict adherence to batch time. However, at the same time the overall network can still enjoy the benefits of something that is closely associated with batch processing - netted settlement - if required. This does require network parties to ultimately agree to certain settlement procedures if net settlement is desired (e.g. settlement times and windows), but it grants higher flexibility.

3.3.2.2.1.2 Payment: Cash on Ledger

In this context, a clear difference between Commercial Bank Money and Central Bank Money should always be made. Several providers claim they offer services of ‘putting cash on ledger’, i.e. offering a form of token in a network (mainly DLT-based), in order to ensure in the same system a form of Delivery of Assets for another transfer of value (i.e. payment or delivery of asset). However, in order to have a claim to the Central Bank on the Ledger, additional features are needed, which mainly depend on the specific chosen design, the regulatory framework of the Issuer Central Bank, as well as the impact on the financial ecosystem.

3.3.2.2.2 Immediate settlement: Implications to value chain and market structure

DLT-based systems could be adopted with the aim of standardizing and streamlining processes, leading to cost savings by reducing unnecessary duplication of activities (e.g. for reconciliation) and better risk management. The market is evolving also regarding clearing and settlement and new needs and solutions may emerge. In this regard, an important consideration for investors, banks and FMIs who may want to adopt DLT is on the business case. In other words, how material are the expected cost improvements compared to the required investments. Another question is whether these advantages can be achieved within the current ecosystem or by other means. Moreover, when looking at benefits such as immediate settlement, one could question that if cash and assets could be made available upfront for a DLT solution to enable immediate or same day settlement, why can’t the same also be achieved in existing ecosystem (as it is technically feasible, although is not market practice). There are also further considerations on whether cost benefits related to more automated asset servicing via smart contracts could translate into lower fees to the end investors or greater transparency towards issuers.

For example, immediate settlement does not require ring-fencing of cash and assets when integrated is needed with the exchange to ensure that positions can be secured before the trade is confirmed.

Worth highlighting is that real time settlement, which is performed also in the most current legacy systems, would only reduce, and not eliminate (as only pre-funded transactions do), the credit risk, e.g. that the counterparty doesn't have cash or securities.

3.3.2.2.3 Liquidity issues from asset clearing and settlement on DLT network

The specific arrangement for participants, the system and the broader market when using DLT in comparison with existing arrangements may have implications for liquidity, at the level of the single entity and the whole financial ecosystem. For example, the risk that DLT-based solutions can create closed loop network may impact the overall liquidity and result in liquidity management issues and fragmented liquidity pools, as well as impact negatively the overall adoption of DLT-based solutions. For example, privately issued securities without the aim to be traded on a regulated market under Model 1 imply the use of a closed system for these services, which may reduce the liquidity at disposal to the system and hinder further investment and participation from other market participants. Liquidity risks may arise during the migration period in case of model 2a, with consequences that span from loss in efficiency to additional costs for the service providers. Model 2b considers the use of the non-DLT and DLT-based systems in parallel and may imply a reduction of the overall liquidity as the securities would be available only in one of the two systems and as consequence, be blocked (or 'frozen') in the other one. In model 2c, the use of an additional layer on 'top' and bridging the two DLT-based systems with the use of a token for the settlement, would not need to be subject to the same regulation that would apply to securities, while it can drain the liquidity that is available in the market and result in efficiency losses and market fragmentation.

CONCLUSIONS

Body text

GLOSSARY OF DEFINITIONS

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.

Centralized or Notary schemes: These trusted entities are acting automatically in case of events on some chains or are reactive to issue signed messages, if asked by the network. As centralized schemes, trusted entities cooperate with each other to ensure interoperability.

Dematerialisation: The substitution of paper-form securities by book-entry securities. Securities in book-entry form exist as computer records instead of as paper certificates. Book-entry form is mandatory in the EU for all securities that are publicly traded or are financial securities according to Article 3 CSDR.

Distributed ledger: A shared database where records can be updated by a set of *participants*, with no need for the central database management system used to validate such updates in traditional databases.

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

Hashing: 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.

