CAST | COMPLIANT ARCHITECTURE FOR SECURITY TOKENS

White Paper - “Call to Action”

Version 1.0

May 2021

TABLE OF CONTENTS

1 | CAST OVERVIEW 5
1. CAST Framework manifesto 6
2. CAST Framework description 7
2.1. Native Security Tokens 7
2.2. Tokenization as a step towards securities digitization 8
2.3. Overview of the CAST Framework 10
2.4. The components of the CAST Framework 12
2.4.1. Operational component 12
2.4.2. Legal and regulatory constraints 12
2.4.3. Technical component 13
2.5. Understanding transfer management principles 13
3. CAST Framework ecosystem/community 15
4. Key challenges 19
4.1. Capital market constraints 19
4.2. Business challenges coverage 19
4.2.1. Challenges matrix 19
4.2.2. Addressing these challenges with the CAST Framework 20
2 | CAST OPERATIONAL FRAMEWORK 22
1. Roles and responsibilities 23
2. Key features of the operational component 25
2.1. Focus on transaction management for Security Tokens 25
2.2. Focus on business terms for Security Tokens 29
2.3. Focus on safekeeping of Security Tokens 29
3. Services map 30
3.1. Issuance services map 31
3.2. Trading services map 33
3.3. Transaction processing services map 34
3.4. Settlement services map 36
3.5. Registry management services map 37
3.6. Corporate actions services map 37
3.7. Safekeeping services map 37
4. Process workflows 38
4.1. Issuance workflow 38

4.2. Trading workflow 41
4.3. Coupon payment workflow 44
4.4. Settlement transaction processing 45
3 | CAST LEGAL & REGULATORY CONSTRAINTS ASSESSMENT 47
1. Roles and legal bindings 49
2. Understanding KYC principles 50
3. Integrating DLT into financial regulation: the European example 51
4 | CAST TECHNICAL FRAMEWORK 53
1. Instrument registry pre-requisites 54
2. Security Token pre-requisites 54
3. Settlement Transaction Repository (STR) pre-requisites 57
3.1. General principles 57
3.2. Business continuity plan 58
3.3. Privacy management 58
3.4. Authentication 59
4. The Oracles 60
4.1. General principles 61
4.2. Registrar setup 62
4.3. Settlement Agent setup 62
4.4. Security holder and agent setup 63
4.5. STR authentication 63
Acknowledgements 65
5 | APPENDICES 66
APPENDIX 1: DEFINITIONS 67
APPENDIX 2: CHALLENGES MATRIX EXPLAINED 71

Executive Summary

This White Paper introduces a comprehensive operational model proposal, the **CAST Framework**, designed for the issuance, custody, and OTC trades of financial instruments on a blockchain (the "**Security Tokens**") published online in an open-source manner. It has been approved and trialed in substantial issuances of Security Tokens realized in 2019, 2020 and 2021 by systemic regulated institutions (banks, supranational, brokers, etc.), notably within the Societe Generale Group.

The purpose of this White Paper is to propose a framework at bank-grade level designed to facilitate the establishment of acceptable market practices for capital market participants (issuers and investors), recognized trusted third parties (banks, investment firms, fund administrators, lawyers, consultants, etc.), as well as start-ups and technology service providers, and to serve as a milestone for ongoing and future discussions with various policymakers and regulators across countries.

The CAST Framework has been designed to hybridize common market standards by major banks related to financial instruments with new approaches related to blockchain-based disintermediation and open-source designs. While the CAST Framework has already been subject to various internal and external approvals by regulated institutions on Security Token issuances, it may evolve over time as it may be adapted to local legal, financial and/or operational requirements, regulatory changes and potential technology improvements. The CAST Framework community is a growing ecosystem which will work on furthering the issuance and trading of Security Tokens and facilitating the gradual industrialization of this new market.

The CAST Framework is constructed around three components: the operational framework, legal & regulatory constraints, and technical rules. Its architecture is based on common reference functions within capital markets. One of the key features of Security Token architecture is to duly identify the roles and responsibilities of the stakeholders involved. Among them, some trusted parties play key roles, including:

- The Registrar, an agent of the Security Token Issuer, which is responsible for registering Investors' positions on the DLT and for keeping the register of the Security Token holders on behalf of the Issuer, and which carries out also in most cases the role of Settlement Agent, an agent of the Security Token Issuer, which is responsible for handling the cash leg of the Security Token transactions, and
- The traditional post-trade and asset servicing actors (e.g. custodians, back office/middle office departments, etc.), whose activities will be substantially impacted by the use of DLT.

Our understanding of the current adoption process of DLTs and Security Tokens by capital market participants (Issuers, Investors, etc.) is rooted in the following key tangible facts:

- Rising interest among institutional Investors for Digital Assets and DLT-based projects;
- The project by major central banks, such as the European Central Bank, to issue central bank digital currencies (CBDCs) by 2025; and
- The current implementation of major regulatory reforms providing legal certainty for Digital Asset projects, such as the EU "MiCA" and "pilot regime" regulations, which will provide rules related to Digital Assets applicable directly at the European Union level by 2022.

1 | CAST OVERVIEW

1. CAST Framework manifesto

In recent years, the blockchain, and Distributed Ledger Technologies (DLTs) more broadly, have entered the financial area with narratives emphasizing the potential revolution or disruption of the financial industry that DLTs can trigger, based notably on the promise of bringing lower operating costs by reducing the number of intermediaries and proposing faster transaction execution. Beyond this, we believe the main benefits of DLTs are much wider, as they give Issuers access to a broader pool of liquidity and allow Investors to build truly diversified portfolios. DLTs will remove most of the current market access barriers, dramatically improving market efficiency and price discovery. Securities and cash will move on a single global network, faster and at a lower cost than at any time before. Securities and cash will exist independently of the infrastructures and entities that currently support them, primarily financial institutions and banks. Operations, control, and monetary policy channels will move away from the infrastructure to the instruments themselves. As a result, ways of financing the economy and implementing monetary policies will evolve. New business models will emerge and existing business models will have to adapt.

The arguments put forward by DLT promoters are often driven by and limited to technological arguments, based on native DLT features such as immutability, automation by code, decentralized governance, or transparency. Proof of concepts produced to promote DLTs are frequently conducted from a technological standpoint only.

In this regard, many discussions have focused on the type of DLTs to be considered, either public/permissionless or private/permissioned ones. Technology is evolving very fast and can reshuffle the cards in either side's favor. Even if this White Paper takes an agnostic approach when talking about DLTs, the authors' firm belief is that new disruptive market infrastructures and new business models can only come with public DLTs and native Digital Assets, in the same way as a new information industry was previously born with the Internet.

DLT promoters barely consider the highly regulated environment of financial markets and the complexity of operations within existing market infrastructures, which are real barriers to adoption.

We believe DLT promises make sense and offer opportunities to challenge existing legal, regulatory, operational and technical frameworks (and their underlying legacy systems).

We believe in DLTs as a lever to initiate a transition phase of hybridization of existing market infrastructures in order to catalyze the adoption of Digital Assets, by accompanying legal, compliance, operational and technical teams in their upskilling and understanding about DLTs.

Accordingly, Digital Assets, notably Security Tokens, should be handled like any other similar assets from a legal, regulatory and operational standpoint. By integrating them into existing financial and banking operations, seemingly insurmountable challenges will be addressed: "practice makes perfect".

To foster the adoption of Digital Assets, we believe it is essential to bring together financial market stakeholders, technology services and consulting providers, and DLT promoters:

- to keep pace with innovation, market demand, and regulatory and legislative policies to deliver on DLT potential;
- to propose a secure, compliant and trusted transition model;
- to promote collaboration and the emergence of standards.

To do so, we believe in an open-source approach in which anyone can contribute on either legal, regulatory, operational, or technical matters in order to build the foundations of shared frameworks and standards and to design new services for members of the eco-system.

2. CAST Framework description

2.1. Native Security Tokens

Digital Assets are "digital representations of value or rights which may be transferred and stored electronically, using Distributed Ledger Technology or similar technology"[1].

From a regulatory perspective, Digital Assets can be categorized in two main subsets: Digital Assets that qualify as financial instruments and Digital Assets that do not:

- Digital Assets that qualify as financial instruments under applicable regulations are commonly called "**Security Tokens**".
- Other types of Digital Assets encompass different subtypes: Utility Tokens, Stablecoins (asset-referenced tokens, e-money tokens), crypto-currencies.

The CAST Framework provides solutions compatible and compliant[2] with traditional banking practices, frameworks, and standards to deal with Security Tokens.

According to the European proposal for a regulation on a pilot regime for listed Security Tokens[3], the "tokenization of financial instruments, that is to say their transformation into crypto-assets to enable them to be issued, stored and transferred on a distributed ledger, is expected to open up opportunities for **efficiency improvements in the entire trading and post-trading area**." Besides, and as stated in the European proposal on Markets in Crypto-assets ("**MiCA**")[4], crypto-assets "have the potential to bring significant benefits to both market participants and consumers. By **streamlining capital-raising processes** and enhancing competition, issuances of crypto-assets can allow for a cheaper, **less burdensome** and more inclusive way of financing notably for small and medium-sized enterprises (SMEs)."

The potential efficiency gains arising from the use of Digital Assets are indeed tremendous, provided existing complexity is not integrated into DLT-based infrastructure solutions. Otherwise, complexity could even be magnified through DLT integration. The CAST Framework was thus designed to provide streamlined solutions that are compatible and compliant[5] with traditional banking practices, frameworks and standards, aimed at avoiding increases in complexity.

---

[1] Article 3(2) of the EU Project Proposal for a Regulation on Markets in Crypto-assets (MiCA).

[2] For the sake of clarity, the term "compliant" refers to compliance with market practices, frameworks and standards adopted by regulated financial entities. Compliance with existing legal and regulatory obligations requires an internal self-assessment by each legal entity interested in developing a Security Tokens issuance and trading project. **The CAST Framework documentation has no contractual value, and does not, and is not intended to, constitute and/or provide legal or professional advice, or certify any compliance with applicable law and/or regulatory requirements.**

[3] See: EU Pilot Regime Regulation proposal: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0594

[4] See: EU Proposal for a Regulation on Markets in Crypto-assets (MiCA): https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020PC0593&from=EN

[5] See note 2.

For this reason, for now, the CAST Framework's scope is limited to so-called **'native' Security Tokens** and does not deal with 'non-native' Security Tokens, as dealing with these might involve importing the complexity inherent to the legacy systems. Native Security Tokens are based on Smart Contracts used to natively manage Investor rights and obligations in respect of financial products and are **considered to be financial instruments**. The EU implicitly follows a "substance over form" policy on the characterization of Security Tokens as financial instruments, as does the US federal regulator, the SEC. Indeed, in 2019, in its consultation document on EU regulation of Digital Assets, the European Commission stipulated that "*where security tokens meet the necessary conditions to qualify as a financial instrument, they should be regulated as such*".

In contrast, non-native Security Tokens are DLT representations of pre-existing financial instruments issued outside of the DLT. Dealing with non-native Security Tokens could thus mean dealing with the existing complexity embedded by the underlying asset, in addition to the DLT integration. On the contrary, handling native Security Tokens streamlines processes and aims at reducing the complexity of current mechanisms.

	Traditional Security	Security Token	
		Non-Native	Native
In scope ?	✗	✗	✓
Blockchain			
Financial Market infrastructure			
Comment		✓ Security token is an "ownership certificate" of underlying security	✓ Security token is an intrinsic financial instrument under applicable laws

Table 1: CAST Framework's scope: native Security Tokens

2.2. Tokenization as a step towards securities digitization

The tokenization of financial instruments[6] represents the second step towards the dematerialization of securities. The first step has consisted in transitioning from a paper representation of securities to an electronic representation (through book-entry account). This transition has taken place in Europe since the 1980s, for example in France in 1981[7], in Switzerland in 2010[8], or more recently in Germany by 2022[9]. With the rise of DLTs, the second step consists in having natively digital securities.

DLTs and the tokenization of financial instruments will enhance innovative solutions to digitalize securities as well as many processes related to their issuance, trade, settlement, and delivery-versus-payment. The

[6] The tokenization of financial instruments refers to the process of digital representation which enables the issuance, custody, and trade of financial instruments on a DLT.
[7] Article 94-II of the Finance Law for 1982, law no. 81-1160 of December 30, 1981.
[8] The Federal Intermediated Securities Act of October 3, 2008, which entered into force in 2010.
[9] German Electronic Securities Regulation due to be adopted in 2021.

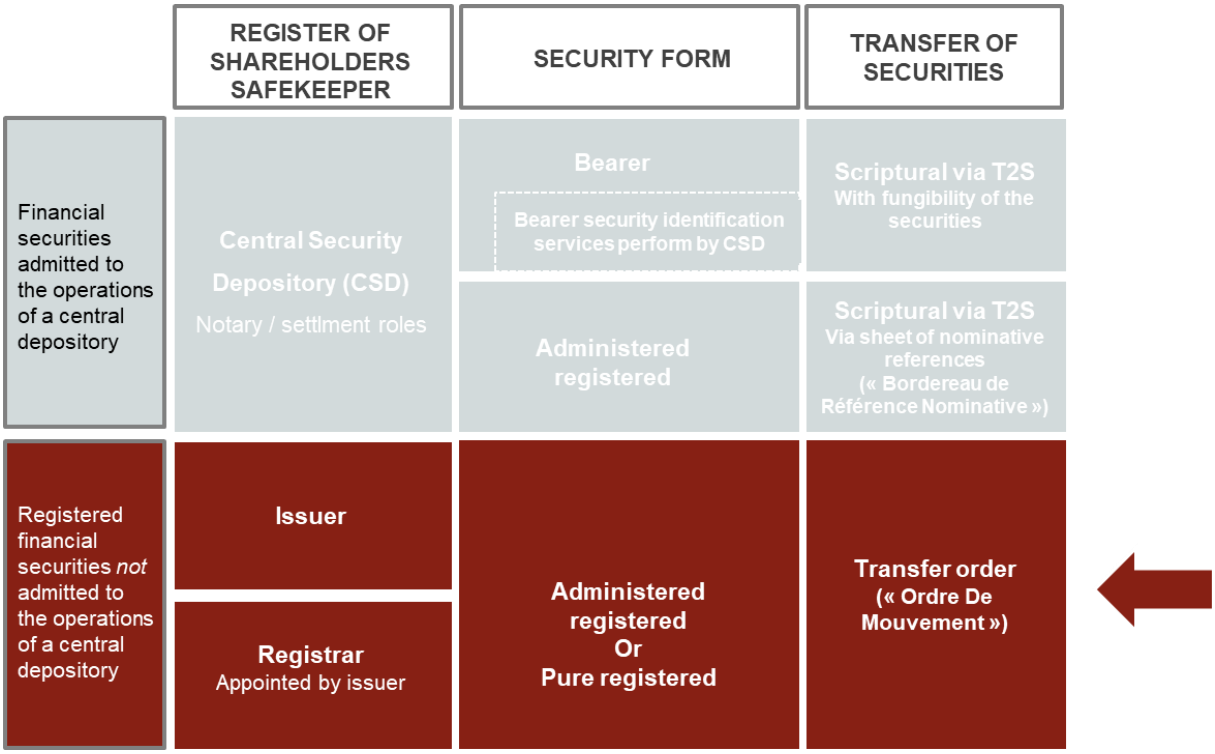
way market infrastructures and their applicable regulations have been designed for the past 30 years relies mostly on book-entry account registration and unautomated verification processes, which are subject to substantial costs and human error. The switch to native digital market infrastructures and digital capital markets will be a key feature of the years to come, and DLTs represent an important step in that direction.

In that process, the CAST Framework is designed as a model immune to national regulatory specifics. However, specific national legal and regulatory aspects related to the issuance, custody, and trading in financial instruments on a DLT remain at that stage and should be taken into account. Current regulatory burdens are the main reasons why market infrastructures such as regulated trading venues (MTFs, ATS, etc.) and settlement service providers (CSDs) are struggling to develop DLT-based projects for the time being, and why the EU is elaborating *ad hoc* rules for DLT-based trading venues and CSDs.

The CAST Framework has been developed to take into account these regulatory and operational burdens encountered by current market infrastructures and participants, and to facilitate the issuance, custody and trading of unlisted[10] Security Tokens. To that end, some countries like France have already provided legal and regulatory certainty for the issuance, custody, and trading of unlisted Security Tokens. The aim of providing regulation for unlisted financial instruments issued on a DLT is to prepare for the next stages, where it will be legally possible to issue, provide custody and trade in listed financial instruments on a DLT. At the EU level, this step could be reached as soon as 2022, after the adoption of the EU “pilot regime” regulation.

Securities law is essential to assess and obtain legal certainty for a Security Token-based project. For decades, securities law has been assessed only at a national level, resulting in numerous discrepancies between the respective existing national securities laws. With Security Tokens there is an opportunity to consider securities law globally from the beginning and to try to avoid the regulatory fragmentation seen in current capital market systems as far as possible. For any Security Token project led by a regulated entity, a comprehensive analysis by the entity’s legal and compliance departments is required. For illustrative purposes, the following table summarizes the securities law applicable to Security Tokens under French law, which provides one of the clearest and most straightforward frameworks for Security Token issuance and trading:

[10] Listed financial instruments refer to financial instruments admitted to trading or traded on a trading venue and recorded in book-entry form by a CSD, while unlisted financial instruments refer to financial instruments which are not admitted to trading or traded on a trading venue and which can be registered in a DLT without being recorded in book-entry form by a CSD.



As in many countries in the EU and elsewhere, the possibility to issue and trade listed Security Tokens remains unclear from a legal perspective in France. For unlisted Security Tokens, which are not admitted to the operations of a CSD, the Security Tokens can take the form of “pure registered” or “administered registered” securities. The bearer form currently seems unsuited to Security Tokens.

2.3. Overview of the CAST Framework

The CAST Framework is intended to bring about an open ecosystem of Digital Asset early adopters. Its initial version has not been designed to optimize the final state of a DLT-based financial industry; many more developments will emerge as adoption grows. It is a proposal to facilitate the transition from the existing financial and market infrastructures as far as possible.

The CAST Framework is constructed around **three components** that propose business rules, a legal/regulatory/contractual assessment, and operational schemes, based on the following pre-requisites:

- Taking a holistic approach covering the whole life cycle of Security Tokens (structured on the basis of this Framework);
- Ensuring interoperability with the current systems in order to facilitate the transition to digitization;
- Securing an internal and/or external review and assessment of operations with regard to current and on-going regulations (KYC-AML, embargoes-sanctions, securities law, etc.);
- Remaining agnostic of underlying DLT technologies in order to have enough flexibility to be able to handle technical developments and the future landscape.

The **legal & regulatory component** refers to a set of roles and contractual setup designed to facilitate the determination of contractual responsibilities and the assessment of compliance with existing regulations and to incorporate the impacts of forthcoming regulatory changes.

The **operational component** covers the whole life cycle of Security Tokens and describes how market participants interact with each other.

The **technical component** provides a set of technical pre-requisites to build technical capabilities and solutions to facilitate integration within current systems.

These components are strongly embedded with each other and must be considered as a whole.

They have been designed to perform the first three real Security Token transactions conducted by Societe Generale – FORGE (SG – FORGE) in 2019[11], 2020[12] and 2021[13].

These real market transactions had to pass internal legal, compliance, risk and technical tests and controls applied by Societe Generale Group and other regulated institutions. They were challenged to obtain the signoffs required to operate in accordance with existing international banking standards.

The content of this White Paper is, however, the sole responsibility of the authors involved and does not engage Societe Generale or Societe Generale - FORGE.

The CAST Framework brings robust answers to the concerns that may be raised by financial institutions' internal stakeholders. It provides building blocks that can be leveraged to develop new capabilities related to Security Tokens, at a lower cost than "starting from scratch", with the certainty of encompassing all required aspects, and the flexibility to adapt to major regulatory, operational and/or technical developments.

The CAST Framework White Paper is subject to change at any time without notice. It is provided for general and illustrative information purposes only and does not, and is not intended to, constitute an investment recommendation or investment advice within the meaning of current regulations. The CAST Framework documentation has no contractual value, and does not, and is not intended to, constitute and/or provide legal or professional advice, or certify any compliance with applicable law and/or regulatory requirements.

This document does not have the aim or effect of creating an attorney-client relationship between the reader, user or browser and its authors, contributors, contributing law firms, service providers and their respective employers. Moreover, the CAST Framework White Paper relates to circumstances prevailing at the date of its publication and may be updated later to reflect subsequent developments. The content on this document is provided "as is". No representations are made that the content is exhaustive and/or error-free. The featured examples are rather used as didactic illustrations to help the reader understand the extent to which the CAST Framework can be applied.

[11] Press release: https://www.societegenerale.com/en/news/newsroom/societe-generale-issued-first-covered-bond-security-token-public-blockchain

[12] Press release: https://www.societegenerale.com/en/news/newsroom/societe-generale-performs-first-financial-transaction-settled-central-bank-digital

[13] https://www.societegenerale.com/en/news/press-release/first-structured-product-public-blockchain

2.4. The components of the CAST Framework

2.4.1. Operational component

The **CAST Framework** provides market participants with a detailed operational mapping of services involved in the whole life cycle of a native Security Token. This service mapping is based on standardized process flows related to major business events (based on ISO 20022). It has been designed in such a way that it is **completely interoperable with current post-trade operations**.

