



CRYPTO ASSETS: MOVING FROM THEORY TO PRACTICE

- Revision 2022 -

A further analysis of how to issue, settle, safekeep and service Crypto Assets, with recommendations and best practices to maintain compliance with laws and regulations and use standards to maximise interoperability between market participants



April 2022

ABOUT ISSA

ISSA is a Swiss-domiciled association that supports the securities services industry. ISSA's members include CSDs, custodians, technology companies and other firms who are actively involved in all aspects of the securities services value chain.

ISSA - Shaping the future of Securities Services.

DISCLAIMER

It is ISSA's intention that this report should be updated periodically. This document does not represent professional or legal advice and will be subject to changes in regulation, interpretation, or practice. None of the products, services, practices or standards referenced or set out in this report are intended to be prescriptive for Market Participants. Therefore, they should not be viewed as express or implied required market practice. Instead they are meant to be informative reference points which may help Market Participants manage the challenges in today's securities services environment. Neither ISSA nor the members of ISSA's Working Group warrant the accuracy or completeness of the information or analysis contained in this report.

© International Securities Services Association ISSA 2022

No part of this glossary may be reproduced, in whole or in part, without the prior permission from ISSA.

Foreword

The ISSA Working Group on Distributed Ledger Technology (DLT) and Crypto Assets is delighted to present this new paper. ISSA published the original [Crypto Assets: Moving from Theory to Practice](#) paper in November 2019 and this version focuses on the changes in the intervening period rather than repeating the original findings. However, in order to appreciate the full picture, the two papers should be read together. The Glossary of Terms has been added to the ISSA website.

In the past two years, the industry has seen substantial progress in moving DLT from theory into practice. There are now examples of functioning capabilities within securities markets, but these are not yet operating at scale, nor is there a full-scale live DLT system which addresses all aspects of the securities market. These DLT implementations offer some guidance on market structures or business models, but other models are continually being developed. As the paper highlights, the laws and regulations governing Crypto Assets also continue to evolve. In addition, while a number of DLT systems addressing parts of the market are live, the wider implications of DLT in terms of technical performance, efficiency gains, business model impacts, new service potentialities and possible future evolutions are still difficult to predict.

The paper explores the changes in issuance, settlement, safekeeping and asset servicing of Crypto Assets from a practical point of view. It incorporates new sections on Reference Data, Withholding Tax, Insurance, and Cyber & Network Management, which were not covered in the original version. It also highlights the legal and regulatory implications of developing services and platforms for the issuance and trading of Crypto Assets.

The paper draws on the experience of participating members of the ISSA Working Group involved in building products, devising strategies or supporting projects that make use of DLT in existing lines of business in the securities industry. It also takes fully into consideration the robust business and technical standards in place today that strengthen the securities services industry and protect the customers being served.

The ISSA Working Group nevertheless believes that sharing the collective experiences and perspectives of a broad set of industry participants in this paper will contribute to and advance the understanding of DLT and Crypto Assets within the securities markets. Its ambition is to promote a grounded, practical discussion that reaches beyond the hype surrounding DLT. The industry discussions, and those within the regulatory community, can help to build a solid foundation for the Crypto Asset market(s) in general and for a safe and efficient post-trade environment for Crypto Asset issuers and investors in particular.

Target Audience

This paper is addressed to market intermediaries, such as custodian banks, clearers, brokers as well as to asset managers, issuers, industry associations, financial market infrastructures specifically such as CSDs, exchanges and CCPs, regulators and FinTech providers.

Acknowledgements

This report is the result of efforts by a team of experts drawn from ISSA Operating Committee members and other ISSA participating firms. Special thanks go to the authors and the participating firms listed in Appendix. The ISSA Executive Board wishes to thank all supporters for their contributions.