Hash-locking: this method uses the preimage of a specific hash on both chains to realize interoperability. The cryptographic proof generated on ledger X will trigger an event on ledger Y, without any third party involvement.

Native digital asset (cf Model 1): a security that has been originally issued, recorded and kept in DLT-based system

Node: Any machine (e.g. computer) that is connected to the DLT network.

Oracle: A *node* of the DLT network that certifies to other nodes the occurrence of specific events outside the network (e.g. change in asset prices, weather conditions, etc.).

Participant: A legal entity or natural person that connects via a node to use a distributed ledger, and the technology behind it, to manage information.

Private key: One of two keys (the other being the *public key*) used in asymmetric cryptography and held privately by its owner and used 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.

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.

Restricted network: A DLT network that can be accessed only by a specified set of *participants*, who can then be assigned different roles. See also *unrestricted network*.

Sidechains / Relay schemes: 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.

Smart contracts: Algorithms that are coded to update records when a set of conditions are met.

Semantic interoperability: prevails in case of agreement regarding meaning, interpretation and intension of use of the same state. For example, an event will be executed by ledger B when a token is locked on ledger A. The token cannot be used on Ledger A anymore.

Syntactic interoperability: focuses on the ability of ledgers to communicate with other ledgers regarding data formats and communication protocols. Notary and relay schemes guarantee syntactic interoperability between two ledgers. Regarding hash locking, interoperability is limited to the hash stored in the smart contracts and the hashing algorithm.

(Asset) Tokenisation: a process of creating a *token (of an asset) - a mere representation of an asset, which is already available elsewhere.*

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

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*.

Wallet (Digital): 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. There are certain broad types of wallets: (i) Hot wallets: which are functioning online and are connected in some way to the Internet; (ii) Warm wallets: e.g. dedicated device which generates keys, signs transactions, and broadcasts them to the network via a connection to a host computer; (iii) Cold wallet: offline, stored on a platform that is not connected to the internet.

ANNEX I – MODELS - examples[45]

The issuance of native digital asset – Bond-I by the World Bank (August 2018) (ISIN: AU0000020612)[46]

The World bank has launched bond-I a bond instrument created, allocated, transfer and managed through its life cycle using DLT. The issuance took place on a private, permissioned blockchain platform developed by the Commonwealth Bank of Australia which also mandated as the arranger for the bond. The transaction took place under the Australian jurisdiction. The two-year bond raised A$110 million.

The issuance and settlement of money market transaction of native digital asset - European Commercial Paper (ECP) via blockchain by Continental (February 2019):[47]

Continental has issued an ECP as native digital assets in order to undertaken a delivery vs. payment transaction via blockchain.
The security was issued, signed and traded digitally using a qualified electronic signature. The issuance took place under Luxembourg law and distributed under German law via a direct issuance and distribution. All requirements relating to this transaction were handled by digital and legally binding means using blockchain technology.
The transaction was initiated and settled directly between the parties. The trade (including payment processing) was processed using blockchain. The documents and funds were exchanged within minutes instead of days.

The Issuance and settlement of shares as native digital assets on a private blockchain via LiquidShare platform[48]

Liquidshare is a platform that allows issuance of native digital assets on blockchain. The platform is based on a private and restricted blockchain network.
The entirety of the issuance is registered onto LiquidShare's blockchain and accounted for via an issuance smart contract that keeps track of the total number of securities composing each issuance. Issuances are classically identified by means of an ISIN number. Every issuance has it is unique account in the blockchain.
Settlement is arranged through an atomic DVP in the blockchain of securities vs tokens backed by commercial bank money and by central bank money.

An issuance and safekeeping of bonds as native digital asset via Bitbond platform (April 2019)[49]

Bitbond is a platform that enables end-to-end security (bond) issuance process on DL in compliance with EU prospectus regulation and German BaFin.[50]
The Platform is built on the stellar protocol and allows for, among others, onboarding of investors; issuance of fiat backed e-money used for on-chain payments within the platform or custody solutions for native digital assets.
The issued securities are distributed directly into Investors' digital asset custody wallets (The securities remain in the Issuer account at the Custodian until investors have funded their account and the DvP is triggered).
The custody of issued asset takes place via Bitbond's platform. Bitbond utilises key management software replacing private keys with Multi Parti Computation (MPC). Investors can access and use their custody wallet via a web-based interface.