This Framework has been designed around key operational best practices:

- **Identification and assessment of operators' roles and responsibilities**. As explained in chapters 2 and 3, and on the basis of current market practices for unlisted financial instruments, determining the roles and responsibilities of the operational validators of a Security Token transaction *ex ante* is key to ensuring that the financial instruments and the cash will be transferred and received in a safe manner. Two functions are required to settle a transaction: one dedicated to the instrument leg (the Registrar) and one dedicated to the cash leg (the Settlement Agent). The Registrar initiates the transfer of ownership but requires the Settlement Agent's action to settle it. Both functions must act in a coordinated way, and in most cases the Registrar plays also the role of Settlement Agent. In the event where the Registrar is a separate entity from the Settlement Agent, neither can fully process a transaction on its own.
- **DLT-agnostic.** The CAST Framework is technology-agnostic with regards to the choice of DLT, meaning that it can be implemented regardless of the underlying technological choice.
- **Business Continuity Plan**. Under the CAST Framework, a continuity plan must be put in place and maintained to prevent any potential technological disruption and to protect the data registered on a DLT infrastructure (e.g. Ethereum, Tezos, etc.), for regulatory and compliance reasons.
- **Confidentiality**. Only minimal public information about a Security Token transaction is recorded on-chain (in the DLT). Any sensitive information is recorded off-chain (outside of the DLT) in the Registrar's Settlement Transaction Repository (STR). While privacy features are being upgraded by different blockchain communities (for instance using ZKP, mixers, etc.), this off-chain device is currently an optimal solution that meets financial institution's standards and should be adopted by participants in accordance with local regulations. The settings regarding on-chain recordings may evolve at a later stage if privacy technologies advance to the required level of security.

2.4.2. Legal and regulatory constraints

The **CAST Framework** provides market participants with details[14] of the set of agreements needed to legally bind all parties involved in unlisted financial instrument issuance (the Issuer, its Agents, Investors, etc.), which could apply to native Security Token transactions and take into account the main applicable legal and regulatory constraints. The current contractual framework used for financial instrument issuance should be used wherever possible to provide legal certainty to Security Token transactions. The Agency Agreement and the other contractual agreements currently used by financial institutions are designed to be applicable globally and to adapt to any specific regulatory requirements and changes. They allow stakeholders to deal with each other with a clear set of obligations, duties, and responsibilities while regulatory frameworks applicable to Digital Assets are being set up by regulators locally and globally. This Framework is based on the contractual **standards followed by global financial institutions**. It has been tested and validated for Security Token issuance by a large international banking group and by major

[14] See chapter 3 (pp.46-53).

international law firms. It covers very specific issues such as financial crime (KYC/AML, embargoes, and sanctions, etc.) and confidentiality duties and provides a clear framework for Business Continuity Planning and crisis management operations in case of incident.

2.4.3. Technical component

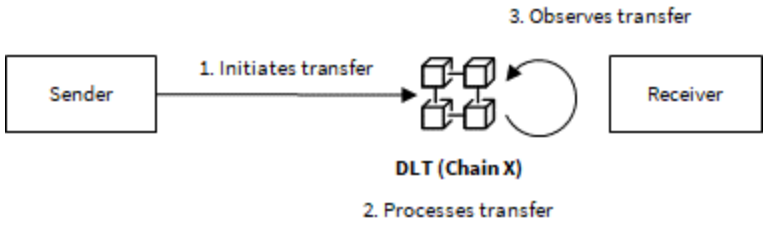
As explained above, the CAST Framework is **technology-agnostic** and **interoperable** with both traditional financial and DLT-based market processes. Market participants can choose to perform their operations with different levels of DLT integration. For instance, native Security Token settlement operations are compatible with the use of fiat money, through existing payment systems such as Target 2 (T2) in the Eurosystem, or they can be settled in Central Bank Digital Currencies (CBDC), using DLT as a digital cash underlying technology layer. Furthermore, in the case of a CBDC settlement, DLT protocol interoperability is possible under the CAST Framework, and the Security Token could be transferred using protocol X (Ethereum or Hyperledger for instance) and settled against CBDC cash transferred on protocol Y (Tezos or Corda for instance).

More specifically, the CAST Framework technical component is based on four pillars:

- The **instrument registry**. The instrument registry is a Smart Contract that records all instruments created by the Registrar on a standardized basis.
- A set of **Security Token pre-requisites**. The CAST Framework provides functional pre-requisites based on high level operational standards defining operational sequencing.
- A **Settlement Transaction Repository (STR)** consists in a technological feature, managed by the Registrar, designed to store key information related to Security Token transactions, notably the identity of Security Token holders or their agents for any specific date and the history of all Security Token holders or their agents since issuance. The STR is a crucial part of the Business Continuity Plan which protects the integrity of the data registered on the DLT from potential technological disruption.
- **Oracles**. DLT integration with existing systems is made possible by the **Oracles**. Based on the **CAST Framework**, the Oracles feed Security Tokens' Smart Contracts with the required data and allow optimal integration of post-market operational chains with DLT infrastructures. The Oracles based on the CAST Framework are shared on an **open-source** basis, which reduces the cost of such integration.

2.5. Understanding transfer management principles

For certain types of Digital Assets (native non-security tokens such as crypto-currencies or Utility Tokens) issued on DLTs, a transfer of Digital Assets occurs when both the sender and the receiver, after agreeing on the terms of the transaction, settle the transaction on a peer-to-peer basis. They can involve a third party (such as a trustee) to implement conditional mechanisms, but basically the sender initiates a transfer on the DLT, then the receiver observes the receipt of the Digital Asset (confirmation mechanisms can be implemented to allow the receiver to confirm receipt).



The main issues with such a setup of disintermediated peer-to-peer transactions are the following:

1) Lack of regulatory checks: any sender can transfer a Digital Asset to any receiver, which raises concerns about the checks required for any transfer between the sender and the receiver from a legal and regulatory standpoint (KYC-AML, sanctions,-embargoes, etc.).
2) Irreversibility of transactions: such transfers are not reversible: only the receiver can initiate a transfer to return a Digital Asset it is not supposed to hold. No trusted third party can alter a peer-to-peer Digital Asset transaction when it has been fully completed and registered on the DLT.

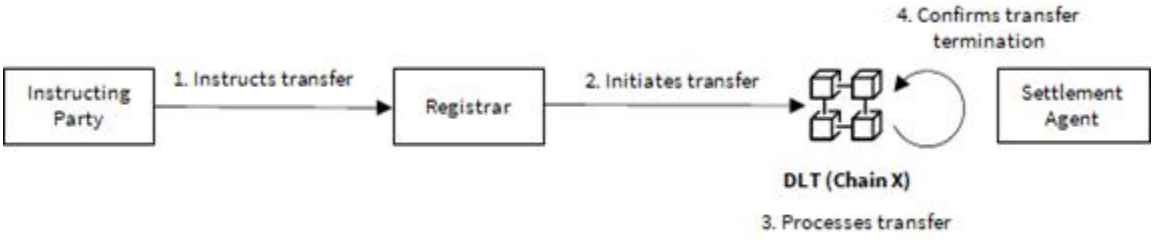
To avoid such concerns, the CAST Framework provides a setup adapted to regulated transactions on financial instruments registered on a DLT:

1) Pre-approvals and regulatory checks before any operation on Security Tokens:

The Registrar (appointed by the Issuer) bears the responsibility for initiating any transfer of Security Tokens on behalf of the Issuer, under conditional approval of the Settlement Agent. The Instructing Party must first instruct the Registrar to do so, either directly or through its custodians or brokers.

Before processing any transfer, the Issuer and/or its Registrar is responsible for conducting KYC diligence on both the sender and the receiver to ensure that the regulatory conditions are met for such transfer.

The Settlement Agent (appointed by the Issuer) must confirm the termination of the transfer. This confirmation may be conditional on any other obligation related to the transaction (e.g. payment obligation).



As a consequence, under the CAST Framework, a sender and a receiver cannot perform any transaction involving the transfer of Security Tokens without the intermediation of a trusted third-party, the Registrar, duly appointed as such by the Issuer.

This setup ensures that any transaction involving a transfer of Security Token has been checked (from a legal and regulatory standpoint, notably regarding KYC/AML and embargoes-sanctions issues) since its inception.

The responsibilities of both the Registrar and the Settlement Agent are coded directly in the Security Token's Smart Contract and are documented in the issuance contractual framework.

2) Possibility of adapting to technological or regulatory constraints:

On the occurrence of any regulatory issue (e.g. an Investor red-flagged for embargoes-sanctions reasons) or technological issue (e.g. a temporary disruption of a DLT), the Registrar acting on behalf of the Issuer should have the possibility to block a potential Security Token trade for a given Investor, to freeze a given Investor's Security Token and to provide technological solutions to switch from one DLT to another or from a DLT to current infrastructures if necessary.

3. CAST Framework ecosystem/community

Created under an open-source and inclusive philosophy in order to maximize take-up, provide incentives for regulated institutions to develop their DLT-based projects, and facilitate the adoption of market standards for Security Tokens compatible with the ones of traditional financial instruments, the CAST Framework is designed to be analyzed, implemented, and improved by various kinds of stakeholders.

To facilitate the gradual adoption of the CAST Framework and common market practices by many types of corporations and foster their participation and inputs to enhance its effectiveness for various use cases, a Governance Body will be set up. The Governance Body will bring together the main stakeholders interested in Digital Asset and Security Token projects (banks, start-ups, technology service providers, financial institutions, etc.) to govern the CAST Framework and amend it from time to time if necessary. The philosophy of the Governance Body will be based on the following pillars: the development of new business models based on digital technology and open-source digital ecosystems, breakthrough innovations, and the technological modernization of market participants and of financial services provided to clients.

Market participants (banks, financial institutions, fund administrators, etc.) could consider the CAST Framework as a way to advance their ongoing experimental and/or industrial Security Token projects. At the same time, public officers (legislators, regulators, central banks) could more accurately assess the fine line between existing market infrastructures and their potential future developments, while various kinds of service providers, start-ups, experts and entrepreneurs (in finance, , technology, consulting, legal or other areas) could strengthen their service offers related to Security Tokens and tokenization projects at a banking-grade level.

The various players that we consider to be stakeholders of the CAST Framework ecosystem/community notably include the following:

- **Financial institutions** keen to benefit from the advantages Digital Assets can offer**.**

Using blockchain technology and Digital Assets provides new business possibilities and efficiencies (e.g. lower nominal issuance, new kinds of asset structuring through computer code, access to new pools of Investors and markets), greater transparency, because the ledger is viewable by all market participants, built-in encryption, improved traceability, the ability to settle transactions and provide trade and post-trade operations at speed, reduced complexity, and lower operating costs.

For sensitive trades, it is also possible to restrict which entity can hold, buy or sell a specific asset, both on the primary and the secondary trading markets. Given market regulators' increasing focus on matters of national security and concerns regarding money laundering and financial crime — however broadly this may be defined — this level of control is highly attractive for regulated entities.

- **Central Banks.**

The rise of digital currencies poses direct challenges and brings opportunities for Central Banks. If a private digital currency were successful, it could remove large parts of the total value stored and exchanged in society from the Central Bank's control. The Central Bank would lose control of the money supply, at least in part, and might find itself less able to use its ability to set interest rates as an effective tool of monetary policy. In addition, the creation of a digital currency (e.g. an e-euro, an e-dollar or an e-yuan) by a Central Bank could be a significant way to enhance its use and sovereign impact worldwide. These are some of the reasons why Central Banks are now investing heavily in researching and testing Central Bank Digital Currencies (CBDCs) and why many are looking for private partners with experience in the market for tokenized assets to assess and experiment CBDCs' wider potential.

- **Policymakers/Legislators**[15] **with an appetite to promote innovation.**

The global fintech market will be worth an estimated $309.98 billion by 2022 and is growing at a rate of around 25% a year [1]. Legislators and policy makers more generally have a clear interest in helping this sector grow and in trying to capture as much of it as possible for the markets they govern and represent.

For further context, we can see this in the EU's release of its Fintech Action Plan in 2018 and in the European Commission's adoption of the Digital Finance Package in September 2020, designed to give technological innovators in Europe the legal and regulatory framework they need to expand and diversify, as well as in the French government's "Action Plan for Business Growth and Transformation" (PACTE), and the recent UK government review into that country's fintech sector and other similar national plans.

The global financial market as a whole is valued in the trillions. Global bond markets and global equities alone are estimated respectively to be worth $128.3 trillion [2] and $90 trillion [3]. As more and more of this market is traded using technologically innovative platforms and instruments, the jurisdictions that foster the greatest technological innovation in their financial sectors will benefit the most.

- **Regulators that have created frameworks for blockchain innovation and want to enhance their adoption by market participants for industrial/experimental purposes.**

The worldwide blockchain market is forecast to grow by 69.4% between 2019 and 2025, reaching a market value of $57 billion [4]. Based on current forecasts, however, the EU's share of this market will be worth less than $10 billion [5].

[15] [1] https://www.prnewswire.com/news-releases/global-fintech-market-value-is-expected-to-reach-309-98-billion-at-a-cagr-of-24-8-through-2022--300926069.html
[2] Estimate by the ICMA of the overall size of the global bond markets in terms of USD equivalent notional outstanding as of August 2020: https://www.icmagroup.org/Regulatory-Policy-and-Market-Practice/Secondary-Markets/bond-market-size/
[3] https://www.cnbc.com/2019/12/24/global-stock-markets-gained-17-trillion-in-value-in-2019.html
[4] www.prnewswire.com/news-releases/the-global-blockchain-technology-market-size-is-expected-to-reach-usd-57-641-3-million-by-2025--registering-a-cagr-of-69-4-from-2019-to-2025--300902333.html
[5] https://www.idc.com/getdoc.jsp?containerId=prEUR145465319

An important means to sustainably increase the development of digital capital markets at national and global level is to create *ad hoc* bodies, organizations or working groups to develop dialog between public policymakers and private participants on the emerging disruptive changes. The development of digital capital markets would be assessed through real life experimentation based on blockchain technology (beyond the "proof-of-concept" hype). This applies as much to regulators as it does to financial professionals and technologists. Experiments can be realized by market participants (issuance, secondary markets) as well as by public institutions (e.g. the EU "pilot regime" regulation on listed Security Tokens which is under adoption in Europe).

To build a regulatory framework that is robust, transparent, flexible, scalable and fit for purpose, regulators can benefit from providing open discussions and collaborating with private companies on live examples of blockchain-based products being traded in the market. It may be not sufficient to work only with beta or proof-of-concept platforms and products. These innovations need to turn into real, fully-fledged, if appropriate fully regulated, operating models and operations and they must be designed to gradually move to industrial mode.

Providing such a well-governed regulatory framework with appropriate legal certainty is key to building a successful Digital Asset and DLT market in which legal certainty is a given and in which Investors and market participants have full confidence and are willing to actively engage. For this reason, regulators, like policymakers, are displaying a strong interest in encouraging regulated financial institutions to expand into Distributed Ledger Technology, Digital Assets and other areas of financial technological innovation and are actively lending their support.

- **Fund administrators, asset servicing providers, and transfer agents.**

At a time when the institutional investment community is under constant and ever-more aggressive operating and margin pressure, fund administrators, asset servicing specialists, and transfer agents are considering new business opportunities and cost efficiencies. Client interest in Digital Assets, securitization, and tokenization is increasing, even turning into clear demand. Market models are responding – some aspects will be fully transferable (such as corporate actions, pricing, and rates), while other requirements will likely evolve as the market matures. Firms are considering the impact this will have on their role, operational response, and service models locally, regionally, and globally.

- **Corporates.**

Corporates are interested in finding new instruments with which to attract Investors. Working with specialists in tokenized assets gives them the opportunity to offer the market new and innovative financial products, helping to attract institutional (and potentially retail) Investors at favorable rates. These stakeholders will benefit from the increased transparency and network effects DLT can bring to their investor and client base.

- **Technology integrators and consulting firms** — often the large and well-known consultancy firms that lead the B2B technology and services market — are looking for ways to help crypto-clients integrate mainstream market platforms and established financial platforms integrate Digital Asset markets**.**

An open-source, blockchain-agnostic framework that offers these firms the ability to successfully and easily embrace and bridge both blockchain and their clients' current technologies should be of great interest.

A certification program has been designed to make it easier for certified companies to offer services and advise their clients on their use and to facilitate implementation of the Oracles and the CAST Framework.

- **Technologists and professionals** looking for trusted partners with which to study and/or develop digital financial products**.**

Companies that specialize in blockchain- and Digital Asset-related products often need partners with which to develop their products. There are several reasons for this:

- Many blockchain and fintech providers focus exclusively or mainly on the technology. Engaging with the regulatory and other requirements needed to develop their own financial products may undercut their fast-moving, low-overhead business model. To overcome this limitation, develop products for their technology platforms and find clients, these technology firms need partners with financial services expertise.
- Smaller Digital Asset specialists may not have the resources to do this on their own. We have seen this since the introduction of the EU directive AMLD 5. The stringent regulatory requirements may have been too much for some crypto firms, forcing them to close because they could not re-engineer their systems to be sufficiently, let alone fully, compliant.
- To gain a wide audience, Digital Asset exchanges and other services need a high level of interoperability with the financial services platforms and systems already in use. This can be achieved much more easily by working with established and regulated partners.

Subgroups within this audience include:

- Core developers of the underlying blockchain tech stack looking for ways to accelerate the development of new features and products while ensuring ease of integration and full regulatory and governance compliance,
- Digital Asset exchanges and communities that want to plug into broader capital market frameworks and platforms as a way of extending their institutional reach,
- ICO groups that want a quick path to meeting regulatory standards, as a way of boosting their credibility without incurring prohibitive costs or technical overheads,
- Specialized blockchain fintechs that wish to offer their products and services on technical platforms that are interoperable and give them a wider audience reach,
- Academics, experts, and trade associations willing to conduct in-depth studies of the financial, regulatory, technological and/or operational aspects of the financial instrument tokenization process and its potential impacts and new market standards, practices, and regulations.

- **Other initiatives / Competitors (or “Co-opetitors”).**

The reaction of competitors to open-source platforms and the CAST Framework depends on their approach to the blockchain and tokenized assets markets. If they are intent on building their own closed systems, then this will appear to them as a potential threat. For many, however, the creation of an open framework (described below) will present a great opportunity. Such an open framework offers the opportunity for many firms to easily participate and align their systems and platforms within it, therefore increasing interoperability and reach, generating potential, guaranteeing liquidity, and providing considerable mutual value.

4. Key challenges

4.1. Capital market constraints

Integrating DLT within capital market infrastructures not only requires strong technical capabilities but also a deep understanding of the multiple constraints of capital markets. The complexity of financial regulation and capital market infrastructure operations must be tackled upfront to enable successful DLT integration within capital markets.

Understanding the key concepts of capital markets and current regulatory and operational constraints thus appears as a pre-requisite for DLT integrators and security token stakeholders.

In the particular case of the integration of security tokens, key elements that must be managed cover the following topics:

- Defining the key notion of ‘financial instruments’ (securities);
- Securities’ life cycle;
- Capital markets key stakeholders and their respective roles;
- Legal and Regulatory framework principles;
- Key concepts of safekeeping and security transfer.

4.2. Business challenges coverage

The CAST Framework aims at providing practical propositions for **DLT integration** within current financial infrastructures. The objective is to facilitate the issuance, trading, and post-trade processing of native Security Tokens, taking into account capital market regulatory and operational constraints. We believe providing a clear framework that considers the potential challenges stakeholders may face for DLT integration should facilitate and accelerate adoption.