Table of Contents

Foreword	3
Target Audience	4
Acknowledgements	4
Table of Contents	5
1. Introduction.....	6
1.1 The Need for a Safe Environment for Crypto Asset Issuers and Investors	8
1.2 Securities Tokens Will Co-exist with Traditional Securities Issuance	10
2. Issuance Crypto Assets Have the Potential to Simplify the Issuance Process	11
3. Unique Identification of Crypto Assets.....	12
4. Settlement	14
4.1 On-ledger Payment Models for Crypto Asset Settlement	14
4.2 Types of Central Bank Digital Currencies (CBDC) and Stablecoins (SC) Useable in On-ledger Settlement.....	14
4.3 On-ledger Settlement on Multiple DLT Networks or Tokenisation Platforms.....	18
5. Asset Servicing - The Potential Benefits of DLT in Traditional Corporate Actions.....	21
6. Withholding Tax (WHT)	21
7. Safekeeping	23
7.1 Protecting the Private Keys of Investors from Loss	23
7.2 Insurance of the Crypto Assets	24
7.3 Cyber Security & Security of the Crypto Asset and Ransomware Risks.....	25
7.4 Safekeeping the Crypto Asset itself	26
7.5 The Varieties of Digital Wallets.....	27
8. Shareholder Transparency Requirements.....	28
9. Network Management Requirements.....	29
10. Law and Regulation.....	29
10.1 The Legal and Regulatory Status of Crypto Assets is Evolving.....	29
10.2 The Current Regulatory Status of Crypto Assets	31
11. Interoperability	34
11.1 Interoperability Between DLT and Existing Networks is Making Progress	34
11.2 Interoperability Depends on Standards.....	35
11.3 A Potential Role for ISO 20022	37
12. Conclusion.....	39
Appendix: Working Group Members	42

1. Introduction

This paper presumes that the audience is largely aware of Distributed Ledger Technology (DLT) and the opportunities and challenges that are present. This is not the primer that the first paper was but rather an expansion and clarification of areas which have changed over the last two-year period.

The ISSA Working Group agrees that it is undeniable that simply reproducing the existing environment on DLT is pointless. Adopting the technology makes sense only if it enables new configurations and distributions of the work currently undertaken by issuers, custodian banks, CCPs and CSDs. Fortunately, the disruptive potential of DLT does extend beyond a reduction in the number of intermediaries that exchange and reconcile data in the linear chains of intermediation prevailing at present between issuers and investors.

DLT technology has made possible the development of a new type of asset: the Crypto Asset. The term is applied loosely to a wide variety of commodities, as well as assets issued on DLT networks (as with most technological innovations, the terminology of an emergent industry is in flux, and no taxonomy can do full justice to the variety of Crypto Asset projects and products in existence and being launched¹), but a Crypto Asset is best understood as a specific sub-category of digital assets. All counterparties can see and use the same set of data with cryptographically confirmed issuance, termination, ownership and transfer. A digital asset is any asset that can be issued, valued, owned and transferred in a digital form.²

In **Figure 1**, the ISSA Working Group has chosen to divide Crypto Assets into four main categories for the sake of comprehensibility.

The first is **Payment Tokens**, which encompass DLT-based settlement tokens used both for payments on a single chain and for settling cash legs in delivery-versus-payment transactions across interoperating platforms. This category contains not only genuine crypto currencies such as Bitcoin and Ethereum, but also fiat currencies issued in digital form by central banks (also known as Central Bank Digital Currencies, or CBDCs), and Stablecoins which attempt to reduce the price volatility of crypto currencies by linking their value to real assets or fiat currencies.

The second category consists of **Securities Tokens**, which further divide into two groups. The first are known as Asset-backed or “non-native” Securities Tokens. They represent existing instruments - such as stocks, bonds, derivatives and funds - in a new digital form, traded, safekept and settled on a DLT network. Asset-backed tokens could also be used to represent existing illiquid or non-bankable assets such as commodities, titles to real estate and fine art. The second, known as Digital

¹ For a full discussion of the terms used by regulators, see *Global Cryptoasset Regulatory Landscape Study*, Cambridge Centre for Alternative Finance, Judge Business School, University of Cambridge <https://econpapers.repec.org/bookchap/jbsaltfin/-201904-gcrs.htm>

² See the Glossary <https://issanet.org/dlt-and-crypto-assets-glossary/> for a comprehensive list of terms used for digital assets

Native Securities Tokens, create a new group of digital financial assets that are issued directly on to - and exist only on - the DLT network.