[45] The enumeration hereafter is illustrative and not exhaustive. Please note that the use cases describe the views of the companies leading the initiatives and not of the Ami-SeCo Fintech TF
[46] Press release: https://www.worldbank.org/en/news/press-release/2018/08/23/world-bank-prices-first-global-blockchain-bond-raising-a110-million
[47] Press release https://www.commerzbank.de/en/hauptnavigation/presse/pressemitteilungen/archiv1/2019/quartal_19_01/presse_archiv_detail_19_01_79242.html
[48] LiquidShare is a company that offers a variety of services such as the issuance of native digital assets and their subsequent custody. LiquidShare offers also a platform based on blockchain technology, where securities issued directly on blockchain can be held and transferred.
[49] Note: Live issuance on Stella blockchain, ISIN assigned in July 2019 (DE000A2TR7Q2); see further details in prospectus (EN) and in German. https://www.bitbondsto.com/de
[50] see: https://www.bitbondsto.com/files/bitbond-sto-prospectus.pdf

The issuance and safekeeping of bonds as native digital assets by Banco Santander (Sep 2019)[51]

Banco Santander issued an end-to-end blockchain bonds as a native digital asset registered in a permissioned manner on the public Ethereum blockchain (with standard public Ethereum proof of work mechanism). Assets were issued as a set of fungible ERC-20 tokens.
The bonds could only be accessed by the owner using their private key, stored by a regulated custodian. Parties other than the custodian could only interact with the asset on the blockchain via a built application. They could authenticated themselves by entering PINs in the application to access their private key for the purpose of taking actions on the blockchain[52] Corporate actions, including the issuer call used to trigger the maturity of this security, were initiated with the user authenticating themselves to the blockchain by entering their PIN to access their private key. Smart contracts were designed to execute logic in a distributed manner. Post-trade processes were managed on the chain by the smart contracts and the application.
The legal documents underpinning the instrument were customised to reflect the nature of the bond as both a regular security under existing securities regulations and also as a native digital asset[53].

The issuance of a debt security as an native digital asset by Dealfabrix (October 2018)[54]

Dealfabrix is a DLT-based capital markets platform enabled the issuance of "Schuldscheindarlehen" (debt security) directly on a permissioned blockchain. The entire workflow in the issuance was conducted digitally directly on the platform.
DLT has been applied to remove the traditional paper-based issuance processes. The legal validity of the contracts concluded and of the securities or obligations issued on the platform was ensured via DLT specificities such as immutability and distributed information with integrated conventional technology such as electronic signature and two-factor authentication.

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

SDX has been implementing a distributed securities settlement and custody system on distributed ledger. It provides account for securities as native digital assets and private stablecoin needed for the payment leg in DvP transactions.
The system operates on three types of nodes: Notary node (operated and controlled by SDX) which signs all transactions in order to be processed; Participant Node – where new transactions can be initiated (operated by each participant); SDX Node – where newly initiated transactions can be stored (operated by SDX). The number of participants is controlled by SDX (private DLT). SDX has full control over who can participate and who will get a node in the SDX DLT infrastructure.
For the purpose of safekeeping of native digital assets the SDX is using Hardware Security Model which store private keys. The CSD application built on top of SDX DLT infrastructure is account based, allowing also traditional custody chain.
SDX claims to offer a market model in trading that eliminates clearing through atomic trading and settlement, at the same time the SDX CSD DLT infrastructure can also interact with a traditional clearing system and settle the transfers accordingly.
The settlement is conducted on a peer to peer basis between the involved nodes. In an atomic trading and settlement scenario, it is a multilateral settlement instruction that is settled as a whole or not. For bilateral settlements, the participants instruct SDX to settle the respective transfer on the intended settlement date.
The payment leg (on and/or off chain) is organised with the use of private stable coin that is funded through a dedicated SDX account in the Swiss RTGS system SIC. The stable coin comes with counterparty risk towards SDX.