4.2.1. Challenges matrix

Distributed Ledger Technologies (DLTs) have the potential to promote data sharing and collaboration in financial business processes beyond the level achieved by current distributed databases. DLTs have the potential to add value to market players by allowing different institutions to share the management of information in a distributed ledger and perform common procedures to update this information. DLTs have the potential to bring new opportunities and efficiencies to the financial industry at the global level. The strengths of these technologies include:

1. Full traceability / Full transparency
2. High resiliency
3. Data consistency
4. Consensus disintermediation benefits
5. Simplified settlement and reconciliation

However, these technologies are still at an early stage of development and must respond to various challenges. As with any emerging technology, challenges and doubts exist around DLT reliability, speed, security, and scalability. The challenges raised by integrating DLT can be categorized into three main groups:

1. Operational risks and costs
2. Regulatory requirements
3. DLT features and maturity

OPERATIONAL RISKS AND COSTS	REGULATORY REQUIREMENTS	DLT FEATURES	DLT MATURITY
Execution risk	Strict and diversified financial regulations	Emerging forms of cyber attacks	Scalability
Lack of standards	Knowledge gap of legal agents	Immutability	Interoperability
High cost to implement	Regulatory uncertainty	Identity framework	Insufficient infrastructure
Resiliency	Business Continuity Plan	Intellectual property	Unchartered territory
Data management	Confidentiality	Decentralized governance	Lack of Accountability

An explanation of each of the challenges listed here is provided in the APPENDICES*.*

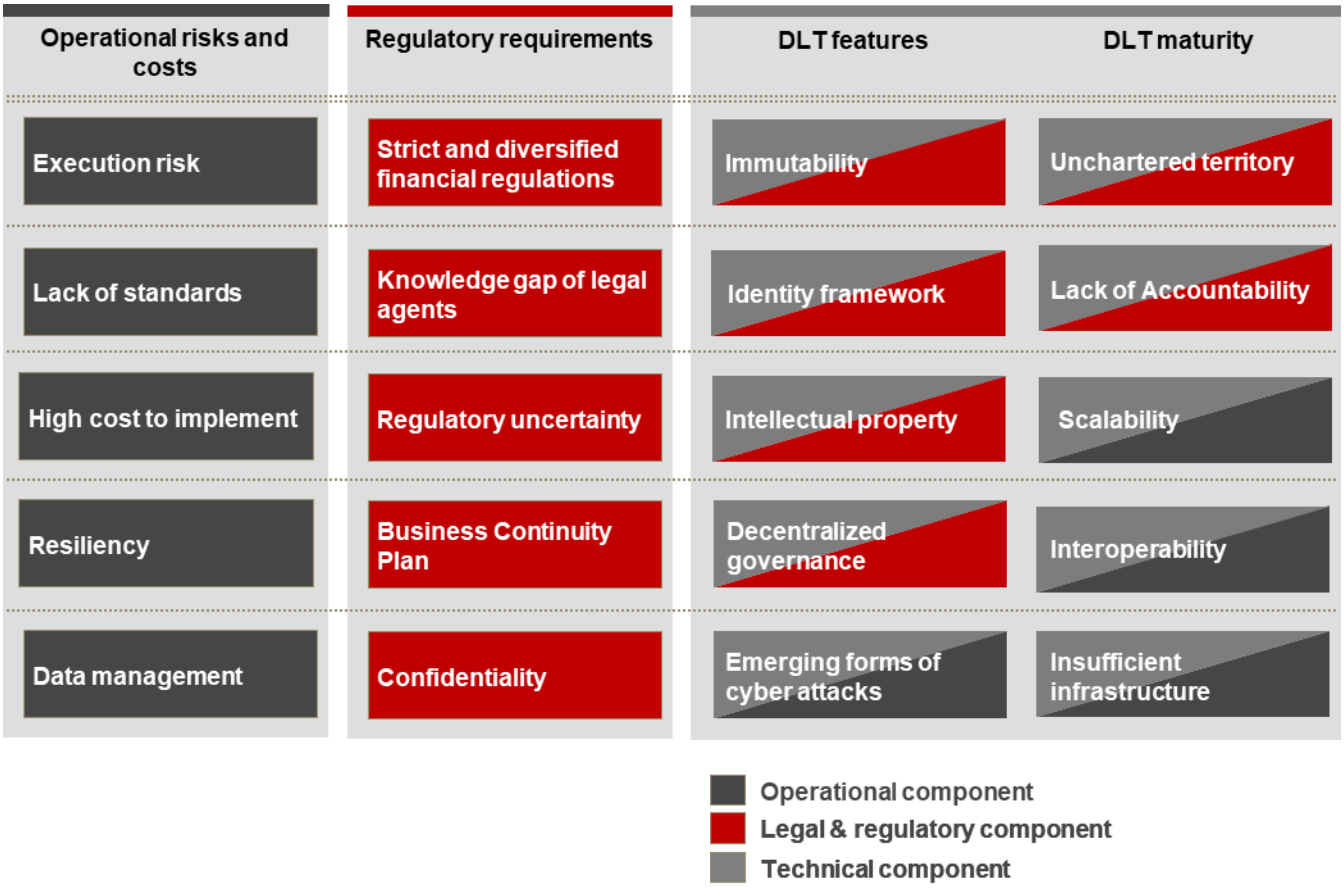
4.2.2. Addressing these challenges with the CAST Framework

The CAST Framework has three main components:

1. An operational component
2. An assessment of legal & regulatory constraints and contractual possibilities
3. A technical component

Each of these components provides market participants with a set of practical elements helping them deal with these challenges, as mapped below:

- Black boxes indicate that these challenges are covered by the operational component;
- Red boxes indicate that these challenges are covered by the legal and regulatory component;
- Gray and black boxes indicate that these challenges are covered by both technical and operational components;
- Gray and red boxes indicate that these challenges are covered by both technical and legal & regulatory components.


Operational risks and costs
Regulatory requirements
DLT features
DLT maturity
Execution risk
Strict and diversified financial regulations
Immutability
Unchartered territory
Lack of standards
Knowledge gap of legal agents
Identity framework
Lack of Accountability
High cost to implement
Regulatory uncertainty
Intellectual property
Scalability
Resiliency
Business Continuity Plan
Decentralized governance
Interoperability
Data management
Confidentiality
Emerging forms of cyber attacks
Insufficient infrastructure
Operational component
Legal & regulatory component
Technical component

2 | CAST OPERATIONAL FRAMEWORK

The main objective of the operational component of the CAST Framework is to provide a global understanding of the operational challenges arising in the management of a Security Token and its related transactions, based on:

- a set of common definitions;
- a cartography of existing and new services involved in the whole life cycle of a Security Token;
- a description of process flows related to major business events;
- considerations about the many different ways of adapting existing services to manage Security Tokens.

This framework brings flexibility to implement a Security Token value chain in very different ways, leveraging existing services and infrastructures.

This framework is agnostic of the type of DLT and payment systems used.

1. Roles and responsibilities

The intrinsic characteristics of DLT lead to a partial transformation of the roles undertaken by market participants.

The CAST Framework proposes an environment in which stakeholders can adapt their operations to progressively integrate all the potential that DLT may bring to help optimize their processes.

Service providers may take one specific role or a plurality of roles, depending on their business strategy, capabilities, and the regulatory environment where they perform their activities.

A set of potential contractual agreements associated with the CAST Framework would detail and govern the various roles undertaken by market participants interfacing DLT with current systems, as described below. While they should be adapted to internal stakeholders' assessments and to each project considered, they can provide stakeholders with a solid framework in which they can safely interact.

The major roles covered by the CAST Framework are listed below:

Role	**Responsibilities**
Issuer	• Issues the Security Tokens • Based on the advice of the Lead Manager and/or Structuring Manager, selects the type of registered form and the type of DLT used to record the Security Tokens • Is responsible for recording of noteholders and transaction on the DLT • Can appoint Agents (through an Agency Agreement) to be responsible for noteholder registration, transaction recording on the DLT, registry keeping and settlement execution
Structuring Manager	• Determines the Security Tokens' financial terms with the Lead Manager • Determines the key structuring features of the Security Tokens' Smart Contracts covering their issuance, registration, transfer, and custody in accordance with the relevant Security Tokens' term sheet of the issuance
Lead Manager	• Facilitates the purchase and sale of Security Tokens

Registrar	• Is responsible for developing the Security Tokens' Smart Contract • Provides on-chain registration of the Security Tokens on the DLT upon issuance and transfer • Performs duties as defined by applicable law, or that fall under the regulation of the country of activity and acts on behalf of the Issuer: ✓ Compliance monitoring, including KYC diligence with regard to Security Token holders; ✓ Delivering notices to the Security Token holders; ✓ Processing of all notifications including subscriptions, redemptions and conversions; ✓ Processing of the Security Token's transfer upon receipt of appropriate instructions; ✓ Processing of dividend/distribution payments and reinvestment instructions.
Fiscal Agent	• Handles the fiscal duties related to dividend/distribution payments and reinvestments • Liaises with competent tax authorities in this respect as required by the Issuer
Calculation Agent	• [If relevant] Determines the amount of payment owed by the Issuer to Security Token holders
Settlement Agent	• Proceeds with: ✓ the cash settlement related to the Security Token upon issuance ✓ the different payments owed by the Issuer to Security Token holders, including coupon payments and redemptions ✓ the cash settlement related to the transfer of the Security Tokens on the secondary market
Custodian	• Provides solutions for the storage of the private cryptographic keys associated with a financial instrument on behalf of Investors and/or additional safekeeping services ("**Custody services**")
Issuance Facility Operator	• Provides a technical platform to process issuance • Is responsible for providing the Registrar with all transaction data required for on-chain registration (of the noteholders) and transaction settlement • Provides a KYC/AML authentication mechanism applying to its users (dealers, Investors and Issuers)
OTC Facility Operator	• Provides the reception and transmission of orders service and/or order execution on behalf of Investors • Is responsible for providing the Registrar with all transaction data required for on-chain registration (of the noteholders) and transaction settlement • Provides a KYC/AML authentication mechanism applying to its users (dealers, Investors and Issuers)
Smart Contract auditor	• Performs an independent audit of the Smart Contracts to ensure computer code development best practices are met and compliance with the financial terms of the Security Tokens
Crypto-Asset Service Provider (CASP)	• [If relevant] Any person whose occupation or business is the provision of one or more non-securities Digital Asset services to third parties on a professional basis

2. Key features of the operational component

2.1. Focus on transaction management for Security Tokens

The following focus presents a high-level perspective for the transaction management process applicable for primary and secondary markets. The aim is to maintain an operational management system which ensures an interoperability with the current existing post-trade systems.

A **transaction** is an agreement between parties to transfer Security Tokens from party A to party B, expressed in terms of delivery and/or payment obligations.

A **delivery or transfer obligation** refers to the obligation for a party (the sender) to transfer securities to its counterparty (the receiver).

A **payment obligation** refers to the obligation for a party (the sender) to transfer funds to its counterparty (the receiver).

The terms of the obligations are undetermined at the time of the transaction agreement.

A transaction can have none or many delivery obligations. The **delivery leg** refers to all delivery obligations related to a transaction.

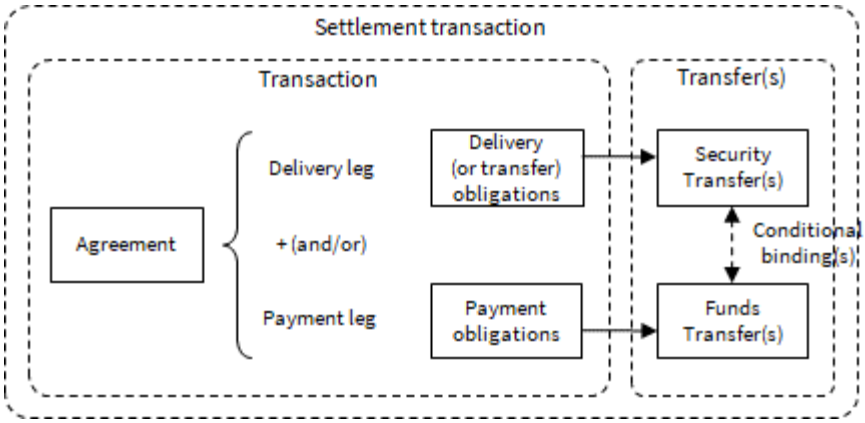
A transaction can have none or many payment obligations. The **payment leg** refers to all payment obligations related to a transaction.

Both the delivery and the payment obligations are expressed in terms of **transfers** (either funds or securities) with conditional and/or unconditional bindings.

In order to settle a transaction, the parties involved must provide information on how to settle each obligation. The **settlement instructions** provide the required information (e.g. intermediaries, accounts, etc.) to settle obligations by determining the transfers to be performed.

The settlement instructions are sent to all participants involved in the settlement process. From the sender's or the receiver's perspective, settlement instructions can be categorized as **delivery instructions** or **receipt instructions**.

A **settlement transaction** refers to the combination of a transaction and all related transfers.



The **settlement method** refers to the method by which the obligations of a transaction are settled. It defines, if need be, the conditional processing between both the delivery and payment legs. For instance, the DvP settlement method states that the transfer of a security only happens after the payment is made.

Below are the most common settlement methods:

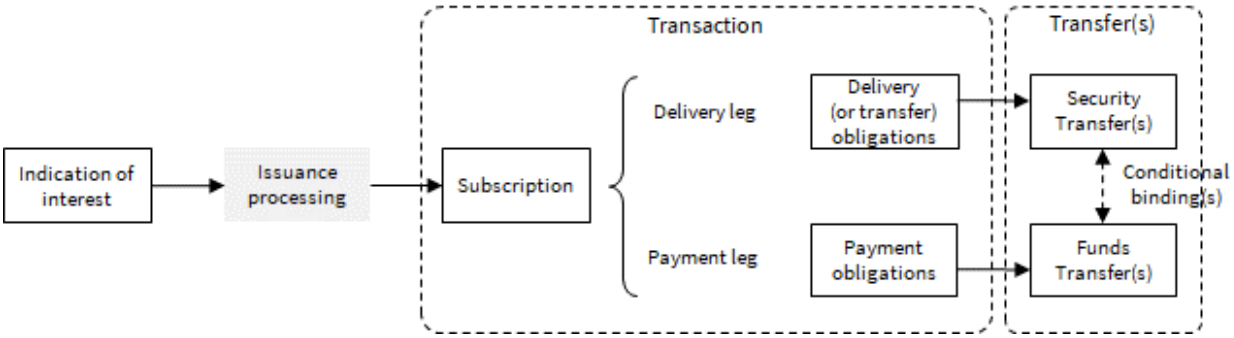
Settlement method	Delivery leg	Payment leg
Delivery-versus-Payment (DvP)	✔ (1 obligation)	✔ (1 obligation)
Payment Free of Delivery (PFoD)	✘	✔ (1 obligation)
Delivery Free of Payment (DFoP)	✔ (1 obligation)	✘
Delivery-versus-Delivery (DvD)	✔ (≥2 obligations)	✘
Payment-versus-Payment (PvP)	✘	✔ (≥2 obligations)

The settlement method has an impact on the way the settlement instructions are structured. Depending on the settlement method, the delivery, receipt, and payment instructions can be expressed separately or combined:

Settlement method	Settlement instructions
Delivery-versus-Payment (DvP)	• Deliver versus Payment (DvP) instruction (e.g. Swift MT543) • Receive versus Payment (RvP) instruction (e.g. Swift MT541)
Delivery Free of Payment (DFoP)	• Deliver Free (DF) instruction (e.g. Swift MT542) • Receive Free (RF) instruction (e.g. Swift MT540)

An **indication of interest (IOI)** is an underwriting expression showing a conditional, non-binding interest in buying a Security Token that is currently in registration.

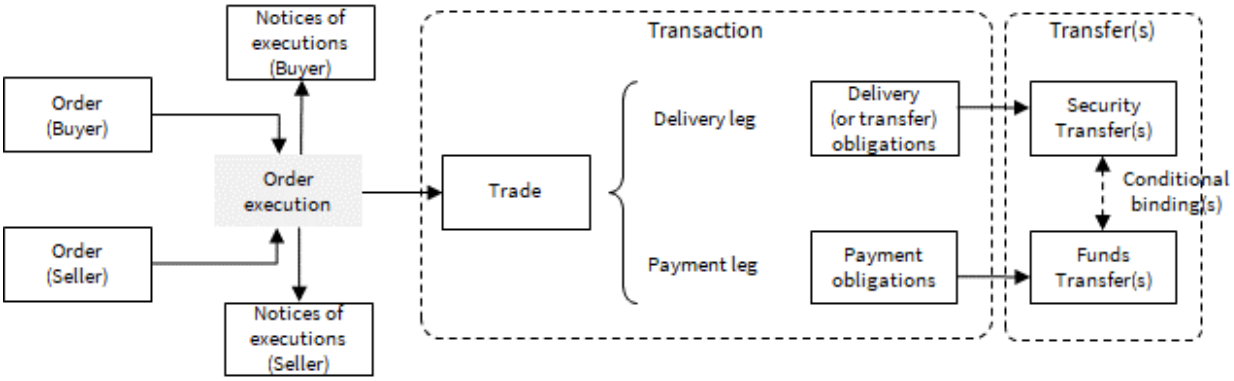
An IOI is originated by an Investor (instructing party) and submitted by its dealer (executing party) during an issuance process. Once the issuance allocation step is performed, the IOI is converted into a **subscription**, which is a transaction/agreement to buy a security against payment. At the time of the agreement the security is generally not yet issued.



An **order** is an instruction to buy or sell a security.

Execution refers to the process by which the order is completed. Completion is reached by matching opposite orders. The details/terms of the execution are communicated to the parties involved through a **notice of execution (NOE)**.

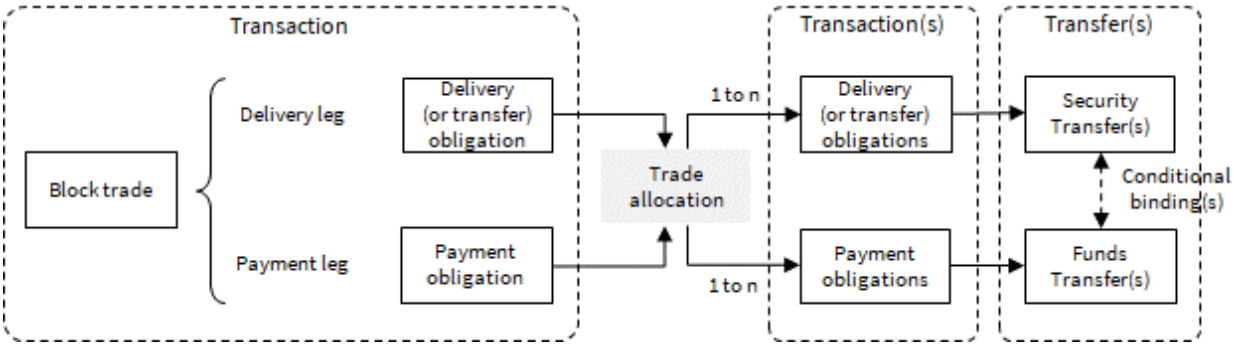
A **trade** is a transaction referring to the result of an order execution. An order execution can generate one or more trades.



A **block trade** is a high-volume trade, generally negotiated privately by execution parties (brokers/dealers) on behalf of a large number of instructing parties.

Trade allocation consists in splitting the block trade delivery and payment obligations across the instructing parties (which can in return split their obligations across their clients) for settlement.

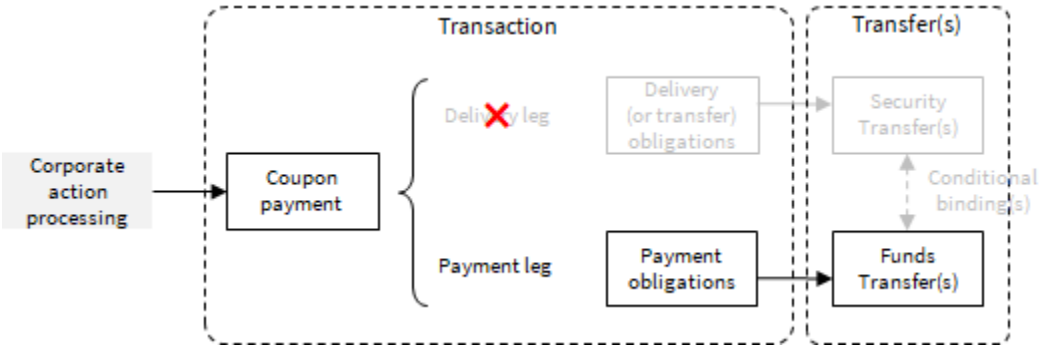
As a consequence, a block trade transaction can result in one or many transactions, depending on the allocation mechanism used.



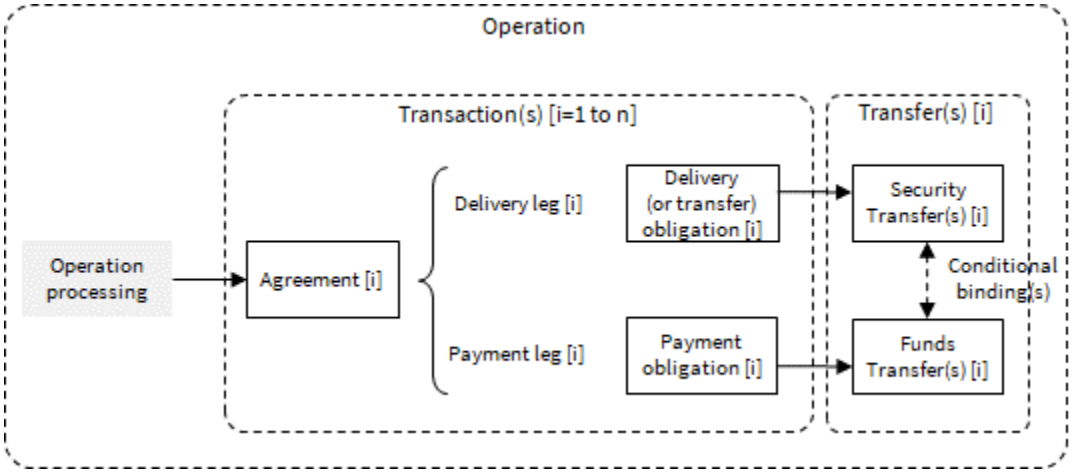
A **corporate action** is a voluntary, mandatory with choice, or mandatory corporate event that can bring a change to the related Security Token and/or its life cycle.

Some corporate actions such as a dividend or coupon payment may have a direct impact on Security Token holders. Such events will result in one or many transactions, generated during the processing of the corporate action.

For instance, a coupon payment results in as many payment transactions as there are security holders:



An **operation** refers to any event/process resulting in the generation of one or many transactions (and their related settlement transactions).