The third category is known as **Utility Tokens**. These tokens are designed to be purchased by end-investors interested in gaining access to a current or prospective product or service or app. Their promise to investors is that increased use of the product, service or app will lead to an increase in the value of the tokens. Golem, for example, is a Utility Token that aims to enhance the value of its tokens by persuading investors and consumers to rent their unused computing capacity to members of the network.

The fourth category added for this revision is **Non-Fungible Tokens (NFTs)**. NFTs are cryptographic tokens that explicitly define a singular asset. These assets are generally digital but theoretically can be actual hard assets. The non-fungible expression is the key to their value. Any dollar bill is fungible with any other; you do not check the serial number on the note when you accept it from a bank. A Non-Fungible Token is the equivalent of not only wanting a particular serial number, but also saying that the note with that serial number XXX is not equivalent to any other dollar bill and so to exchange that serial number you may want YYY dollars for the bill.

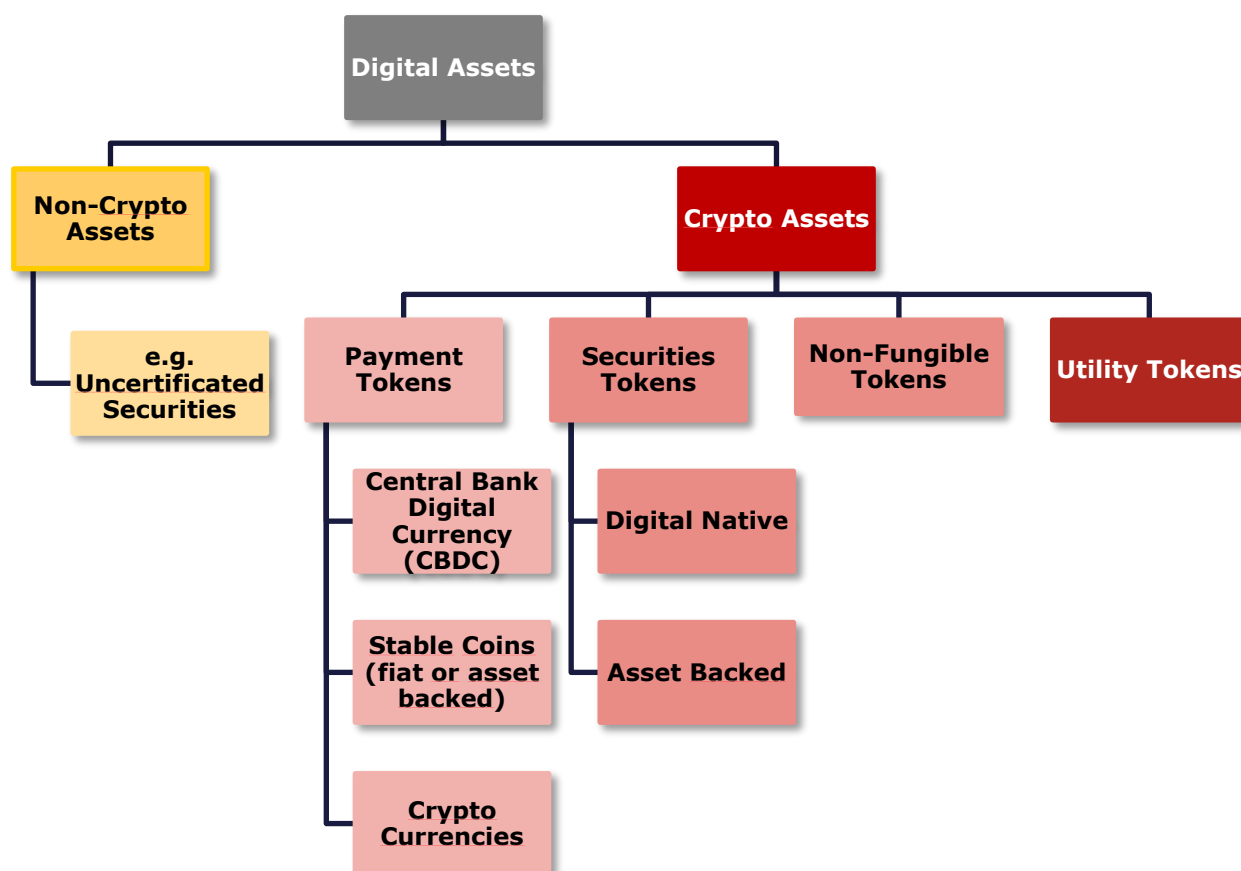


Figure 1: What is a Crypto Asset?

The path of evolution of assets on Distributed Ledger Technology followed the technology’s rise to prominence in 2009 when the Bitcoin launched as the first crypto currency. Later Crypto Assets became available on the DLT or blockchain. This was followed by Blockchain 2.0 based on protocols such as the Ethereum network in 2015. Blockchain 2.0 provided the opportunity to create a token to support multiple and different business models, including the implementation of smart contracts. This has enabled the creation of both the Initial Coin Offerings (ICOs) and now the current Non-Fungible Tokens (NFTs). Blockchain 3.0 focuses on creating solutions for services and industries outside the world of finance.