[51] Press release https://www.santander.com/en/press-room/press-releases/santander-launches-the-first-end-to-end-blockchain-bond%C2%A0
[52] Only Santander Securities Services had the ability to bypass the Nivaura application to access the blockchain and they did not have access to any party's private key.
[53] Customised legal documents ensured the status of the instrument as a regular security. Since a Banco Santander unit bought and held the full quantity of the security until maturity and there was no secondary market, the security was fully compliant with existing European securities regulations.

[54] https://www.dealfabrix.com/

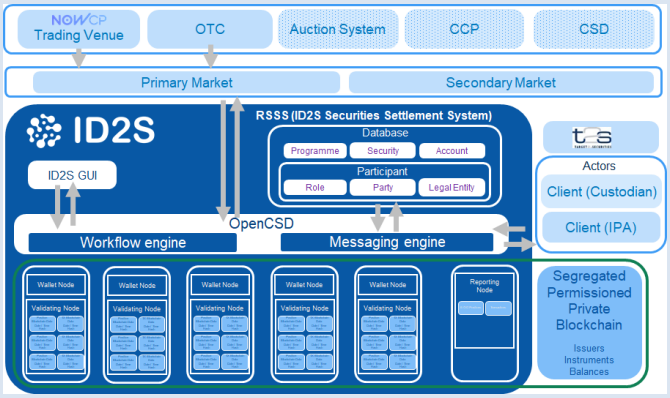
A migration of traditionally issued securities onto blockchain by Commerzbank (Sep 2017) (ISIN: DE000A1V4HP3)[55]

A traditionally issued ECP have been traded and simultaneously key elements of the transaction were replicated and simulated on blockchain. The standard number of required intermediaries was reduced, this allowed for an immediate posting. Real-time settlement was done using Target2.

Blockchain as a data recording system for transactions by ID2S CSD

ID2S is an EU CSD providing issuers with an automated process for NEU CP issuance from initial set up in its static data environment until final settlement in TARGET2-Securities (T2S). It operates a securities settlement system dedicated to transactions in NEU CP issued within ID2S.

The CSD operates ID2S SSS Platform (RSSS), which utilises a segregated, permissioned, private blockchain. The use of blockchain is limited to acting as the golden record of both securities transactions processed through ID2S and asset/security ownership recorded on ID2S. The data committed to the blockchain is replicated across multiple identical nodes.



The Primary Market issuance is processed within RSSS using blockchain. ID2S creates the issuance account in the blockchain and then records subsequent state changes in the blockchain relating to the movements between issuance, distribution and custodian / investor accounts.

A settlement of tokens representing securities on DL by Commerzbank (Oct 2019) (ISIN: DE000A1V4HP3)[56]

Commerzbank, Deutsche Börse and MEAG, have conducted a transactions where a secondary market securities – made available through a tokenisation, have been settled using tokens referencing commercial bank money.

Tokenisation as a tool to denote baskets of bonds for collateral swaps (November 2019)[57]

Deutsche Börse and HQLAX DLT-based platform allows for frictionless collateral swaps in the securities lending market. The securities are issued traditionally and grouped in the form of basket of securities. For the purpose of conducting DvP, the baskets are tokenised and represented on DL by tokens. This eliminates the operational requirement to physically move securities across fragmented securities settlement systems. [58]

[55] Press release: https://www.kfw.de/KfW-Group/Newsroom/Latest-News/Pressemitteilungen-Details_434560.html

[56] Press release: https://www.deutsche-boerse.com/dbg-en/media/press-releases/Commerzbank-Deutsche-B-rse-and-MEAG-to-reach-further-step-in-post-trade-services-using-distributed-ledger-technology--1631510

[57] https://www.commerzbank.com/en/hauptnavigation/presse/pressemitteilungen/archiv1/2019/quartal_19_04/presse_archiv_detail_19_04_85450.html

[58] For more details, please see: https://www.hqla-x.com/operating-model

Settlement of a repo transaction using tokens representing securities on DL by Commerzbank, DE (Feb 2019) (ISIN: DE000A1V4HP3)

The Settlement of a repo transaction by Commerzbank was undertaken using tokens generated for both traditionally issued securities and commercial bank money. DLT was used to execute the simultaneous swap of the tokens on a DvP basis.