Below are some examples of operations:

Operation	Transactions
Issuance	1-to-n transactions (subscriptions) between the Issuer and subscribers
Trade	1 transaction (trade) between the buyer and the seller
Coupon payment	• 1 transaction (coupon payment) between the Issuer and the Paying Agent • 1-to-n transactions (coupon payments) between the Paying Agent and the security holders • Conditional binding: the fund transfers between the Paying Agent and the Security Token holders are conditional on the fund transfer between the Issuer and the Paying Agent
Redemption	• 1-to-n transactions (redemptions) between the Security Token holders and the Issuers

2.2. Focus on business terms for Security Tokens

A **term sheet** is an indicative document that shows the basic terms and conditions of an issuance and the characteristics of the instrument to be issued.

The **final terms** refer to the definitive terms and conditions of an issuance and the characteristics of the instrument to be issued.

2.3. Focus on safekeeping of Security Tokens

A **safekeeping account** is an account (generally a record in a book-entry system) maintained by an **account servicer** on behalf of an **account owner**, with the purpose of holding traditional securities.

A **cash account** is an account (generally a record in a book-entry system) maintained by an **account servicer** on behalf of an **account owner**, with the purpose of recording all cash-related transactions, notably cash receipts and payments.

A **crypto account** is a concept proposed under the CAST Framework designed to encompass the public cryptographic key, the private cryptographic key and the public address of a given holder of Security Tokens or other kinds of Digital Assets. A crypto account is provided by a **crypto servicer** to a **crypto owner** or generated by the crypto owner itself, for the purpose of holding Security Tokens or other kinds of Digital Assets for a specific DLT. Unlike a safekeeping or cash account, it is not a record in a book-entry system, but it is based on a (cryptographic) private key whose detention acts as a proof of ownership. A public key is derived from the private key which in turn is derived into a public address. This public address can be considered as the account number of the crypto account.

A **wallet** is a storage solution for private keys. By extension, a wallet is a safekeeping solution for crypto accounts.

A **custodial wallet** is a wallet where private keys are provisioned and stored by a third-party (the Crypto-Asset Service Provider).

SSI (“Standard Settlement Instructions”) are settlement instructions that have been agreed in advance. They serve as a reference for transaction settlement, indicating the default securities and/or cash accounts to be used.

Crypto SSI are equivalent to SSI. They indicate the default crypto accounts to be used for transaction settlement involving tokens. They can include default cash accounts to be used if the payment leg of a transaction is settled in traditional cash.

3. Services map

The services map identifies all the functions or services involved in the Security Token life cycle, without pre-empting the underlying technologies used (DLT or current technologies) or the service providers.

It is a generic map that can be used as a set of building blocks for designing new Security Token services or operational and technical capabilities (e.g. Issuance Facility, trade confirmation utility, etc.), and for identifying integration pre-requisites with current services or systems.

Services map

Issuance		Origination	Structuration	Placing	Issuance processing
Trading		Order routing	Order execution		
Post-trade	**Transaction processing**	Transaction capture	Trade allocation	Trade confirmation & affirmation	Settlement instructions notification
		Position management	Pricing & valuation	Risk management	Referential management
		Accounting management	Treasury management		
	Settlement	Settlement transaction processing	Fail & claim management		
Asset Servicing	**Registry Management**	Settlement instructions processing	Record keeping	Audits	
	Corporate actions	Tax duties processing	Corporate actions processing		
	Safekeeping	Securities safekeeping	Securities administration	Tax duties management	

3.1. Issuance services map

Services	Description
Origination	• Refers to the services provided to the Issuer, including market insights and advice, • Responsibility of the originator, generally an ECM (Equity Capital Markets) or DCM (Debt Capital Markets) team in association with the Issuer
Structuring	• Refers to the determination of the characteristics of the Security Tokens to be issued (e.g. type of instrument, underlying DLT, etc.), or modelling; • Responsibility of the Structuring Manager appointed by the Issuer
Placing	• Refers to the search for Investors on behalf of the Issuer; • Responsibility of the Lead Manager appointed by the Issuer
Issuance processing	• Refers to the execution of the issuance, including: ✓ Term sheet production; ✓ Book building (IOI collection); ✓ Allocation; ✓ Price fixing; ✓ Final terms production; ✓ Instrument creation; ✓ Book execution (IOI conversion into subscriptions); • Performed by the Registrar, on an electronic platform provided by an Issuance Facility Operator, as mandated by the Issuer.

During the issuance phase, most of the services are performed off-chain, leveraging current services.

While the origination phase aims at increasing issuance opportunities for the Issuer, the purpose of the structuring phase is to identify the type of instrument to issue, with the relevant terms and conditions, and to design the expected features of the Security Token.

The underlying DLT to be used depends on criteria fixed by the Issuer and the Structuring Manager, but also on available services (e.g. off-the-shelf or customizable Smart Contract libraries) provided by the Registrar that match those criteria.

The Issuer appoints the Registrar and the Settlement Agent (some Registrars and Settlement Agents may offer joint services, and in most cases the Registrar will also carry out the role and functions of a Settlement Agent), through an Agency Agreement.

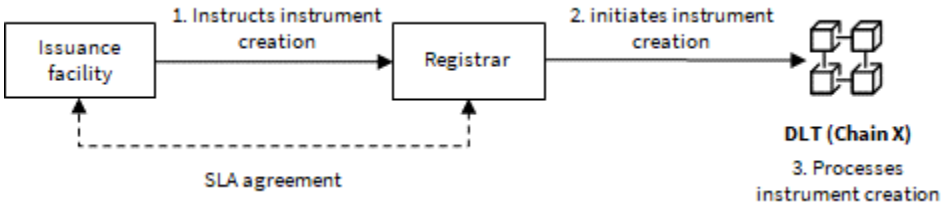
For the placement phase, if applicable, the Issuer generally appoints a dealer as Lead Manager to search for Investors. In case of syndication, a group of underwriters is set up by the Lead Manager. The dealer and the underwriters act as executing parties for the Investors (instructing parties).

The Issuer also contracts with an Issuance Facility Operator to process the issuance by the Registrar on its Issuance Facility.

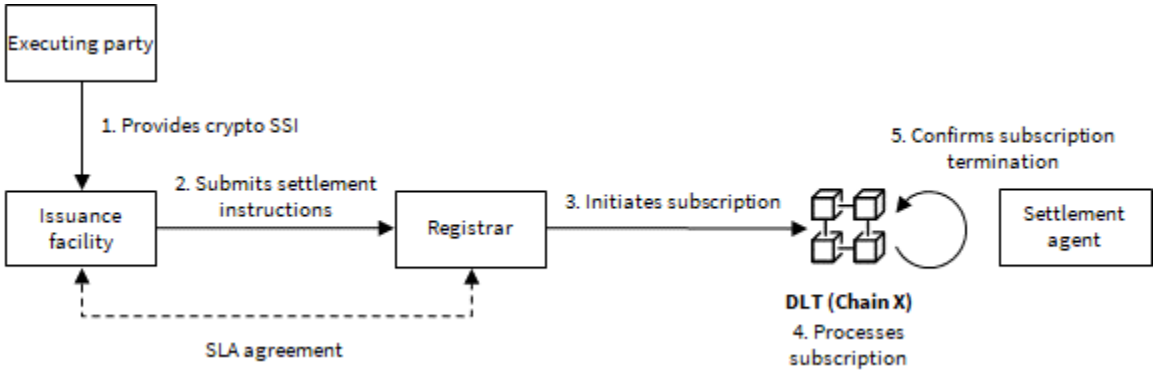
The Issuer and Registrar apply their own KYC processes to the Lead Manager (and the underwriters), which in return, applies its own KYC process to the Investors.

If the Issuance Facility Operator and the Registrar are two different legal entities, the Issuance Facility Operator and the Registrar need to have a contractual agreement:

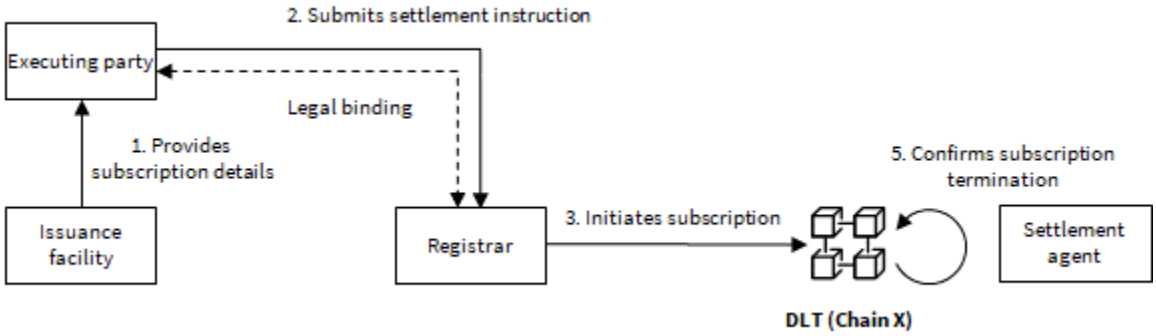
- during the issuance processing stage, the Issuance Facility Operator submits the term sheet to the Registrar for the creation of the instrument (a Smart Contract is created and tokens are allocated to the Issuer).



- the Issuance Facility Operator also manages subscriptions, according to one of the following models:
  1. **direct subscriptions registration model**: the Issuance Facility Operator sends the settlement instructions related to the subscriptions (based on crypto SSI provided by the executing parties) directly to the Registrar. This model requires the executing parties to enter their crypto SSI on the Issuance Facility.



  2. **indirect subscriptions registration model**: the Issuance Facility Operator sends the subscriptions details to the executing parties, which in return instruct the Registrar to initiate their subscriptions on-chain by submitting corresponding settlement instructions. This model requires the Registrar and the executing parties to have a legal binding, which adds complexity to the model.



On receiving the subscription instruction, the Registrar initiates the settlement process.

It is to be noted that the Registrar and the Issuance Facility Operator can be either one single entity or two different entities, depending on the preferred Security Token project setup.

3.2. Trading services map

Services	Description
Order management	• Refers to the collection, routing and management of orders; • Responsibility of the executing parties, generally brokers/dealers.
Order execution	• Refers to all the means and services by which an order is executed. • Responsibility of the OTC Facility Operator.

During the trading phase, services are performed off-chain outside of the DLT, leveraging current services. It is only after the off-chain trading of the Securities Tokens that the ownership transfer will be registered on the DLT.

At first, during the trade phase, instructing parties submit their orders directly to the OTC Facility Operator or to the executing parties. In the latter case, the execution parties can then either route the orders to an OTC Facility for execution by the OTC Facility Operator, or handle the execution themselves over the counter (OTC), typically by telephone or other relevant means chosen by the execution parties.

Instructing parties and/or executing parties are generally granted access to an OTC Facility through a specific application program that requires due diligence (including KYC/AML-CFT diligence) to be performed by the OTC Facility Operator.

Once the orders are executed, trades are generated and notices of execution (including trade details) are sent to the respective counterparties of each trade.

The counterparties of a trade can agree that the trade will settle as recorded at the time of execution (unless both agree to cancel). These are referred to as “locked-in” trades.

In such cases, the OTC Facility Operator generates and submits the settlement instructions related to the “locked-in” trades to the Registrar off-chain, outside of the DLT. This requires that counterparties document their crypto SSI in the OTC Facility.

Otherwise, where executing parties proceed with the execution of the trade between the instructing parties, the executing parties (and their instructing parties) are in charge of sending the settlement instructions to the Registrar, after passing their internal trade processing services.

3.3. Transaction processing services map

Services	Description
Transaction Capture	• Refers to the capture of a trade (or block-trade) internally by each counterparty of the trade, or by a dedicated third-party, for the purpose of trade validation, allocation, matching and confirmation/affirmation; • Allows downstream processing, notably by corporate departments (e.g. finance, risk and accounting departments). • Responsibility of front-office teams. Results in the trade details being sent to the middle and back-office teams.
Trade Allocation	• Refers to the allocation of the Security Tokens across various accounts. • The instructing party communicates the allocation instructions to the executing party.
Transaction Confirmation & Affirmation	• Refers to the confirmation and affirmation of trade details and settlement terms and conditions between the executing party (broker/dealer) and its instructing party; • Occurs on both the buy-side and the sell-side.
Settlement instructions notification	• Refers to the sending of settlement instructions to relevant parties, including the Registrar. • Responsibility of back-office teams.
Position management	• Refers to the process of managing and reporting positions and related transactions; • A position includes the transaction details and may also include valuation information.
Pricing & valuation	• Refers to the determination of securities prices in order to valuate positions and feed downstream systems; • Responsibility of middle-office teams.
Risk management	• Refers to the process of monitoring and controlling the financial exposure created by a collection of financial obligations with respect to fluctuating risk factors (e.g. market price, creditworthiness, etc.)
Repository management	• Refers to the data management systems required to process any trade involving Security Tokens; • Contains reference data to be adapted (e.g. DLT option for “place of settlement”) and distributed across downstream systems.
Accounting management	• Refers to the corporate departments used to record any transaction; • Accounting systems need to be adapted to take into account the upstream processing of transactions involving Security Tokens.
Treasury management	• Refers to the departments in charge of anticipating and executing funds transfers; • Responsibility of the back-office teams.

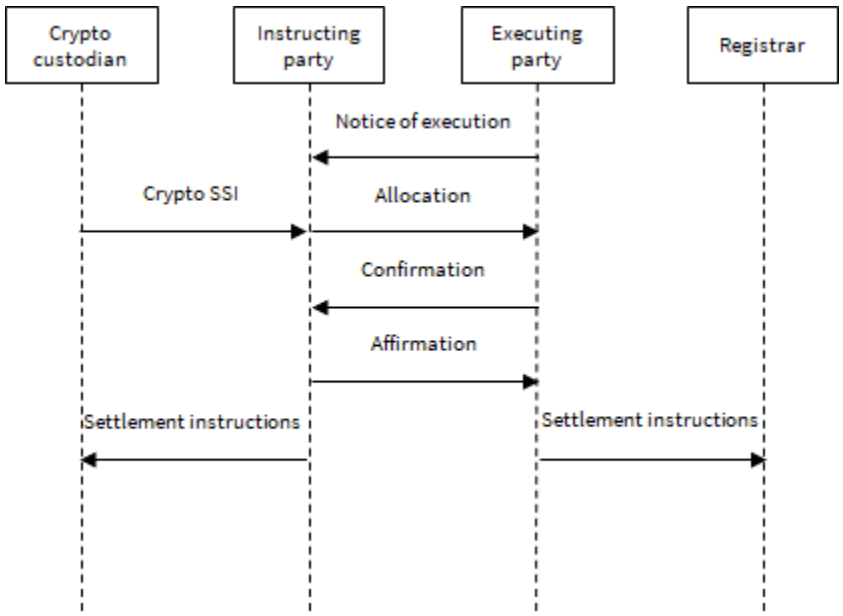
In order to be successfully settled, a transaction (a subscription or a trade) must be accurately recorded and processed in the transaction counterparties’ current systems (post-trade chain).

Front-office, middle-office and back-office teams must validate and operate every stage of the transaction life cycle, to comply with internal duties.

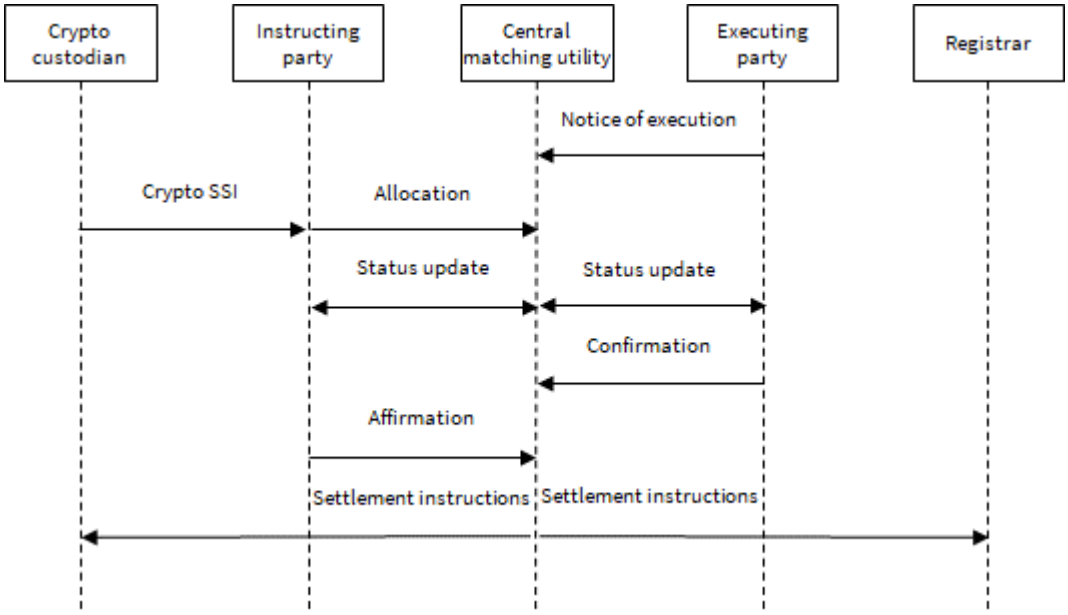
The “matching” process can be defined as the comparison of settlement details by two counterparts to a transaction, following the execution of a trade, to ensure that they meet the terms of the intended transaction.

Executing parties may execute transactions not only on their own account but also on behalf of instructing parties. In this case, the direct market participant may be required to notify its instructing party (or its agent) of the details of the transaction and allow it to positively affirm the details, a process referred to as transaction confirmation or affirmation.

Two party model:



Three party model:



The fundamental challenge for trade processing services is to adapt current systems so they can process transactions involving Security Tokens:

- Reference data may contain information on DLTs and be able to store new objects such as crypto accounts or crypto SSI;
- Downstream services, such as position management or accounting management, should be able to interact with new sources of data (e.g. positions available on the DLT), and define new processing policies (e.g. accounting rules for Digital Assets).
- Treasury management should develop new operational and technical capabilities to handle transfers if the payment leg of a transaction requires Digital Asset transfers instead of traditional cash transfers.
- Etc.

To address these challenges, the CAST Framework comes with a set of open-source technical components, the Oracles, intended to facilitate adaptation of the post-trade chain legacy systems (see chapter 7.4)

3.4. Settlement services map

Activity	Description
Settlement transaction processing	• Refers to the settlement of the delivery leg and the payment leg of a transaction; • Responsibility of the Registrar, the Settlement Agent, and counterparties involved in the payment leg.
Fail & claim Management	• Refers to the management of settlement transaction fails and claims; • Responsibility of both the Registrar and the Settlement Agent.

After having processed the settlement instructions, the Registrar initiates the settlement transaction process.

This phase is strongly impacted by the underlying technologies used in both the delivery leg (Security Tokens) and the payment leg (cash).

While only DLTs can be used for the delivery leg of the Security Token transaction, the payment leg can use either traditional payment systems (e.g. central bank money in Target2) or DLTs or a Target 2 system interoperable with the DLT used as the underlying technology for the cash settlement.

In the event a DLT is used for the cash leg of the transaction, and subject to internal/external regulatory analysis, four types of funds/tokens could potentially be transferred:

- CBDC (Central Bank Digital Currency);
- Asset-referenced tokens, such as stablecoins based on a basket of fiat currencies;
- E-money tokens, such as stablecoins on a 1-to-1 basis with fiat currency;
- Other kinds of Settlement tokens.

There are three types of settlement technological configuration:

Settlement technological configuration	Delivery leg	Payment leg
Cross-chain	Chain X	Chain Y
Mono-chain	Chain X	Chain X
Hybrid	Chain X	Current payment system

3.5. Registry management services map

Services	Description
Settlement instructions processing	• Refers to the collection and matching (if needed) of settlement instructions; • If the settlement instructions provided by the counterparties of a transaction are not pre-matched, the Registrar has the obligation to perform the matching. • Responsibility of the Registrar.
Record-keeping	• Refers to the creation of the Security Tokens' Smart Contract and the recording of settlement transactions in the STR (see chapter 6.4); • Includes services such as instrument registry and token factories; • Includes the recording and maintenance of the Security Token holders' register. • Responsibility of the Registrar.
Audits	• Refers to the audit of the Security Tokens' Smart Contract. • Responsibility of a third party mandated by the Registrar or the Issuer.

3.6. Corporate actions services map

Services	Description
Tax duties processing	• Refers to the collection and processing of tax duties applicable to Security Token holders prior to the processing of any corporate action. • Responsibility of the Fiscal Agent.
Corporate actions processing	• Refers to the processing of corporate actions related to a Security Token. • Responsibility of the Registrar.

3.7. Safekeeping services map

Services	Description
Securities safekeeping	• Refers to the provisioning and the safekeeping of crypto accounts. • Responsibility of the Custodian.
Securities administration	• Refers to the administration of all duties related to the safekeeping of a Security Token on behalf of a client. • May include corporate action monitoring.
Tax duties management	• Refers to tax duties, including fiscal reporting (e.g. IFU capital gains tax return in France) to be managed on behalf of the Investor. • Responsibility of the Custodian.