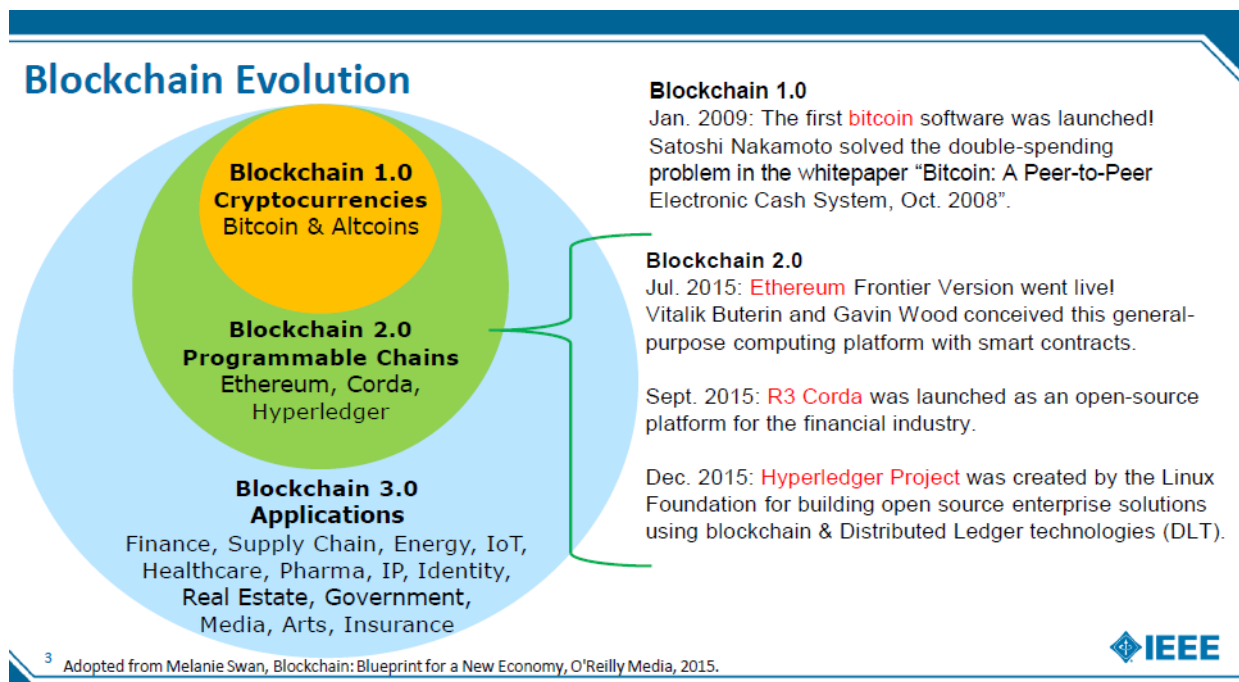


Figure 2: Blockchain Evolution

1.1 The Need for a Safe Environment for Crypto Asset Issuers and Investors

The potential of Crypto Assets to create new investable assets and investment ecosystems is unmistakable. The securities services market acknowledges the transformative potential of Crypto Assets issued on to DLT networks and is experimenting with dozens of proofs-of-concept, go-to-market projects and even implementations. The recent examples of the implementations include the delivery of the first issuance and trade within the regulatory approved SIX Digital Exchange (SDX), and DTCC, Clearstream and Euroclear are all experimenting with, internal only, private DLT implementations for a number of different markets including collateral and private markets. There are many other examples of DLT experiments and this list is not meant to be exhaustive.

There have unfortunately been a number of high profile examples of incompetence, malfeasance and outright fraud within the asset class’s evolution. Therefore many institutional investors are still wary of committing capital to these

instruments in the absence of a reassuring set of Financial Market Infrastructures (FMIs) and intermediaries willing to manage the risks associated with the issuance, trading, settlement, safekeeping and servicing of these assets.

In the capital markets of today, FMIs such as CSDs and CCPs and intermediaries such as custodian banks, undertake the necessary trust-enhancing functions and provide a set of risk-reducing services. CCPs, for example, mitigate counterparty credit risks. CSDs processing securities transactions provide for the legal finality of settlement and the notarisation of issuance that provides certainty of title to assets. Likewise, custodian banks assume sizeable financial risks in, for example, corporate actions and collateral management.

These forms of intermediation obviously cost money, but they also create value. Securities market FMIs and intermediaries assume, transfer, mitigate or reduce the risks of issuing, transacting, settling and owning securities. They have also developed considerable specialist expertise and, by operating with scale economies, keep the costs of safekeeping, settlement, risk management and regulatory compliance within tolerable bounds.