Use of tokens to represent shares on crowd investing platform provided by Conda AG[59]

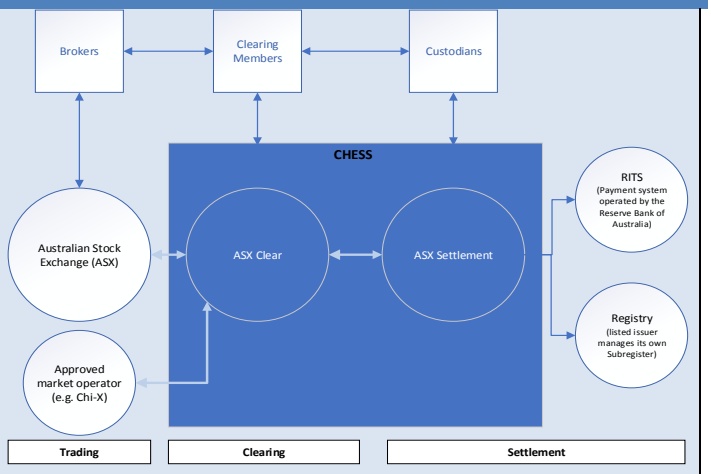
Conda AG is a Crowdinvesting platform that allows for existing assets to be represented by tokens on blockchain in order to be offered to potential investors. The platform responsible that only identified investors can purchase tokens. Whenever a token is transferred from one shareholder to another an entry in the underlying Etherum blockchain occurs, on the basis of which the entry into the company's share register is made. The transfer of the token is therefore equivalent of the transfer of share.

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

Under the ASX value chain system, securities are recorded traditionally in the Register outside ASX (listed issuer manages its own Subregister – see the figure above), while in the Clearing House Electronic Subregister System (CHESS) securities are represented by tokens which represent the underlying assets.[60]

The issuance, custody and safekeeping take place outside of ASX. CHESS system registers and operates solely using tokens of the underlying assets. All positions deposited in ASX Settlement are automatically recorded an electronic subregister.

ASX performs clearing and settlement functions under the supervision of the Australian Securities and Investments Commission (ASIC) and the Reserve Bank of Australia (RBA).



The payment leg is operated outside ASX in a real-time gross payment system (RITS) by Reserve Bank of Australia.

[59] https://www.conda.at/en/crowdinvesting/homepage-at/about-conda/

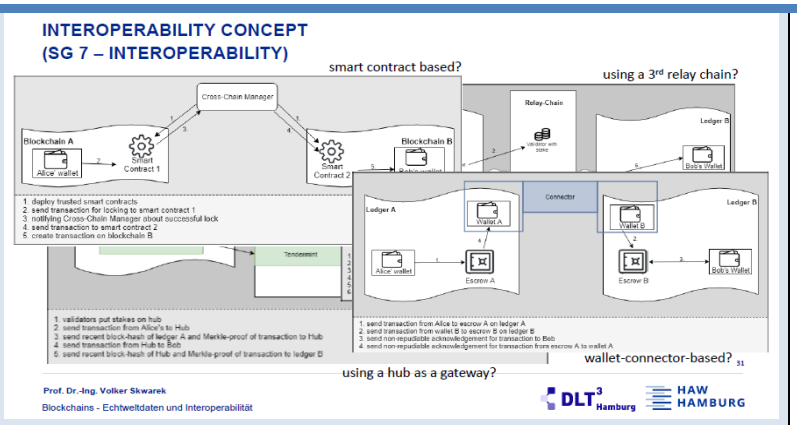
[60] ASX's key partners for the DLT infrastructure are Digital Asset[60] and VMware[60]. ASX signed a memorandum of understanding (MoU) with Digital Asset and VMware to work together on initiatives based around distributed ledger technology. In 2016, ASX purchased 5% of technology partner Digital Asset Holdings.