4. Process workflows

4.1. Issuance workflow

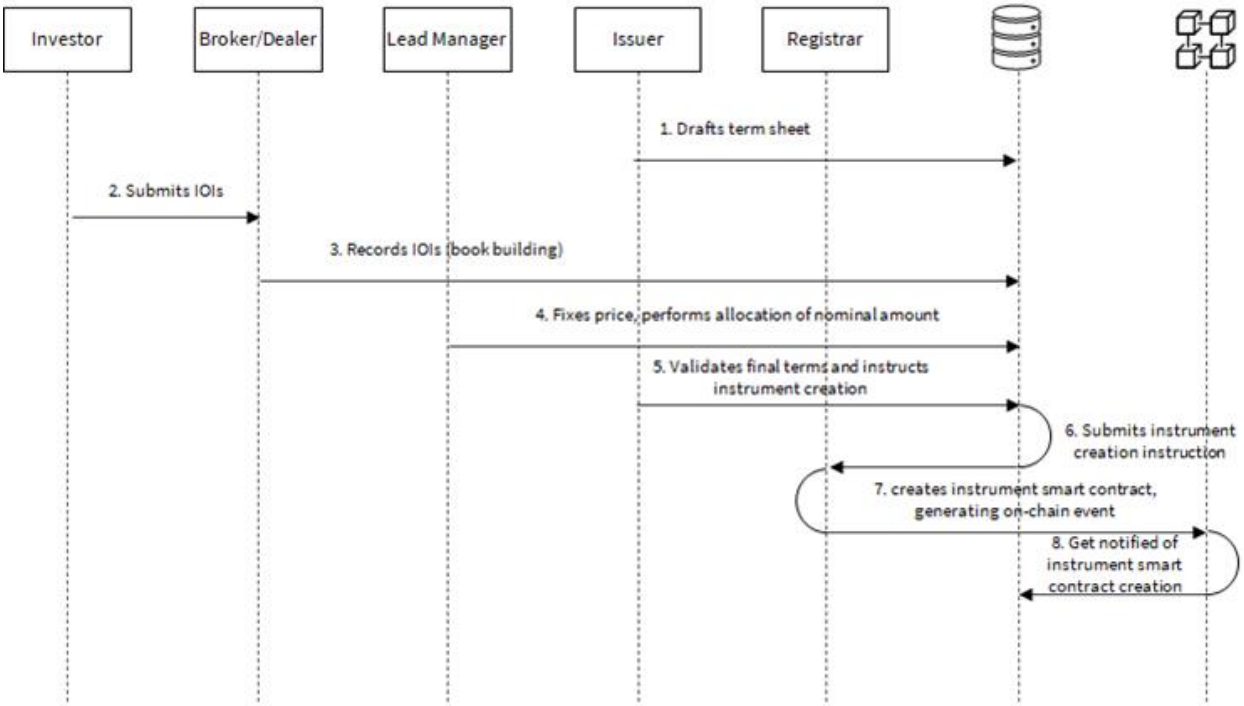
Services map

Issuance		Origination	Structuration	Placing	Issuance processing
Trading		Order routing	Order execution		
Post-trade	**Transaction processing**	Transaction capture	Trade allocation	Trade confirmation & affirmation	Settlement instructions notification
		Position management	Pricing & valuation	Risk management	Referential management
		Accounting management	Treasury management		
	Settlement	Settlement transaction processing	Fail & claim management		
Asset Servicing	**Registry Management**	Settlement instructions processing	Record keeping	Audits	
	Corporate actions	Tax duties processing	Corporate actions processing		
	Safekeeping	Securities safekeeping	Securities administration	Tax duties management	

The issuance workflow depends on the subscriptions registration model (direct or indirect, see chapter 7.2.1) agreed by the parties involved.

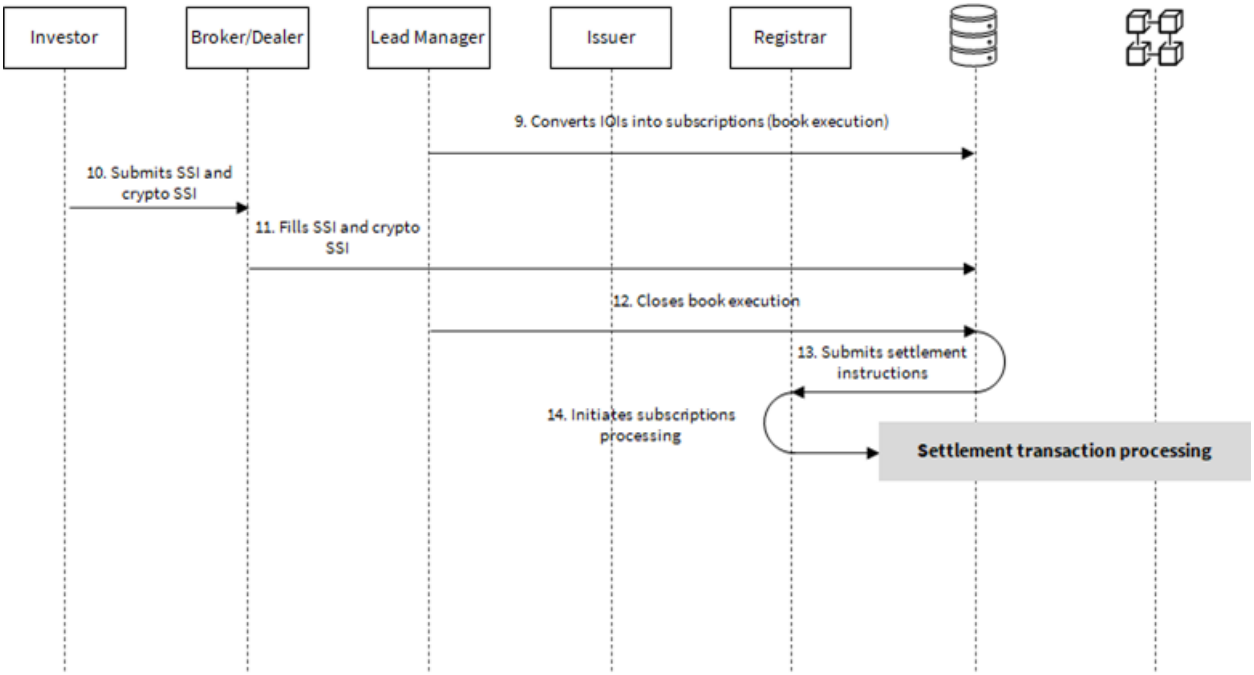
For reasons of simplification, the diagrams below describe the direct subscriptions registration model.

Phase 1: Instrument creation



1. The Issuer drafts the term sheet in the Issuance Facility;
2. The Investors send their IOIs to their respective dealers;
3. The dealers record the IOIs in the Issuance Facility. The issuance book contains all IOIs submitted;
4. The Lead Manager carries out the issuance by fixing the price and allocating the nominal amount to booked IOIs;
5. The Issuer validates final terms and instructs the Security Token instrument creation;
6. The Issuance Facility submits the instrument creation instruction to the Registrar;
7. The Registrar creates the instrument Smart Contract, generating an on-chain event;
8. The event is captured by the Issuance Facility (through its Oracle) to notify the Issuer and the Lead Manager of such event.

Phase 2: Subscriptions management



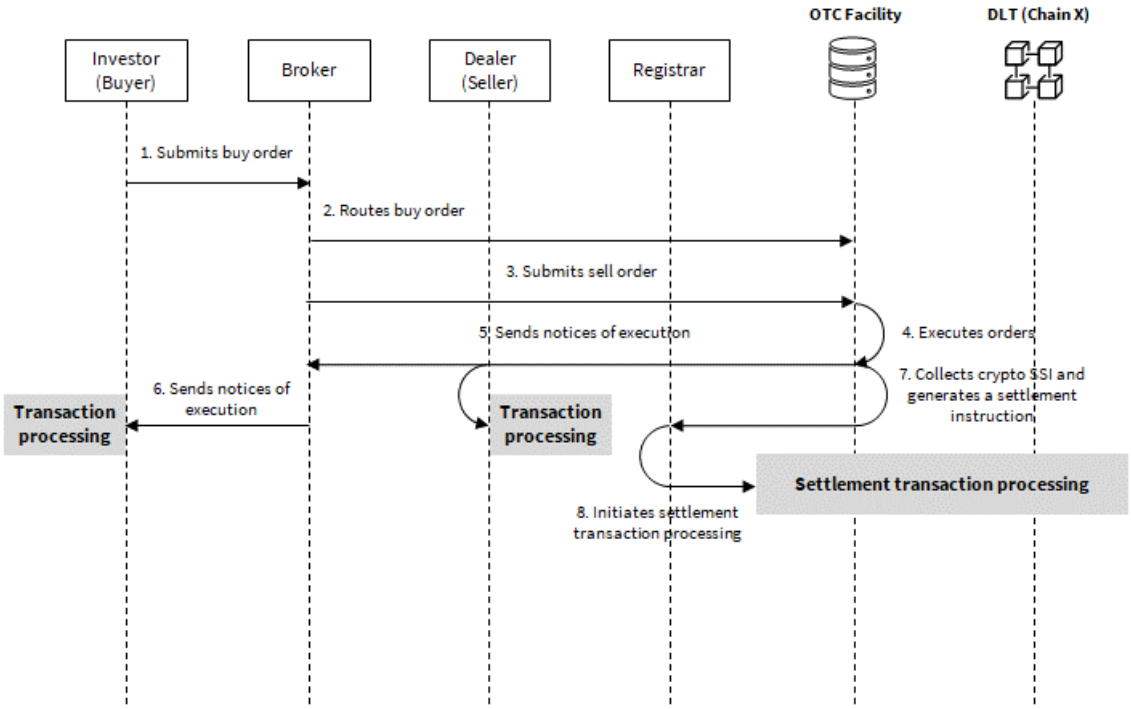
9. Once notified of the instrument creation, the Lead Manager starts the conversion of allocated IOIs into subscriptions (book execution);
10. The Investors provide their crypto SSI to their respective dealers;
11. The dealers enter crypto SSI into the Issuance Facility;
12. The Lead Manager closes the issuance book, generating final subscriptions;
13. Based on the crypto SSI provided, the Issuance Facility generates the settlement instructions and submits them to the Registrar, and submits the settlement instructions to the Registrar;
14. The Registrar processes the settlement instructions (validity checks, etc.) and initiates the settlement transaction processing.

4.2. Trading workflow

Services map

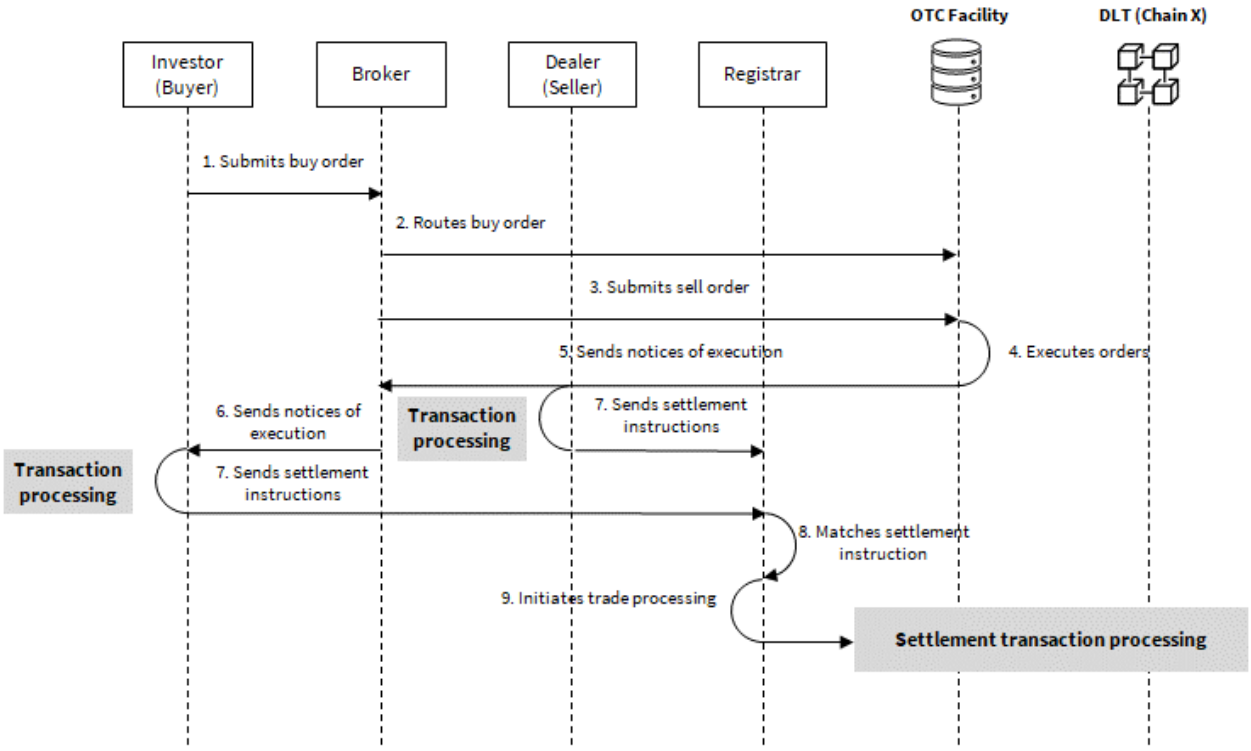
Issuance		Origination	Structuration	Placing	Issuance processing
Trading		Order routing	Order execution		
Post-trade	**Transaction processing**	Transaction capture	Trade allocation	Trade confirmation & affirmation	Settlement instructions notification
		Position management	Pricing & valuation	Risk management	Referential management
		Accounting management	Treasury management		
	Settlement	Settlement transaction processing	Fail & claim management		
Asset Servicing	**Registry Management**	Settlement instructions processing	Record keeping	Audits	
	Corporate actions	Tax duties processing	Corporate actions processing		
	Safekeeping	Securities safekeeping	Securities administration	Tax duties management	

Pre-matched trades



1. The buyer submits a buy order to the broker;
2. The broker routes the order in the OTC Facility to the OTC Facility Operator;
3. The OTC Facility Operator submits the order to potential counterparties;
4. One or several dealers submit(s) a price in the OTC Facility to the OTC Facility Operator; and after obtaining approval of the price by the broker, the OTC Facility Operator executes the order and generates a trade;
5. The OTC Facility Operator sends a notice of execution to the trade counterparties;
6. The broker sends the notice of execution to the buyer;
7. Based on crypto SSI provided by the parties involved, the OTC Facility Operator generates a settlement instruction and sends it to the Registrar;
8. Once it receives the settlement instruction, the Registrar initiates the settlement transaction processing.

Other trades



1. The buyer submits a buy order to the broker;
2. The broker routes the order in the OTC Facility to the OTC Facility Operator;
3. The OTC Facility Operator submits the order to potential counterparties;
4. One or several dealers submit(s) a price in the OTC Facility to the OTC Facility Operator; and after obtaining approval of the price by the broker, the OTC Facility Operator executes the order and generates a trade;
5. The OTC Facility Operator sends a notice of execution to the trade counterparties;
6. The broker sends the notice of execution to the buyer;
7. The settlement instructions are sent to the Registrar;
8. The Registrar matches the settlement instructions;
9. Once it matches the settlement instructions, the Registrar initiates the settlement transaction processing.

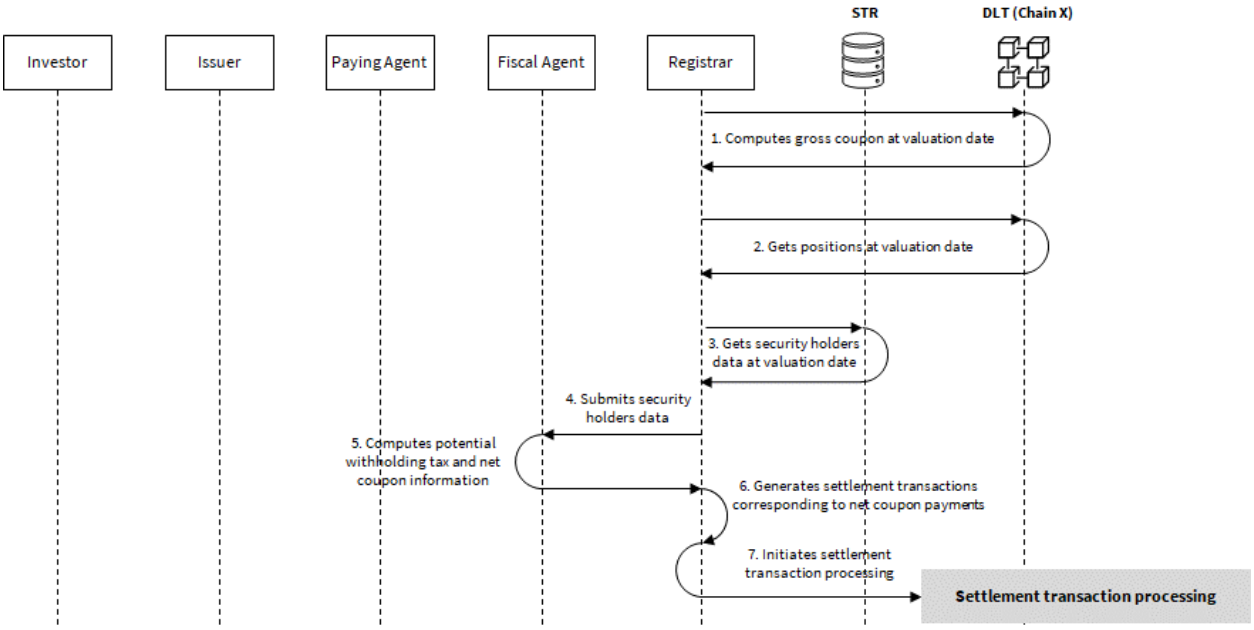
In this model, the settlement instructions are generated by the trade counterparties (after transaction processing within their current systems) and sent to the Registrar.

The Registrar matches the settlement instructions before initiating settlement transaction processing.

4.3. Coupon payment workflow

Services map

Issuance		Origination	Structuration	Placing	Issuance processing
Trading		Order routing	Order execution		
Post-trade	**Transaction processing**	Transaction capture	Trade allocation	Trade confirmation & affirmation	Settlement instructions notification
		Position management	Pricing & valuation	Risk management	Referential management
		Accounting management	Treasury management		
	Settlement	Settlement transaction processing	Fail & claim management		
Asset Servicing	**Registry Management**	Settlement instructions processing	Record keeping	Audits	
	Corporate actions	Tax duties processing	Corporate actions processing		
	Safekeeping	Securities safekeeping	Securities administration	Tax duties management	



1. The Registrar (or the Calculation Agent) computes gross coupon at the valuation date (by querying the Security Token's Smart Contract);

2. The Registrar gets the positions at valuation date (from the Security Token's Smart Contract);
3. The Registrar gets the Security Token holders at valuation date from the STR (through its Oracle);
4. The Registrar sends the gross coupon and the Security Token holders' data to the Fiscal Agent;
5. The Fiscal Agent computes potential withholding tax based on data sent by the Registrar. If any withholding tax is payable, the Fiscal Agent sends the net coupon information to the Registrar;
6. The Registrar generates the settlement transactions corresponding to the coupon payment:
    a. A settlement transaction between the Issuer and the Paying Agent for the gross coupon payment;
    b. Settlement transactions between the Paying Agent and each Security Token holder for the net coupon and tax payment.
7. The Registrar initiates the settlement transaction processing.

4.4. Settlement transaction processing

Services map

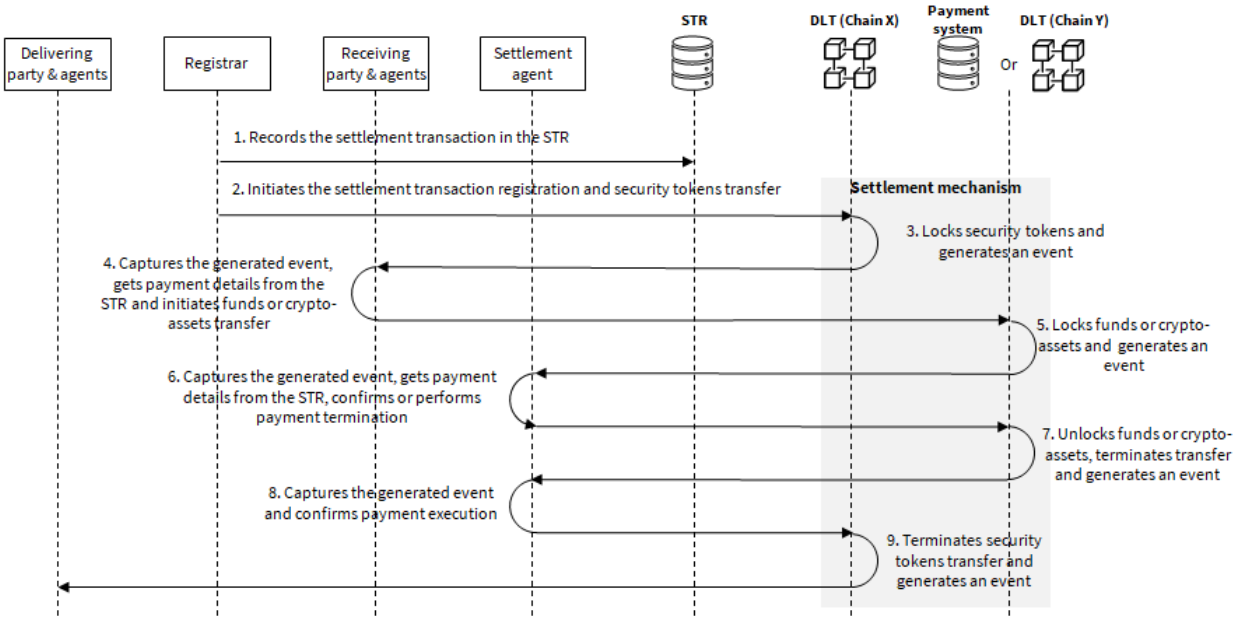
Issuance		Origination	Structuration	Placing	Issuance processing
Trading		Order routing	Order execution		
Post-trade	**Transaction processing**	Transaction capture	Trade allocation	Trade confirmation & affirmation	Settlement instructions notification
		Position management	Pricing & valuation	Risk management	Referential management
		Accounting management	Treasury management		
	Settlement	Settlement transaction processing	Fail & claim management		
Asset Servicing	**Registry Management**	Settlement instructions processing	Record keeping	Audits	
	Corporate actions	Tax duties processing	Corporate actions processing		
	Safekeeping	Securities safekeeping	Securities administration	Tax duties management	

The settlement transaction process is similar for all types of transaction. Depending on the technical configuration of the settlement (cross-chain, mono-chain or hybrid, see chapter 2.3.4), the mechanisms involved can differ:

- Use of Hash Time Locked Contracts (HTLC) for cross-chain or mono-chain configurations;
- Use of DvP Smart Contracts for mono-chain configurations;
- Use of traditional payment systems for hybrid configurations.