The willingness of investors to pay for these services is matched by regulatory endorsements of the contributions these services make to the reduction of systemic risk. It is clear that both investors and regulators value efficient intermediation in securities markets which reduces the risk within the market and for the investors. Indeed, it has become equally clear that institutional investment in Crypto Assets depends on the provision of equivalent services, so it is unlikely that the Crypto Asset markets will dispense with these services although different providers may perform the necessary roles. In fact, Crypto Assets such as Securities Tokens will need regulated entities to provide a safe and efficient environment to qualify as regulated assets fit for investments by regulated institutions in many jurisdictions. Fortunately, FMIs and intermediaries active in the securities markets are already responding to this opportunity alongside new entrants such as FinTechs.

The established providers are also mindful that Crypto Assets in general, and Securities Tokens in particular, are likely to be regulated under existing securities laws and regulations, though regulations adapted to Crypto Assets will likely emerge and stabilise. Since regulators do not wish to introduce regulations that suppress innovative technologies, they have pursued a pragmatic approach to the regulation of participants in the Crypto Assets ecosystem. The pragmatic approach can be summarised as “same activity / business, same risk, same regulation”.

The objective of the regulators is to ensure that issuers and investors are protected and financial market stability is guaranteed, without discouraging innovation by regulating DLT separately. That means that, for the foreseeable future, issuers and investors in Securities Tokens will need regulated third-party providers, such as CSDs and custodian banks, to ensure they remain in compliance. Likewise, issuers and investors active in the Payment and Utility Token markets will also need to address any relevant regulatory requirements. Further discussion of the regulatory status please see Section 10.