ANNEX II – Interoperability solutions

Standardisation initiative:

International Organisation for Standardisation – Blockchain and DLTs

ISO, (ISO/TC 307/SG7 explores the standardisation of blockchain technologies and distributed ledger technologies.[61] In this remit in 2019 and 2020 the organization published 3 standards for blockchain and distributed ledger technologies: "Overview of and interactions between smart contracts in blockchain and distributed ledger technology systems[62]; "Privacy and personally identifiable information protection considerations"[63] as well as "Vocabulary"[64].



[Image[65]]

Examples of interoperability solutions[66]

System for on-chain communication of different blockchain by Cosmos:[67]

Cosmos is a decentralised ecosystem of independent and parallel blockchains that can scale and interoperate with each other using Inter Blockchain communication (IBC) protocol, allowing interoperability between them. All connected blockchains communicate through IBC and the Cosmos network operates as a central hub (Cosmos Hub). The hub is based on a multi-asset Proof-of-Stake blockchain. The main token of the Cosmos Hub is Atom and it is used for staking and governing the blockchain. The token holder can be a either a validator or delegator. Validators operate a full node, which secures the network and processes transactions, while Delegators delegate their Atoms token to validators based on their personal review regarding the trustworthiness of the validators and capability of operating a node. The validators will stake the token and receive the token as rewards every block. These rewards will pass down to the delegators with a small fee withheld for operating the validator node. For keeping validators to stay honest and in case of maliciously acts or publishing incorrect data to the blockchain, the cardsharper will be penalized by losing some of their tokens. A token also grants right for governance: One atom represents one vote for any proposal on the network like software upgrades. Delegators can choose either to vote themselves or they pass the voting power to the validator they delegate to. The validators must vote on every proposal, or they will be penalized.

---

[61] ISO Standard ISO/TR 23455:2019, Blockchain and distributed ledger technologies — Overview of and interactions between smart contracts in blockchain and distributed ledger technology systems, was published on 30 September 2019. See https://www.iso.org/standard/75624.html?browse=tc

[62] https://www.iso.org/standard/75624.html?browse=tc

[63] https://www.iso.org/standard/75061.html?browse=tc

[64] https://www.iso.org/standard/73771.html?browse=tc

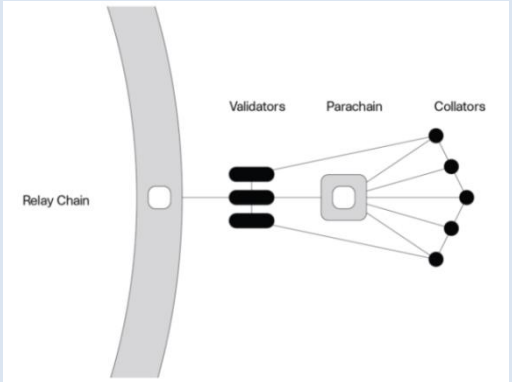
[65] Presented by Professor Volker Skwarek, Hamburg University of Applied Sciences at BaFin Tech Conference 2019, Bonn, 11 September 2019. Slide 16.
Available at: https://www.bafin.de/SharedDocs/Downloads/DE/Veranstaltung/dl_190911_BaFin-Tech_Vortragsunterlagen_5.pdf;jsessionid=0CEB35E36B667EA7660B22AD1F952900.2_cid390?__blob=publicationFile&v=2

[66] The enumeration hereafter is illustrative and not exhaustive. Please note that the use cases describe the views of the companies leading the initiatives and not of the Ami-SeCo Fintech TF