For reasons of simplification, the diagrams below describe a DvP (Delivery-versus-Payment) transaction (e.g. trade or subscription) with a settlement mechanism based on conditional transfers (once initiated, transfers must be validated to be executed).

For a PFoD (Payment Free of Delivery) transaction (e.g. coupon payment), the diagram remains the same, apart from the tasks related to the transfer of Security Tokens.



1. After receiving and matching the settlement instructions, the Registrar records the corresponding settlement transaction in the Settlement Transaction Repository (STR, see chapter 8.3);
2. The Registrar initiates the on-chain registration of the settlement transaction and the Security Tokens transfer;
3. The settlement transaction is registered on-chain (see settlement management chapter 8.2), the Security Tokens are locked or reserved for the receiving party (they still belong to the delivering party), and an event is generated;
4. The receiving party (buyer or subscriber) captures the generated event (through its Oracle, see chapter 8.4), obtains the payment details (by querying the STR through its Oracle), and initiates the fund or Digital Asset transfer;
5. The funds or Digital Assets are locked or reserved for the delivering party (they still belong to the receiving party or are put in an escrow account managed by the Settlement Agent), and an event is generated;
6. The Settlement Agent captures the generated event (through its Oracle) and obtains payment details (by querying the STR through its Oracle). On confirmation that the payment is related to an existing transaction and the amount transferred is correct, the Settlement Agent confirms (or performs) payment termination;
7. On payment termination confirmation, the funds or Digital Assets are unlocked, transferred to the delivering party, and an event is generated;
8. The Settlement Agent captures the generated event (through its Oracle) and confirms payment execution/termination on the delivery chain;
9. On payment execution/termination confirmation, the Security Tokens are unlocked, transferred to the receiving party, and an event is generated.

3 | CAST LEGAL & REGULATORY CONSTRAINTS ASSESSMENT

The **CAST Framework** provides market participants with an assessment of a set of **contractual agreements** binding all parties involved in Security Token issuance (the Issuer, its Agents, Investors, etc.) to ensure processes are designed in line with regulatory compliance requirements related to the issuance, custody and trading of Security Tokens for all stakeholders involved. These contractual agreements detail the roles undertaken by market participants interfacing DLT with current systems. These documents should be written in such way as to provide stakeholders with legal certainty with regards to the issuance, custody and trading of Security Tokens. Some jurisdictions like France and Switzerland have already adopted a clear regulatory framework to allow such unlisted Security Token transactions. Nevertheless, regulated entities and/or Issuers should make their own assessments and obtain internal and/or external legal advice to provide legal certainty for their envisioned Security Token projects. **The CAST Framework documentation has no contractual value, and does not, and is not intended to, constitute and/or provide legal or professional advice, or certify any compliance with applicable law and/or regulations requirements.**

Nevertheless, the CAST Framework directly addresses the very specific legal, regulatory and compliance issues that market participants may encounter when dealing with native Security Tokens. It also provides the required assurance required to deal with DLT and native Security Tokens in a broader sense: it addresses challenges related to the potential lack of experience of stakeholders willing to get onboard by providing a solid legal framework for the different stakeholders, setting out mutual obligations and clear responsibilities. Perceived barriers to entry, such as difficulties in creating and maintaining strong Business Continuity Plans, are anticipated and addressed by the legal and regulatory component of the CAST Framework. This framework also spans DLT with capital market institutional standards on very specific issues, such as a DLT-based identity framework, intellectual property, or cybersecurity concerns.

The CAST Framework's Legal & Regulatory Constraints Assessment is designed to consider existing regulations proactively, although it is committed to considering global discussions on Digital Assets since this topic has emerged on the global agenda. At the global level, jurisdictions either apply existing securities regulations to the various types of Digital Assets (such as in the United States of America) or they try to cover parts of the Digital Asset market by bringing into scope new types of Digital Assets (Utility Tokens and crypto-currencies) and new types of service providers (Crypto-Asset Service Providers) alongside an adaptation of securities regulations to the specific features of Security Tokens (for example in France and in Switzerland currently, and across the EU in the future with the adoption the European "Pilot regime regulation" proposal for DLT market infrastructures). The CAST Framework's Legal & Regulatory Constraints Assessment encompasses existing legal relationships between the various stakeholders and new regulatory issues associated with the tokenization of financial instruments.

For the sake of clarity, in this White Paper, **on-chain** refers to services or activities based on DLT features. In contrast, **off-chain** refers to services or activities based on current technologies only.

1. Roles and legal bindings

The following table summarizes the main agreements that could be established for a Security Token issuance:

Contract	Parties involved	Description
Agency Agreement	Issuer Registrar Settlement Agent Fiscal Agent	Multilateral agreement between the Issuer and its Agents (i.e. the Registrar, the Settlement Agent, the Fiscal Agent) which provides a contractual framework for the various services realized by the Issuer's Agents related to the issuance of Security Tokens and the processing of corporate actions related to the Security Tokens
Mandate	Issuer Lead Manager Structuring Manager (designated)	Mandate under which the Lead Manager is mandated by the Digital Asset Issuer to facilitate the purchase and sale of the Digital Assets by Investors during the issuance of the Digital Assets, and under which the Structuring Manager is designated
Bilateral agreement	Lead Manager Investor	Bilateral agreement between a Lead Manager and each of the relevant Investors related to the purchase and sale of the Digital Assets by Investors during the issuance of the Digital Assets
Service agreement	Issuance Facility Operator Lead Manager Registrar	Multilateral agreement between the Issuance Facility Operator, the Lead Manager and the Registrar related to the use of the Issuance Facility to facilitate the subscription of the Security Tokens by Investors during their issuance
Service agreement	OTC Facility Operator Lead Manager Investors	Bilateral agreement between the OTC Facility Operator and each Lead Manager and/or each Investor related to over-the-counter transfers of Security Tokens on the secondary market
Service agreement	Smart Contract auditor Registrar	Bilateral agreement between the auditor of the Smart Contracts and the Registrar that developed the Smart Contracts
Custodial agreement	Custodian Investor	Bilateral agreement between the Custodian and an Investor regarding Custody Services related to the Security Tokens provided by the Custodian on behalf of its client (i.e. the Investor)

2. Understanding KYC principles

The Issuer must comply with KYC/AML obligations if applicable. This is notably required when the Issuer is a regulated entity such as a credit institution or an investment firm.

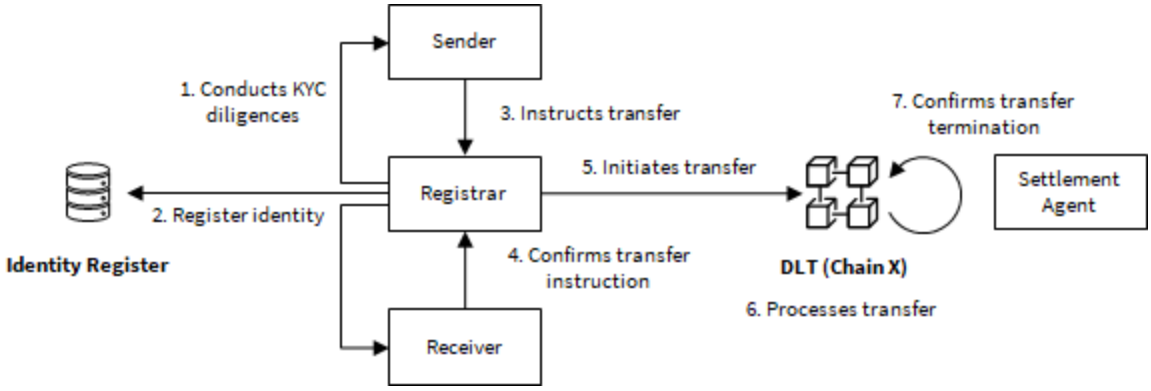
If relevant, through the Agency Agreement, the Issuer can delegate responsibility for conducting KYC diligence on its behalf and for the keeping of records of the Security Token holders' identity to the Registrar.

The Registrar is in charge of defining a KYC policy including at least:

- Identification procedures;
- Risk assessment and management (due diligence);
- On-going monitoring and record-keeping.

The Registrar can implement different, more or less disruptive, KYC models by leveraging blockchain capabilities or by replicating existing practices in the capital markets.

In most cases the Registrar will use existing KYC services to conduct diligence and feed an off-chain identity register. It can operate or outsource all or of the related services according to the entity involved. KYC diligence must be conducted by the Registrar for each party involved in a transaction which has developed a business relationship with such Registrar.



In some cases, and if relevant, depending on the applicable legal and regulatory framework, the Registrar can delegate the realization of the KYC diligence process to a third party while being still responsible for the KYC diligence process realized.

The Registrar can also provide and operate on-chain solutions (such as identity Smart Contracts) to register the Security Token holders' identity through a whitelisting process.

On the one hand, such DLT on-chain mechanisms provide the benefit of on-chain dynamic whitelisting, allowing whitelisted parties to initiate a transaction without instructing the Registrar.

On the other hand, whitelisted parties need to have good DLT understanding and technical capabilities to manage or interact with their identity Smart Contracts. Even in this case, identity Smart Contracts must be instantiated for every DLT where a transaction occurs, bringing complexity and potential discrepancies.

3. Integrating DLT into financial regulation: the European example

Existing financial regulations were created at a time where DLT was not in the spectrum of possibilities and are therefore often inadequate with regard to the emergence of Digital Assets and DLT. From a European perspective, the MiFID 2 regulation is the central piece of EU securities legislation, providing a detailed list of the different forms of 'financial instruments'[16] and of 'investment services and activities' and 'ancillary services'[17] under EU law. A broader set of rules mentioned above (namely the Prospectus Regulation, MAR, EMIR, SFD, CSDR) also applies to financial instruments and to firms that provide investment services and activities in relation to investment services.

The proposal for a European pilot regime regulation[18], as published by the EU Commission in September 2020, provides a transitional regulatory regime to allow for the possibility of issuing and trading in listed securities on a DLT. The EU pilot regime regulation specifies that only a "DLT market infrastructure" (i.e. a market infrastructure based on Distributed Ledger Technology) can benefit from targeted exemptions provided for in the EU pilot regime. According to the first published draft, only two types of actors can be qualified as "DLT market infrastructure" (see Art2(2) of the Draft Regulation): DLT Multilateral Trading Facilities (DLT MTF) and DLT securities settlement systems (DLT SSS)[19].

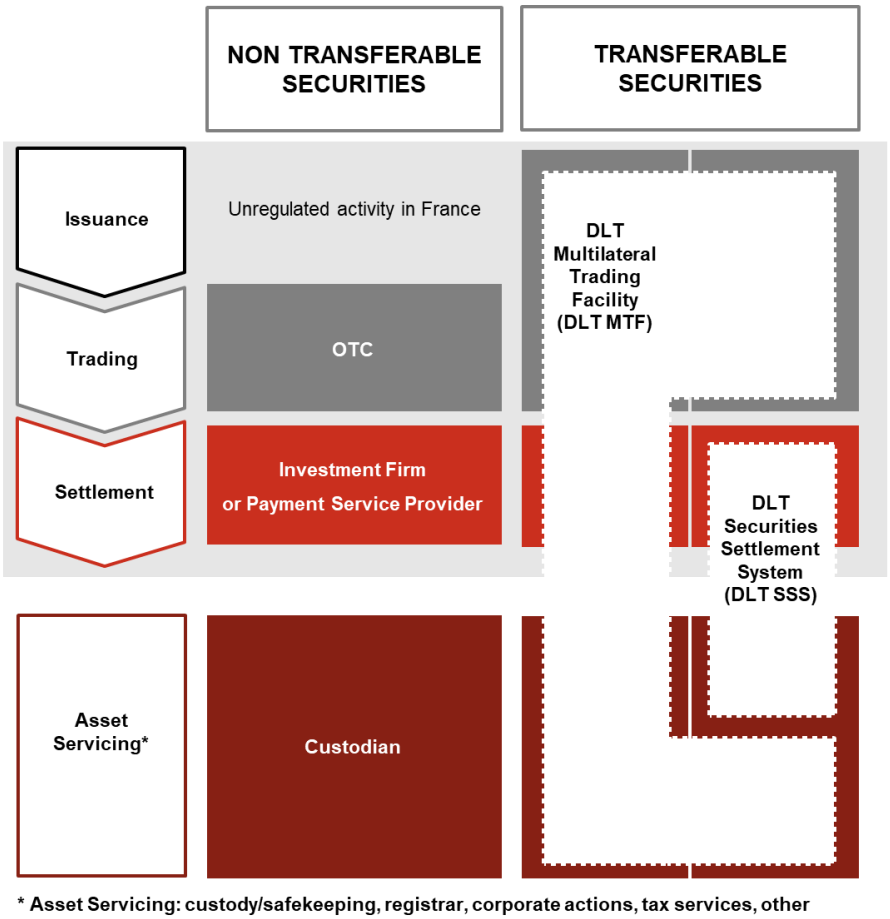
In order to operate a Multilateral Trading Facility using DLT technology (DLT MTF), it is necessary to be authorized beforehand as an Operator of a Multilateral Trading Facility (MTF) within the meaning of MiFID 2. Similarly, to operate a Securities Settlement System using DLT technology (DLT SSS), it is necessary to be authorized beforehand as a Central Securities Depository as defined under the CSDR (see Art. 2(3) and 2(4) of the Draft Regulation). Only DLT transferable securities may be admitted to trading on a DLT MTF and recorded on a distributed ledger by a CSD operating a DLT securities settlement system (see Art. 2(3) and 2(4) of the Draft Regulation) or by a DLT MTF.

The current European proposal on a pilot regime for DLT market infrastructures provides a secure regulatory framework for the listing of Security Tokens within the EU to enhance their liquidity on the secondary market and clearly takes into account DLT near real-time settlement capabilities and proposes allowing DLT MTF an extended activity scope, to include activities "normally performed by a CSD"[20]. If this proposal is adopted, this would imply an extended role for regulated platforms based on Distributed Ledger

[16] i.e. 'transferable securities', 'units of collective investment undertakings', etc.
[17] RTO, 'Execution of orders on behalf of clients', 'Underwriting of financial instruments', Operation of an MTF or of an OTF, 'Safekeeping and administration of financial instruments for the account of clients', etc.
[18] Proposal for a regulation of the European Parliament and of the Council on a pilot regime for market infrastructures based on distributed ledger technology.
[19] These last two concepts do not exist to date in European law and have been introduced in the draft European regulation on the pilot regime.
[20] See: Proposal for a Regulation of the European Parliament and of the Council on a pilot regime for market infrastructures based on distributed ledger technology. Quote: *"The use of distributed ledger technology, with all transactions recorded in a decentralized ledger, can expedite and condense trading and settlement to nearly real-time and could enable the merger of trading and post-trading activities. However, the current rules envisage the performance of trading and settlement activities by separate market infrastructures. Regulation (EU) No 909/2014 of the European Parliament and of the Council (the Central Securities Depositories Regulation) requires that financial instruments admitted to trading on a trading venue within the meaning of Directive 2014/65/EU (Market in Financial Instruments Directive, MiFID II) be recorded with a central securities depositary ('CSD'), while a distributed ledger could be potentially used as a decentralized version of such a depository. Therefore, it would be justified to allow a DLT MTF to perform some activities normally performed by a CSD. Therefore, when granted the relevant exemption(s), a DLT MTF should be allowed to ensure the initial recording of DLT transferable securities, the settlement of transactions in DLT transferable securities and the safekeeping of DLT transferable securities."*

Technologies (DLT MTFs), which could provide services throughout the Security Tokens' life cycle, from issuance to safekeeping.

For the purposes of the EU pilot regime as proposed, the following features apply:



When a financial instrument is admitted to trading on an MTF, it must be recorded with an authorized Central Securities Depository in accordance with the Central Securities Depository Regulation, while the registration of a security and the settlement of related transactions could, in practice, take place on a distributed ledger. Therefore, it would be justified to allow a DLT MTF to perform some activities normally performed by a CSD. Accordingly, when granted the relevant exemption(s), a DLT MTF may be permitted to ensure (i) the recording, (ii) the settlement and (iii) the safekeeping of DLT transferable securities (see Art. 2(3)).

4 | CAST TECHNICAL FRAMEWORK

The CAST Framework's technical component provides the technical principles that shall be integrated in any solution to comply with the legal & regulatory and the operational framework.

1. Instrument registry pre-requisites

The instrument registry is a Smart Contract that has permanent existence and acts as a source of trust for all the Instruments created by a Registrar. Its Smart Contract address is used as a single reference to prevent complicated configurations.

It serves as a single configuration point to allow the stakeholders to discover the existing Smart Contracts it provides:

- The Smart Contracts can be found by ISIN Code;
- The Smart Contract addresses can be changed to a new version in case of a bug or hacking;
- The Smart Contracts can be recorded in the instrument registry;
- Stakeholders can be informed of new official Smart Contracts by subscribing to the registry events.

2. Security Token pre-requisites

The Registrar provides the Issuer with the relevant Security Token Smart Contract for a specific DLT, based on the outcomes of the structuring phase: type of instrument, corporate actions to be implemented, and privacy considerations.

The Registrar can leverage Smart Contract templates/libraries available in its token factories – one for each DLT supported.

Whatever the DLT chosen, the Security Tokens' Smart Contract must include at least the following four (4) modules in its code:

Module	Description
Instrument Management	• Stores the financial details of the envisioned financial instrument (e.g. amount, quantity, ISIN code, etc.) as indicated in a dedicated documentation (term sheet and/or final terms, etc.); • Sets out all the methods available to obtain or calculate relevant information (e.g. coupon calculation, list of schedules or installments, etc.).
Operator Management	• Stores the list of operators authorized to perform operations; • Sets out all the methods to be used to grant rights to an operator or revoke their rights.
Balances Management	• Stores security holders' addresses and corresponding balances; • Sets out all the methods to be used to obtain relevant information (e.g. balances).
Settlement Management	• Stores the settlement states of all transactions processed by the operators; • Exposes all the methods to be used to change a transaction's settlement state.

The **instrument management module** is intended to be open to all stakeholders involved in the Security Token issuance and allows them to obtain all the information about the instrument. Depending on the privacy policy defined by the Issuer, all or part of the information is available.

The **operator management module** is only available for the Issuer of the Security Tokens. It is based on a whitelisting mechanism allowing the Issuer to declare operators and grant them specific rights according to pre-defined profiles, such as the Registrar and the Settlement Agent profiles. These rights allow the operators to use the methods set out in the instrument and settlement management modules.

The Issuer is the only one to use the operator management module. It allows the Issuer to appoint or revoke operators.

It consists in a whitelist of authorized parties to whom are attributed specific profiles, such as the Registrar and the Settlement Agent. Each profile specifies the methods available to each operator on the separate modules (and their related methods) of the Security Token.

For instance, a Registrar can initiate a subscription or a trade, but only the Settlement Agent can confirm the termination of the payment leg to trigger the settlement of the delivery leg.