1.2 Securities Tokens Will Co-exist with Traditional Securities Issuance

A wholesale displacement of the existing structure of post-trade services in the securities markets by Securities Tokens is unlikely to occur in the short to medium term. The risks, funding and liquidity implications and costs of making the market-wide changes to the current blend of technologies, governance systems and market structures into a new sophisticated, standardised and robust ecosystem are too high relative to the foreseeable benefits.

The ISSA Working Group concludes that Securities Tokens issued, traded, safekept, administered and settled on DLT networks or tokenisation platforms, i.e. whole new ecosystems for the securities lifecycle, will co-exist with the current ecosystem for some time to come. There may be a transition to a single model at some point, but alternatively divergence may continue for an extended time horizon. After all, DLT-based ecosystems (as currently construed) lack some of the scale advantages of traditional securities, such as the liquidity released by netting of transactions by CCPs.

In addition, while Securities Tokens remain the subject of rapidly increasing experimentation, the securities markets provide a well-established way of raising and channelling capital from savers to organisations that can put it to productive use. The FMIs and other intermediaries processing securities transactions have adopted global standards, best practices and interfaces to provide interoperability on a global basis. So it is essential that the variety of DLT-based and traditional ecosystems that are now emerging are able to interoperate successfully through standardised data exchanges and interfaces. Without interoperability, both operational efficiency and market liquidity will be at risk.

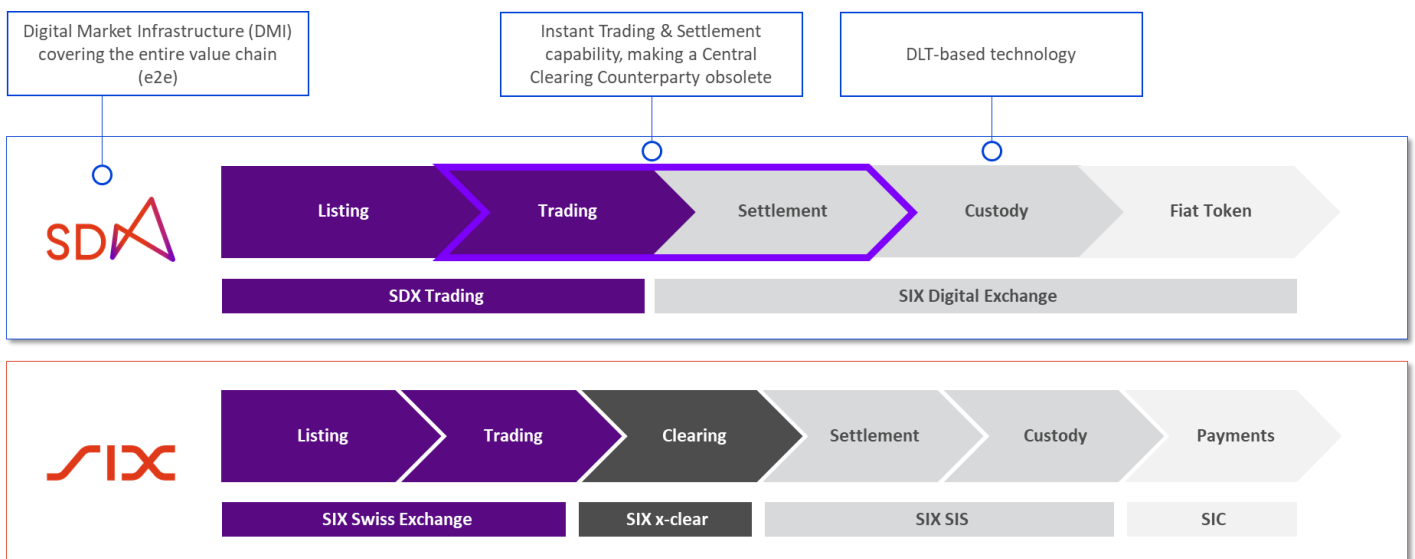


Figure 3: Example of Co-existence and Innovation

Nevertheless, even a partial adoption of Securities Tokens will require changes for existing service providers, such as a willingness to take private keys into custody. Service providers already have private key technology, the simple cryptography