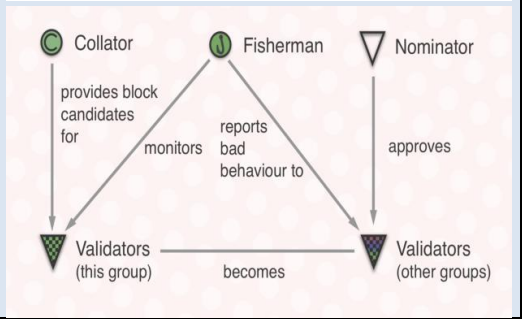
[67] https://cosmos.network/intro

Interoperability platform by Polkadot

The project Polkadot is developed by Parity. Polkadot aims to deliver an exhaustive interoperability platform where all kinds of private or public chains, oracles or future technologies are to be able to exchange the information and transactions in a trustless way.[68] The network of Polkadot has the Relay Chain, which operates as the central connector working (similar to the Cosmos Hub). On the top of it, The system has parachains, which fulfil the role of a bridge and connect the Relay chain with outside live applications like blockchains (Please see the figure).

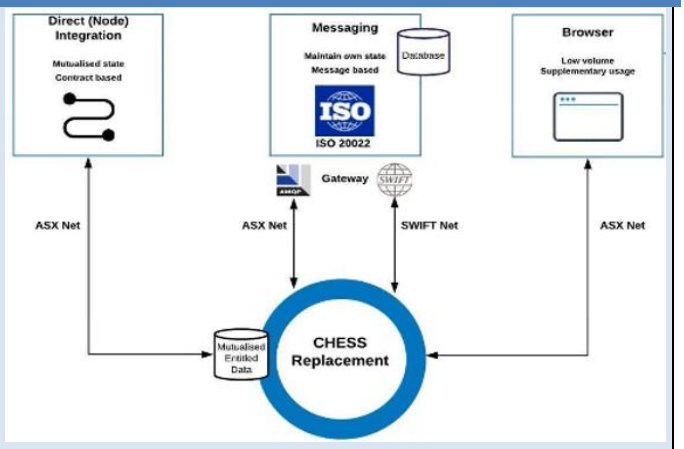


Parachains have their own economies based on Proof-of-stake scheme and tokens called "Dots". The Dots offer governance and also game theoretical incentives for token holders to behave in honestly. The network contains four major stakeholders: validators, nominators, collators and Fishermen. Similar to Cosmos, Polkadot also penalise bad behaviours. Validators do not maintain the fully synchronized database of all parachains. They delegate the task of storing to a collator. The main task of a collator, which needs to operate a full node, is to produce valid parachain blocks. The collator executes an unsealed block with a zero-knowledge-proof and offers it to one or more validators, who take the responsibility for proposing a parachain block to the Relay Chain. Collators and validators receive transactions fees for their tasks. Fishermen are independent and monitor misbehaviour of collators and validators.[69]



Interoperability system for on and off-chain solutions through Digital Asset Modeling Language (DAML) by ASX (ongoing implementation)

In December 2017 the replacement of ASX's CHESS with a new system based on DLT was initiated. The application will be based on Digital Asset Modeling Language (DAML) The replacement of CHESS will be within ASX security perimeters on a private, permissioned, secure network where only known - licensed participants would be authorized to access the system. Private contractual information will be encrypted and segregated, not be shared with all participants. The shared aspect of the solution serves as a transaction notification and synchronization mechanism and includes only hashes (one way cryptographic functions).



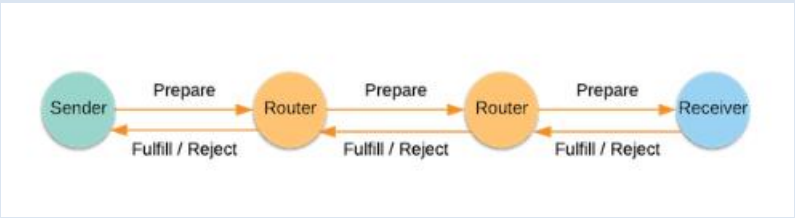
DLT-based replacement for the CHESS system allows other companies to build new services that interact system via DAML, with three main connectivity options:

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

[68] https://polkadot.network/about/
[69] https://wiki.polkadot.network/docs/en/learn-parachains

Interoperability solution based on routing by InterLedger Protocol (ILP)[70]

The ILP is an open protocol based on routing, that aims to enable seamless exchange of value across payment networks. using "connectors" ("routers"), and "interledger packets".