Below the list of available methods that can be found per profile for a specific bond token (defined during the structuration phase with the Issuer):

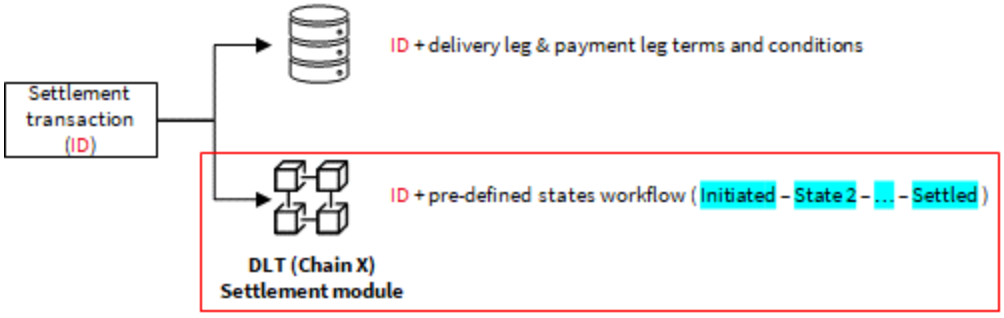
Module	Method	Registrar	Settlement Agent
Instrument Management	createInstrument	✔	✘
	computeNextInstallment	✔	✘
	getPaymentAmountFor	✔	✘
	getPaymentStatusFor	✔	✘
	isAllPaidFor	✔	✔
	initialSupply	✔	✘
	currentSupply	✔	✘
	Name	✔	✘
	Symbol	✔	✘
	isinCode	✔	✘
	denomination	✔	✘
	Divisor	✔	✘
	startDate	✔	✘
	maturityDate	✔	✘
	Instrument Management	✔	✘
	firstCouponDate	✔	✘
	couponFrequencyInMonths	✔	✘
	interestRateInBips	✔	✘
	isSoftBullet	✔	✘
	softBulletPeriodInMonths	✔	✘
Operator Management	authorizeOperator	✘	✘
	isOperatorWithRoleAuthorized	✔	✔
	revokeOperatorAuthorization	✘	✘
Balances Management	getBalance	✔	✔
	getFullBalances	✔	✘
Settlement Management	initiateSubscription	✔	✘
	initiateTrade	✔	✘
	initiateTransfer	✔	✘
	provideTaxPayment	✔	✘
	initiateRedemption	✔	✘
	initiateCall	✔	✘

	initiatePut	✔	✘
	confirmPaymentReceived	✘	✔
	confirmPaymentTransferred	✘	✔
	cancelSettlement	✔	✘

The **balances management module** is intended to be open to all stakeholders and allows them to obtain all information about the positions and balances. Depending on the privacy policy defined by the Issuer, all or part of the information is available.

The **settlement management module** is only used by the operators. It stores the settlement states related to any settlement transaction (stored in the STR, see chapter 6.2).

For each settlement transaction the Registrar records a dedicated settlement state workflow in this module. This settlement workflow depends on the settlement transaction type (e.g. trade, subscription, or coupon payment) and represents the different states of the settlement. These states will be updated by the operators, according to their profile.



Therefore, for each settlement transaction, this module shows the real-time state of the settlement process. All the terms and conditions related to the settlement transaction are stored separately in the STR.

When settlement workflow states change, events are generated on-chain and can be captured by DLT listeners (see Oracles chapter 6.4)

The table below provides a summary of each stakeholder's access rights to the Security Token modules:

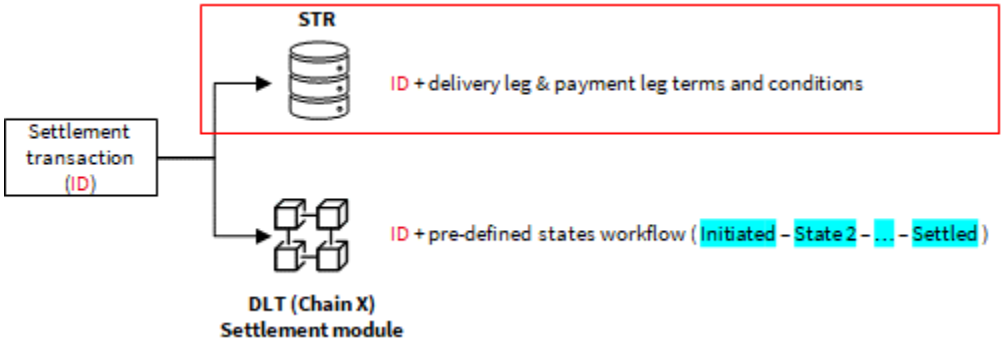
Module	Issuer	Operators	Security holders
Instrument Management	✔	✔	✔
Operator Management	✔	✘	✘
Balances Management	✔	✔	✔
Settlement Management	✘	✔	✘

3. Settlement Transaction Repository (STR) pre-requisites

3.1. General principles

The Settlement Transaction Repository (STR) is an off-chain component provided and managed by the Registrar and constitutes a key part of the Business Continuity Plan of the Issuer and/or its Registrar, as described in Chapter 2. Under the CAST Framework, a continuity plan must be put in place and maintained to prevent any potential technological disruption and to protect the data registered on a DLT infrastructure (e.g. Ethereum, Tezos, etc.), for regulatory and compliance reasons. In order to avoid a "single point of failure" risk and to enhance investor protection, the CAST Framework provides that the Registrar, acting on behalf of the Issuer, has the mandate to keep an external off-chain register of Security Token holders and to be able to switch from one technical infrastructure to another if needed to ensure the business continuity of operations. For instance, it can switch from one DLT to another or from a DLT to current infrastructures, should that be necessary. From the instructing party's perspective (Investor, Issuer), the operational friction related to such a technological switch should be minimized by the recording of all information related to the transaction off-chain by the Registrar in an external technological infrastructure, the Settlement Transaction Repository (STR), which would not be affected by any DLT-related incident, as it is separate from any DLT.

The Registrar stores all the settlement transactions to be processed in the STR, whatever the result of the settlement processing (which is stored on-chain in the Security Token settlement module).



The settlement transactions stored must contain the terms and conditions of the delivery leg (if any) and the payment leg (if any), including notably the identity of the parties involved:

Type of information	Main data stored
Instrument details	Security Token blockchain address, ISIN code, etc.
Transaction details	transaction ID (from OTC Facility), place (OTC Facility), date
	Price
Settlement details	settlement transaction ID
	type (DvP, PFoD, etc.), settlement date
	Registrar LEI, Settlement Agent LEI

Delivery leg details	DLT
	Quantity
	sender LEI, receiver LEI
	sender crypto account, receiver crypto account
Payment leg details	DLT or payment system
	amount, fees, currency or Digital Asset
	sender LEI, receiver LEI
	sender cash or crypto account, receiver cash or crypto account

As a consequence, when matching the content of the STR with on-chain settlement workflow information, the Registrar can:

- Reconstitute the positions and balances of Security Token holders for a specific date;
- Reconstitute the identity of Security Token holders or their agents for any specific date;
- Provide the history of all Security Token holders or their agents since the issuance.

Depending on the regulations applicable to the Security Token, the record of identity of the Security Token holders' agents might not be enough (e.g. administered registered security form not allowed, see chapter 3.2) and it may be necessary to store only the identity of the Security Token holders (e.g. only pure registered security form allowed, see chapter 3.2).

3.2. Business continuity plan

The Issuer is entitled to expect a business continuity plan (mentioned within the Agency Agreement) from the Registrar in case of a major technical issue on the Security Tokens' underlying DLT.

The Registrar must operate on its own at least one full node (redundancy mechanisms would be better) of the Security Tokens' underlying DLT, in order to keep an external off-chain register of the Security Token holders and to be able to reconstitute the register of the Security Tokens (positions, balances and holders' identity) off-chain so it can switch from one technical infrastructure to another if needed to guarantee the business continuity of operations.

The Registrar can then provide alternative solutions to the Issuer:

- Early redemption;
- Deployment of the Security Tokens on a different DLT (for which the Registrar has a token factory);
- Registration of the security in the traditional market infrastructure.

3.3. Privacy management

DLTs are evolving fast in terms of scalability and privacy features, however, on-chain privacy mechanisms (mainly based on zero-knowledge-proof) remain immature in terms of adoption and integration by crypto servicers.

Moreover, existing on-chain privacy mechanisms use more gas and require stronger technical capabilities from the parties involved in a transaction.

As a consequence, as of today, the STR provides a robust alternative to on-chain privacy mechanisms to ensure privacy for settlement transaction terms and conditions.

Once authenticated by the STR (see chapter 6.2.4), stakeholders should only have access to the settlement transactions they are authorized to consult:

Stakeholder	Filter
Issuer	All settlement transactions related to its Security Token
Registrar	All settlement transactions related to a Security Token for which it is registered as Registrar
Settlement Agent	All settlement transactions related to a Security Token for which it is registered as Settlement Agent
Holders	All settlement transactions for which it is registered as sender or receiver, on the delivery leg or the payment leg

Additional filters can be implemented to limit access to specific terms and conditions of a settlement transaction.

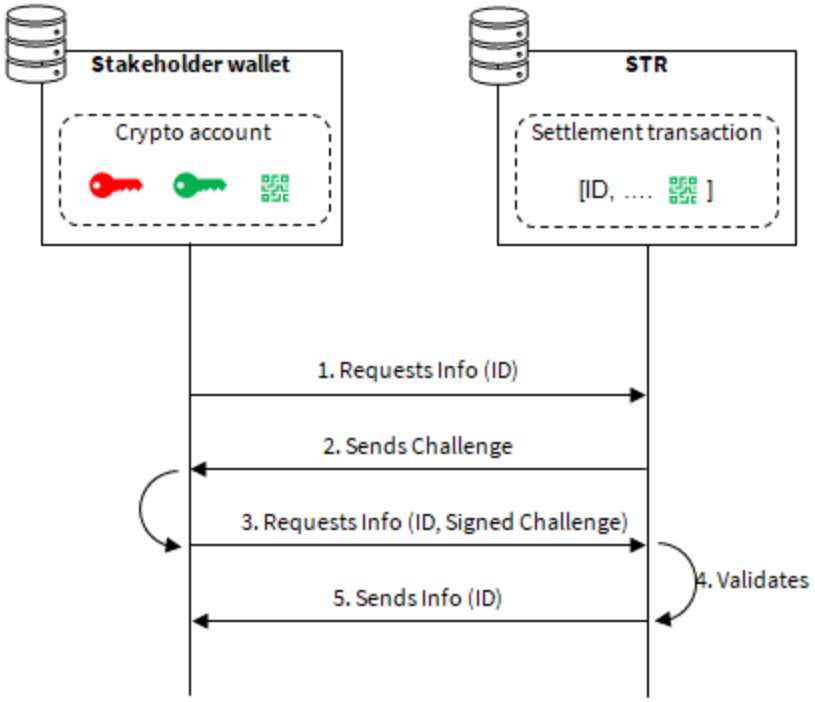
3.4. Authentication

A STR legacy authentication mechanism would oblige stakeholders to ask the Registrar for specific credentials, resulting in a complex and unscalable setup.

Moreover, if the Registrar is revoked, the new Registrar must be able to easily obtain or duplicate the STR, be able to operate it and allow stakeholders to access it without obliging them to request new credentials.

For this reason, access to the STR must require an authentication mechanism that is agnostic to the Registrar, leveraging the use of private keys related to the crypto accounts registered in the settlement transactions (see chapter 6.2.4).

That way, only the holders, the Issuer, and the operators can access the content of the STR, and they do not need specific credentials from the Registrar to access the STR: to simplify the process they authenticate by signing with the private keys of their crypto accounts.



Each Settlement Transaction within the STR stores the crypto accounts addresses of involved parties (e.g. Sender, Receiver, Registrar, etc.).

When requesting access to the STR content for a specific settlement transaction ID (1), the stakeholder is sent a challenge by the STR (2) to prove it really owns the private key corresponding to one of the addresses stored in the settlement transaction.

The stakeholder signs the challenge with its private key and requests information with the signed challenge (3).

The STR verifies that the signed challenge is correct (4) and then sends the requested information to the stakeholder (5).

4. The Oracles

Most capital markets participants are still learning about DLTs and Digital Assets. Their existing current systems are complex and new features or technical capabilities are expensive to implement. Intense pressure on costs makes disruptive investments difficult to make.

Oracles are open-source components (subject to the open-source Apache License version 2.0) that manage interactions between the financial industry's current systems and a list of supported DLTs.

The goal of Oracles is to provide a simple, free of charge solution to connect current systems to supported DLTs and comply with the CAST Framework. Oracles have already been implemented to support real Security Token transactions at front, middle, and back-office levels.

Using Oracles is not mandatory. They can nevertheless be an effective alternative to expensive initial investments to build DLT capabilities and they can reduce development risk. Moving to a full DLT infrastructure to benefit from lower costs in operations can then be progressive, with each market participant transforming its legacy systems and operations at its own pace. With DLT acting as a golden source for any transaction or corporate action, Oracles remove most reconciliation tasks currently performed by the front, middle, and back-offices in a given financial institution or in different institutions.

Different types of Oracles can be implemented, depending on the role of the entity which operates them:

- FRO: Oracle for Registrars
- FSO: Oracle for Settlement Agents
- FIO: Oracle for Investors or brokers/dealers

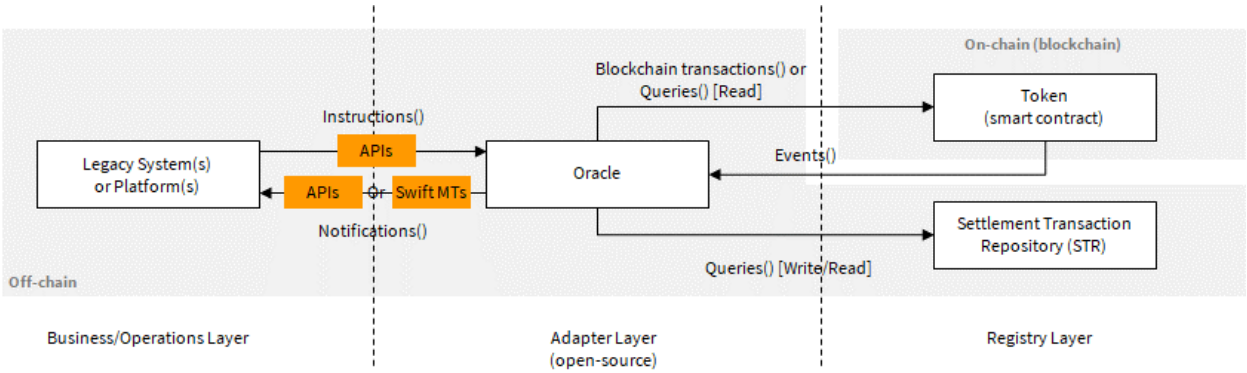
The main functions of the Oracles are to:

- Listen to DLTs and capture events generated during Security Tokens' life cycle;
- Convert captured events into readable information to be consumed by existing systems.
- Interact with the STR to retrieve relevant information on settlement transactions;
- Retrieve available on-chain information;
- Broadcast DLT transactions when acting as Registrar or Settlement Agent

Oracles are accessible through APIs and can produce messages similar to SWIFT messages ("pseudo-SWIFT messages") for better integration of retrieved data into existing systems.

4.1. General principles

Oracles are an adapter layer between existing systems (e.g. post-trade chain) and both the STR and the DLT:



They receive instructions from the business/operations layer and convert them into blockchain transactions (e.g. to create a token) or queries (e.g. to get token public information). The Oracle notifies the business/operations layer using APIs or by generating pseudo-SWIFT messages.

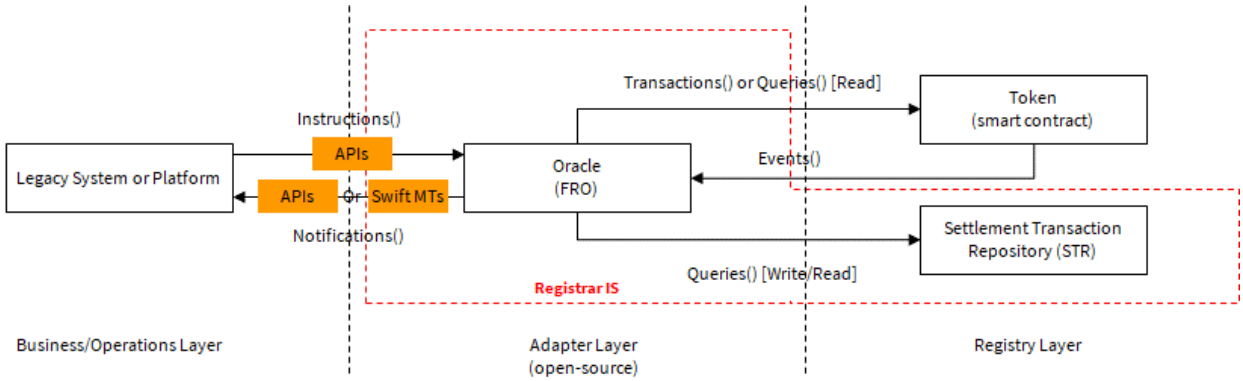
Depending on the market participant role the Oracle can read or write into the STR.

4.2. Registrar setup

The Registrar's Oracle receives instructions (e.g. initiate a trade) from its counterparty (e.g. OTC Facility), converts the instructions into a Settlement transaction written into the STR and then broadcasts a transaction on-chain to perform the corresponding operation (e.g. create a Settlement Workflow).

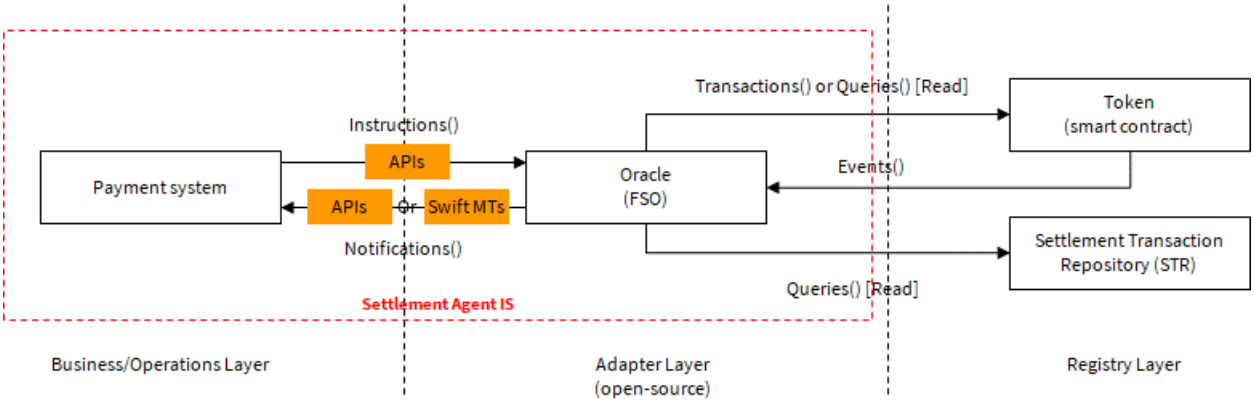
The STR is hosted/managed by the Registrar and stores all Settlement Transactions related to the token for which it is Registrar.

The STR authentication mechanism is agnostic of the Registrar.



4.3. Settlement Agent setup

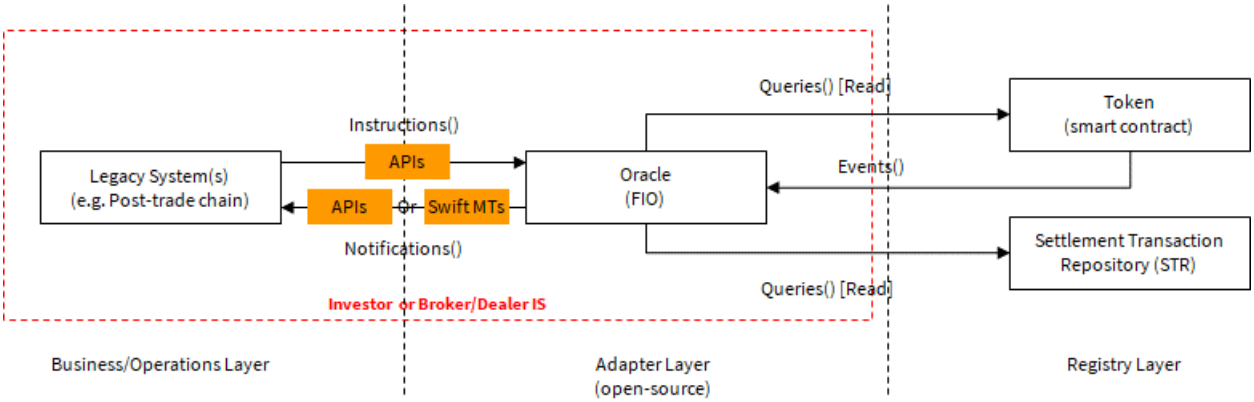
The Oracle receives instructions (e.g. confirm a payment) from the payment system, queries the STR to check the validity of the instructions (e.g. the payment is related to an existing Settlement Transaction and the amount is correct), and if need be broadcasts a blockchain transaction to perform the corresponding operation (e.g. payment confirmation by changing Settlement Workflow state, thus triggering balance updates).