that has been used for decades. The transformation between 2019 and 2022 is that the concept of using this existing technology infrastructure to enable transactions on DLT has been explored and delivered. Entirely new roles, such as smart contract verification services, will also develop. Some of these, such as acting as the governors and / or operators of permissioned DLT networks or tokenisation platforms, will suit existing service providers such as CSDs and custodian banks.

2. Issuance Crypto Assets Have the Potential to Simplify the Issuance Process

The current process of issuing equity and fixed-income securities, whether they are issued publicly or to select investors by private placement, is cumbersome (see Table 1, 2019 paper). It requires the negotiation, agreement and signature of legal documents in which the terms of the issue – such as the pricing, debt covenants, the interest rate references, or the dividend payment dates – are described. New issues also trigger operational requirements, such as eligibility checks for registration, assigning securities identifiers (ISINs, CUSIPS,...etc), collecting subscriptions from investors, paying proceeds to issuers and allocating dividend or interest payments to investors.

In principle, DLT can reduce the cost and complexity of both the legal and the operational aspects of a new issue. However, in the present regulatory and legal construct it cannot obviate the need for legal documentation (such as an offering memorandum or prospectus) or the need for a regulated entity to take responsibility for the integrity of the issue (such as an Issuing and Paying Agent (IPA) and CSD).

Yet a number of the tasks and information exchanges required to originate, syndicate, close, and administer a new issue can potentially be streamlined and orchestrated more efficiently using DLT and Crypto Assets. Investors can subscribe for Crypto Assets directly on the network and hold the assets directly through management of their own keys or delegating the management of their keys to a regulated custodian or CSD. It is in these areas which the ISSA Working Group has seen significant progress over the last two years.

Once the Crypto Assets are issued, they can also be serviced in a more efficient manner on a DLT network and/or leveraging tokenisation platform(s). The benefit a public DLT or shared private DLT can bring is the potential to provide more straight through processing for post-trade administration. For example utilising smart contracts to manage coupon / dividend payments and certain corporate events.

In fact, specialist service providers would be able to join the DLT network as separate “nodes” and offer to complete particular tasks, or parts of tasks, on behalf of issuers. KYC and AML checking services are an obvious example of how DLT networks can not only improve coordination between the elements of a transaction but enhance the service. Some or all of the entirely new roles, such as smart contract verification services, could also join the network as “nodes”. Issuers could auction the right to perform these services on the network.

High Level Process Flow Bond Issuance DLT

Key steps and assumptions:

1. The Payment DLT (P-DLT) will be a generalised term used for the DLT network facilitating the settlement of central bank-like digital cash
2. The Asset DLT (A-DLT) will be a generalised term used for the DLT network facilitating the settlement of the asset
3. The issuer uses an Underwriting Bank and the payments from investors will ultimately be paid by a number of Banks with accounts on the P-DLT
4. It is assumed that the structuring of the bond can be done either traditionally or through one or more digital platforms that plug directly or indirectly into the A and P DLTs
5. It is assumed that smart contracts are used to create and manage transactions on the A and P DLTs

High Level Settlement Flow Between Asset and Payment DLTs During Primary Issuance