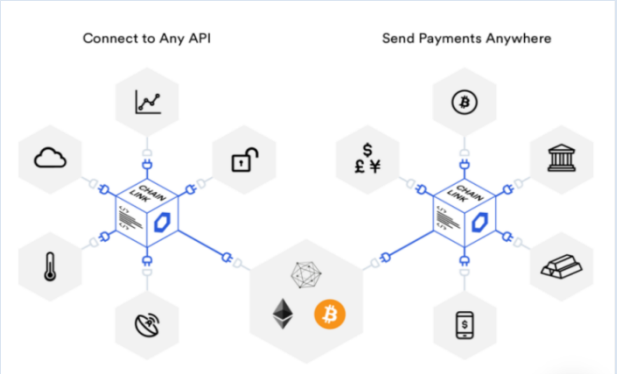
The sender constructs and sends a Prepare packet as a request to the connecting router. The packet is then forwarded until it reaches the receiver. The receiver accepts or rejects the packet by sending a Fulfill or Reject packet as a response. When the sender receives a Fulfill packet, it knows that the packet was successfully delivered to the receiver. The sender then continues to send the remaining Prepare packets until the value is fully transferred.[71] The transactions are secured by means of conditional transfers. ILP is a proprietary protocol.

Open source solution for connecting blockchains by FUSION [72]

Fusion aims to connect different DLTs by means of a common public blockchain using Decentralized Control Rights Management (DCRM) – an open source interoperable solution that offers a decentralised custodian model (cross-chain and cross-system). where assets are hold and transferred on behalf of the user across heterogeneous chains. The DCRM is to offer a hot wallet liquidity with cold wallet security, a key recovery system and, a settlement network, as well as an option of introducing a protection requiring multiple approvals in case of both workflow on-chain or off-chain.[73]

Middleware solution for on and off-chain systems by Chainlink [74]

Chainlink provides smart contracts with inputs and outputs in order to prove contractual performance, as well as multiple outputs to affect outside systems and send payments to complete the smart contract. As a result, Chainlink secures middleware facilitating the interplay of smart contracts and the real world data, allowing them to connect with key external recourses like off-chain data and APIs.

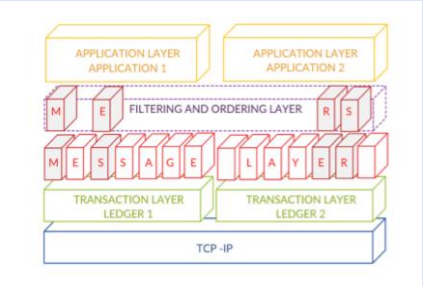


Moreover, Chainlink aims to eliminate the problem of single point of failure that arise when smart contracts are connected to data input through a single node.[75] Before any data becomes a trigger, it is evaluated by multiple Chainlink, in the decentralised oracle network, at the same time maintain the overall value of smart contract.[76]

[70] https://interledger.org/overview.html
[71] https://interledger.org/overview.html
[72] https://www.fusion.org/
[73] https://www.fusion.org/products/dcrm
[74] https://chain.link/
[75] As a result smart contract is only as reliable as that one node.
[76] https://chain.link/features/. For more details please see: https://link.smartcontract.com/whitepaper

DLT-based system for DLT and legacy based solutions by Quant[77]

Quant's Overledger Operating System is a DLT system aiming to interconnect and interoperate disparate DLTs as well as legacy system. It aims to eliminate the problem of single-ledger dependency by facilitating the communication, migration and exchange of information as well as value among different DLTs, by allowing general purpose applications to run on top of them.[78]



[77] https://www.quant.network/
[78] Quant Overledger Whitepaper, published 31 January 2018. pp. 5 and 8, https://www.quant.network/wp-content/uploads/2018/09/Quant_Overledger_Whitepaper-Sep.pdf