4.4. Security holder and agent setup

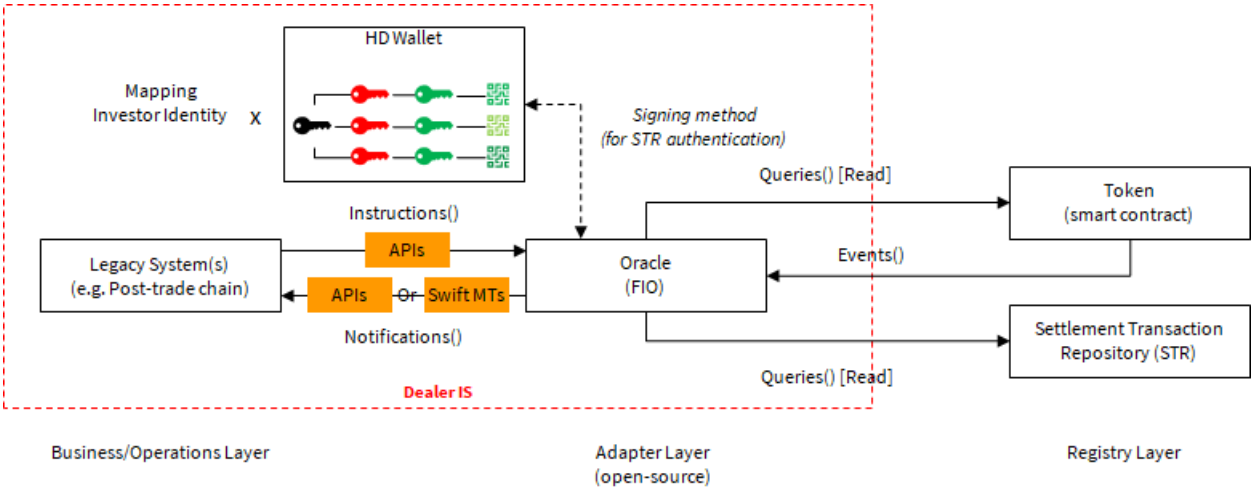
The Oracle receives events each time a settlement transaction is registered on-chain (by the creation of a Settlement Workflow). Events are converted into notifications, either through API data streams or by the generation of pseudo-Swift messages that can be pushed to existing systems (e.g. back-office MQ Series system).

The Oracle can query both the token and the STR to get relevant information (in either API data stream or pseudo-Swift message format).

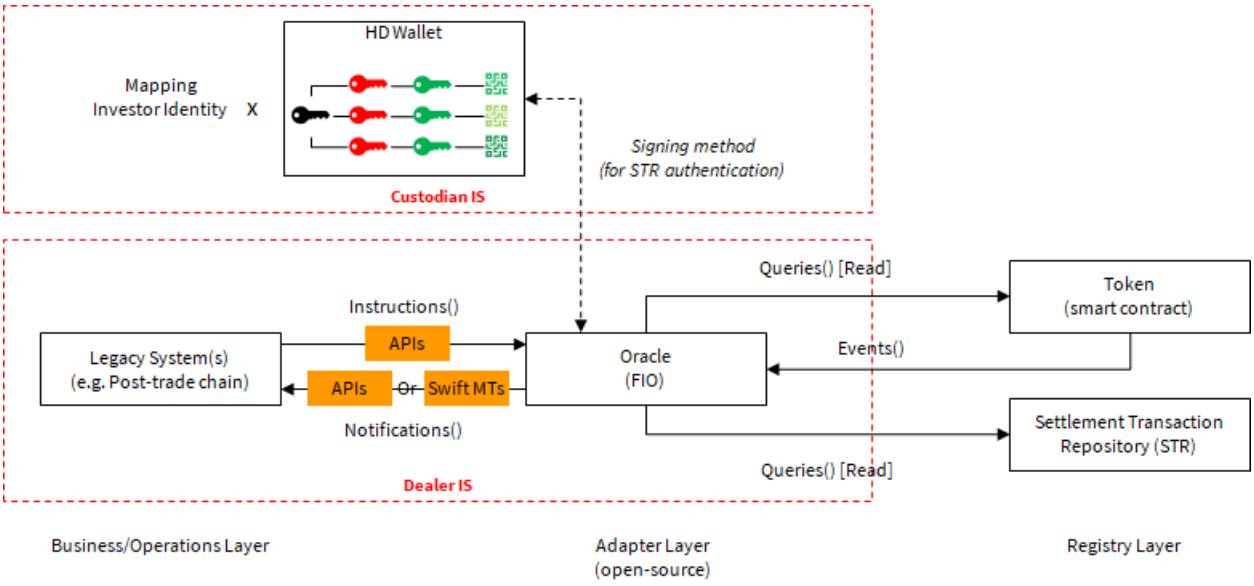


4.5. STR authentication

In order to retrieve information from the STR, the Oracle must be able to activate a signing method from its owner's wallet.



With third-party crypto account management:



Acknowledgements

This White Paper has been written by a working group composed of:
(In alphabetical order)

Jonathan Benichou, Bond structurer at Societe Generale
Stéphane Blemus, Legal counsel at Kalexius law firm
David Durouchoux, COO IT services at Societe Generale Securities Services
Stéphane Duzan, Global IT advisor at Societe Generale Corporate and Investment Banking
Romain Griffiths, Blockchain architect
Julien Muller, Senior trading tool developer at Societe Generale Global Markets
Sylvain Prigent, Trading risk officer at Societe Generale Global Markets
Jean-Marc Stenger, Chief Investment Officer at Lyxor Asset Management

The information and opinions contained herein are the sole responsibility of the authors.

This White Paper benefited from discussions with many stakeholders. The authors would like to thank the reviewers for their time and their valuable comments.

Special thanks go to PwC France who supported us on the regulatory requirements aspects.

5 | APPENDICES

APPENDIX 1: DEFINITIONS

Agency Agreement refers to the multilateral agreement between the Issuer and its Agents (i.e. the Registrar, the Settlement Agent, the Fiscal Agent) which provides a contractual framework for the various services realized by the Issuer's Agents related to the issuance of Digital Assets.

Agent refers to a service provider which is mandated by an Issuer of Digital Assets under an Agency Agreement.

Business Continuity Plan refers to the continuity plan which, under the CAST Framework, must be put in place and maintained to prevent any potential technological disruption and to protect the data registered on a DLT infrastructure (e.g. Ethereum, Tezos, etc.), for regulatory and compliance reasons. In order to avoid a "single point of failure" risk and to enhance investor protection, the CAST Framework provides that the Registrar, acting on behalf of the Issuer, has the mandate to keep an external off-chain register of the Security Token holders and to be able to switch from one technical infrastructure to another if needed to ensure the business continuity of operations. For instance, it can switch from one DLT to another or from a DLT to current infrastructures, should that be necessary. From the instructing party's perspective (Investor, Issuer), the operational friction related to such a technological switch should be minimized by the recording of all information related to the transaction off-chain by the Registrar in an external technological infrastructure, the Settlement Transaction Repository (STR), which would not be affected by any DLT-related incident, as it is set up separate and independently from any DLT.

Calculation Agent refers to the service provider which determines the amount of payment owed by the Issuer to the Security Token holders.

CAST Framework (Compliant Architecture for Security Tokens Framework) means the operating model as well as technological developments in the form of computer programs, the Oracles, developed by Societe Generale - FORGE for the purpose of providing a life cycle target operating model for Digital Assets, notably financial instruments, issued on DLTs. For the sake of clarity, compliance with the CAST Framework does not certify any compliance with the applicable legal and/or regulatory requirements.

Central Bank refers to the public institution that manages the currency of a country or a group of countries and controls the money supply of such currency.

Central Bank Digital Currency (CBDC) refers to a Digital Asset issued by a Central Bank.

Central Counterparty (CCP) means a legal person that interposes itself between the counterparties to contracts traded on one or more financial markets, becoming the buyer for every seller and the seller for every buyer.

Central Securities Depository (CSD) means a legal person that operates a securities settlement system (settlement service), and which provides the initial recording of securities in a book-entry system (notary service) and/or provides and maintains securities accounts at the top tier level (central maintenance service).

Certification Body refers to a company responsible for granting certification and confirming to candidate companies their status as Certified Companies.

Certified Company means a company having completed the application process related to the obtention and use of CAST Certification and which has received confirmation of its status as a Certified Company from the Certification Body.

Crypto-Asset Service Provider (CASP) means any person whose occupation or business is the provision of one or more non-securities Digital Asset services to third parties on a professional basis.

Custody refers to the service of safekeeping and administration of financial instruments for the account of clients, including custodian and related services such as cash/collateral management.

Dealing on own account refers to the trading of financial instruments against the investment firm's proprietary capital.

Delivery-versus-Payment (DvP) is a securities settlement mechanism which links a transfer of securities with a transfer of cash in such a way that the delivery of securities occurs if, and only if, the corresponding transfer of cash occurs and vice versa.

Digital Assets are any digital representation of value or rights which may be registered, issued, transferred and/or stored electronically using Distributed Ledger Technology. Security Tokens are a sub-category of Digital Assets.

Distributed Ledger Technology (DLT) refers to the protocols and supporting infrastructure that allow computers in different locations to propose and validate transactions and update records in a synchronized manner across a network.

DLT MTF refers to a Multilateral Trading Facility (MTF) operated by an investment firm or a market operator that admits listed Security Tokens to trading.

Execution of orders on behalf of clients refers to the execution of buy or sell orders on financial instruments on behalf of a client.

Fiscal Agent refers to the collection and processing of tax duties applicable to Security Token holders prior to the processing of any corporate action.

Governance Body means the company which administrates and manages the community of Certified Companies as well as the CAST Framework and appoints Certification Bodies as the case may be.

Investor refers to an investor which holds one or several Digital Asset(s).

Issuance Facility refers to the facility that will provide Investors with the technological services allowing them to participate in and subscribe to the Security Token issuance.

Issuance Facility Operator refers to the operator of the Issuance Facility.

Issuer refers to the issuer of Digital Assets on a DLT.

Lead Manager refers to the service provider mandated by the Digital Assets' Issuer to facilitate the purchase and sale of the Digital Assets by Investors during the issuance of the Digital Assets.

License refers to the license under which the Oracles are made available and distributed. As of the date of publication of the White Paper, the License is identified as the open-source Apache license Version 2.0.

Operation of a Multilateral Trading Facility (MTF) means bringing together multiple third-party buying and selling interests in financial instruments – in the system and in accordance with non-discretionary rules – in a way that results in a contract. An MTF is the EU equivalent of an ATS (Alternative Trading System) under US law.

Operation of an Organized Trading Facility (OTF) means operating a multilateral system which is not a regulated market or an MTF and in which multiple third-party buying and selling interests in bonds, structured finance products, emission allowances or derivatives are able to interact in the system in a way that results in a contract. Unlike an MTF, equities cannot be listed on an OTF, but an OTF is managed by discretionary rules, contrary to an MTF.

Oracles means the computer code based on the CAST Framework designed for processing data through a distributed ledger, and which are subject to the open-source Apache License version 2.0. Oracles are autonomous and executable technological components acting as distributed ledger adapters (i.e. to capture, collect, register, process and/or transform data stored within a distributed ledger for on-chain specific events, and to enable the access to such data to third party applications via APIs or the exchange of data files using a communication protocol) and as distributed ledger-based transaction generators (i.e. to generate and broadcast on-chain specific transactions).

OTC Facility refers to a facility operated by a regulated entity providing the service of reception and transmission of orders (RTO) and/or execution of orders on behalf of Investors related to over-the-counter transfers of Security Tokens on the secondary market.

Placing of financial instruments relates to the search for subscribers or purchasers on behalf of an Issuer or a seller of financial instruments. Placing may or may not be completed on a firm commitment basis.

Portfolio management refers to the discretionary management of portfolios of financial instruments in accordance with a client mandate.

Reception and transmission of orders in relation to one or more financial instruments (RTO) refers to the receipt and transmission from one Investor to another, on behalf of a client, of orders relating to financial instruments.

Registrar refers to the Agent of the Digital Assets' Issuer mandated to provide the record-keeping of the Digital Assets on behalf of the Issuer (i.e. development of the Smart Contracts creating the Digital Assets and the recording of the Digital Assets on the relevant DLT and of the settlement transactions) as well as to provide registry management services to the Issuer (e.g. to put in place a business continuity plan which would consist notably in keeping at least one full node of the Digital Asset's DLT in order to be able to reconstitute the registry of the Digital Asset holders off-chain). The Registrar can also carry out the role and functions of a Settlement Agent.

Securities Settlement System means a formal arrangement between a plurality of participants whose activity consists of the execution of transfer orders.

Security Token means a security which is issued, recorded, transferred, and stored using a DLT.

Settlement refers to the completion of a securities transaction where it is concluded with the aim of discharging the obligations of the parties to that transaction through the transfer of cash or securities, or both.

Settlement Agent refers to the Agent of the Digital Assets' Issuer mandated to handle cash settlement instructions management in respect of the issuance of the Digital Assets, their sale on the secondary market and/or any payment of interest or principal related to the Digital Assets. The Settlement Agent is a role that can be carried out by the Registrar.

Settlement Transaction Repository (STR) is an off-chain registry managed by the Registrar that stores key information related to Security Token transactions allowing the reconstitution of Security Token holders' positions and balances for a specific date, the identity of Security Token holders or their agents for any specific date and the history of all Security Token holders or their agents since the issuance.

Smart Contracts means a computer program deployed on a distributed ledger in which some or all of the contractual obligations are recorded, replicated or performed automatically.

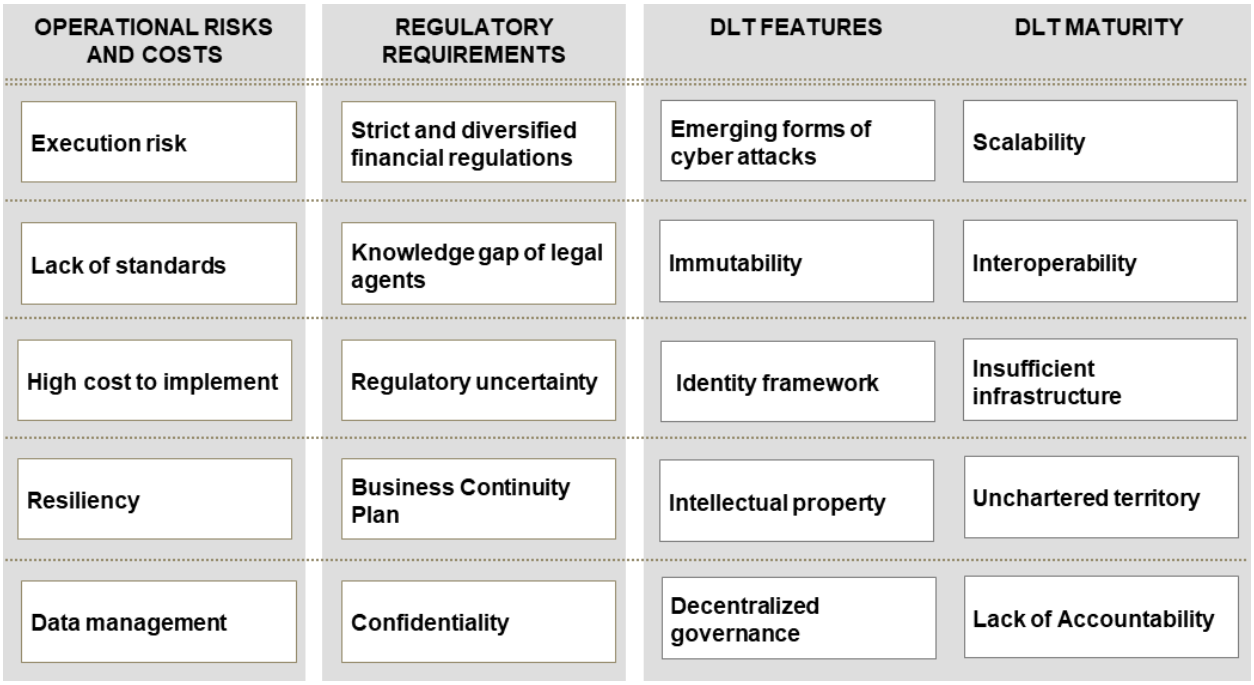
Stablecoins are a type of Digital Asset whose main purpose is to be used as a means of exchange, and which purport to maintain a stable value by referring to the value of one or several fiat currencies that is/are legal tender, one or several commodities or one or several Digital Assets, or a combination thereof.

Structuring Manager refers to the service provider mandated by the Digital Asset Issuer to determine the financial terms of the Digital Asset issue.

Underwriting of financial instruments means the subscription or acquisition of financial instruments directly from the Issuer or seller with a view to reselling them.

Utility Token means a type of Digital Asset which is intended to provide digital access to a good or service available on DLT, and is only accepted by the Issuer of that Digital Asset.

APPENDIX 2: CHALLENGES MATRIX EXPLAINED



The following tables provides a short explanation for each of the challenges listed above.

OPERATIONAL RISKS AND COSTS	
Execution risk	Refers to the risk that a transaction will not be executed as wished by the instructing party (e.g. transaction sent to a wrong address/account).
Lack of standards	Certain types of Digital Assets (with the exception of Security Tokens) do not yet benefit from the same level of standardization as more established financial assets. Many initiatives globally are being undertaken, namely by the International Standards Organization (ISO), which should eventually lead to a higher standardization level. In the meantime, this lower standardization level may represent a challenge for integrating DLT and Digital Assets with legacy systems, from an operational and technical perspective.
High cost to implement	While DLT integration aims at increasing capital market efficiencies, it may in the short term also induce initial investments such as IT system integration with legacy infrastructures, staff upskilling, and operational compliance integration.
Resiliency	Refers to the capacity of a system to recover from incidents in a timely and proper manner. As with any other infrastructure, resiliency is a key topic for DLT and blockchains supporting the exchange and record of Digital Assets. Depending on the technical and governance features of the chosen DLT platforms, resiliency by design may vary. Back-up solutions and overall Business Continuity management is thus key to tackle this challenge.
Data management	A very large amount and wide variety of data can be handled through DLT infrastructures. Proper data security, access and controls are thus key to proper DLT integration and operations. If not properly managed, data may induce operational and compliance risks (such as GDPR related risks, for instance).

REGULATORY REQUIREMENTS	
Strict and diversified financial regulations	Digital Assets are being progressively regulated in a heterogeneous way depending on the jurisdiction and the nature of assets concerned. Integration of the various frameworks by compliance teams may appear challenging but is a necessary pre-requisite for proper operations.
Knowledge gap of legal agents	DLTs evolve very fast, all the more so because most code is shared on an open-source and global basis, making knowledge transfer viral. Keeping up the pace may be a challenge for both regulators and financial institutions' regulatory compliance teams.
Regulatory uncertainty	The very fast innovative dynamics of the DLT ecosystems may be a challenge to follow by regulators. Furthermore, the new business models and technical idiosyncrasies may render some regulations partially unfit, for example, the EU regulation CSDR, at the time of writing this White Paper. This may induce temporary regulatory uncertainty on segments where current regulations are not suitable, as the EU regulators EBA and ESMA advised back in 2019.
Business Continuity Plan	Business continuity planning and crisis management is a key operational element for the financial industry. Public blockchains are decentralized and the continuity of their operations depends on a distributed community. This may appear as a challenge for the financial industry.
Confidentiality	Confidentiality is a very important feature required for financial transactions. DLTs are by design transparent for the whole network, which, used point blank, could be challenging for financial institutions. Privacy features then must be used in order to comply with confidentiality standards.

DLT FEATURES	
Emerging forms of cyber-attacks	As any digital device, DLT infrastructures can be the object of cyber-attacks. The more so when valuable assets are at stake. Specific cybersecurity but also client and Investor protection procedures must be put in place.
Immutability	DLTs are by design immutable. Once a transaction is recorded on the ledger, it is very difficult to change it, unless a majority of nodes agree on it. While this immutability feature is one of the foundations of DLT added value, it may also represent a challenge in situations where data entries are wrongly input into the ledgers. Specific procedures for taking care of these potential incidents must therefore be designed upfront.
Identity framework	Financial institutions must follow strict KYC procedures to comply with AML-CFT regulations. In this context, some may perceive the pseudonymous identity framework of some Digital Assets as challenging. Specific financial security procedures must be put in place.
Intellectual property	Most software code on which DLTs have been developed is open source. Creative Commons licensing is usually used, which differs from the proprietary licensing most financial institutions are used to working with.
Decentralized governance	DLT is based on decentralized governance. Different levels of decentralization can be set up, depending on the openness of the underlying network and consensus mechanisms. Decentralized governance may be perceived as a challenge by financial institutions, as most governance procedures, such as accountability, are based on centralized governance.

DLT MATURITY	
Scalability	DLT has not yet reached the same level of transactional throughput as current market infrastructures. Therefore, scalability may appear as a challenge to overcome when integrating DLT into large scale infrastructures.
Interoperability	DLTs have flourished over the past few years and developed on different underlying protocols. The lack of smooth interoperability between DLTs may be perceived as an obstacle for Digital Asset integration. Furthermore, the different legal treatments concerning Digital Assets globally may limit full Digital Asset interoperability to certain geographical areas.
Insufficient infrastructure	Digital Assets may be perceived as requiring the setup of a whole IT infrastructure. For instance, blockchain node setup, storage and management may hinder financial players in integrating DLT solutions.
Uncharted territory	The financial industry does not yet have much experience in dealing with Digital Assets (with the exception of Security Tokens) - in comparison with what has been done on traditional financial assets. Highly regulated participants may prefer to adopt a wait-and-see attitude before integrating certain types of Digital Assets in their operations, which may slow adoption.
Lack of accountability	The decentralized governance of public DLTs may appear as a challenge for highly regulated entities, as their operations require ex ante risk management and the existence of a clear accountability framework should an incident occur.