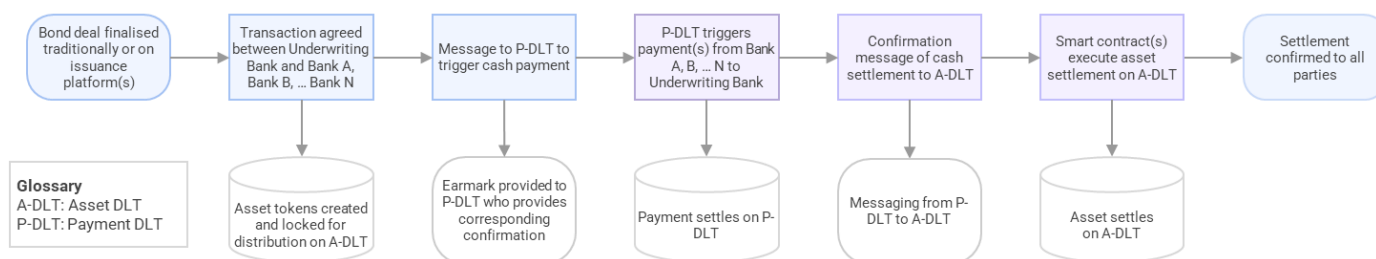


Figure 4: High-level process flow for a bond issuance (Source: Nivaura)

3. Unique Identification of Crypto Assets

Reference data is a key attribute set for any security, irrespective whether for traditional assets or DLT based assets. The traditional asset world has generally done an adequate job in the initial unique identification of an asset through the ISIN (ISO 6166 – International Securities Identification Number) in combination with other identifiers such as the CFI (ISO 10962 – Classification of Financial Instruments), the FISN (ISO 18774 – Financial Instrument Short Name), the MIC (ISO 10383 – Market Identifier Code) and the LEI (ISO 17442 – Legal Entity Identifier).

However, the establishment of a unique identifier for the asset in the DLT context may not be as simple as a traditionally fungible asset. Examples of challenges include the representation of forks, the place of trade (as liquidity may affect price), the jurisdictional dimension of the asset and others. The DLT Standards Working Group (ISSA Working Group) worked with a number of DLT Asset Identifier Organisations in 2021. The conclusion was that there was no “right or wrong” way of describing digital assets, given the challenges. Several identifiers for crypto currencies and assets already co-exist today. The provision of the unique identification of a digital asset is also progressing as the industry matures. The ISSA Working Group has therefore not created a best practice document but rather a matrix (see <https://issanet.org/publications-media/dlt-asset-identifiers/>) that covers all aspects that the ISSA Working Group thinks could or should be covered by a digital asset identifier and the ISSA Working Group has asked the DLT Asset Identifier Organisations to fill in the matrix and update it as their product expands or matures, to provide a reference source for the members. This source will allow the members to understand the offerings in DLT Asset Identifiers and select the source that is most appropriate for their needs and engage with that DLT Asset Identifier Organisation.

For the identification of Central Bank Digital Currencies (CBDCs), the ISO standard for currency codes (ISO 4217) is the de facto standard. The ISO TC 68 Technical Committee for Financial Services did launch an Advisory Group (AG 5) at the end of 2020 to look at digital currencies. The purpose is to provide direction and support for standard definitions and identification of CBDCs and non-FIAT digital currencies and identifying where already existing ISO TC68 standards can and should be used. For the identification of Crypto Assets several standards coexist at the moment. The most commonly used identifier is probably the ticker symbol such as BTC for Bitcoin and ETH for Ethereum.

A new ISO standard for the identification of digital assets called DTI (ISO 24165 – Digital Token Identifier) was published at the end of 2021. This standard consists of two parts:

- ISO 24165-1 describes the method of registration and assignment of a DTI.
- ISO 24165-2 describes the data elements required for registration and display on the DTI registry. The DTI is a random, unique, fixed-length identifier for digital and consists of eight alphanumeric characters. It can be used for a fungible digital asset which uses distributed ledger technology for its issuance, storage, exchange, record of ownership or transaction validation and is not a currency. DTIs will be assigned by a Registration Authority (E-trading Software ETS) and are made available in an online registry.

A partnership between ETS and Association of National Numbering Agencies (ANNA) was established in 2021 to identify synergies between the DTI and existing standards such as the ISIN. Together, the DTI and ISIN will form a bridge between the traditional and tokenized financial world infrastructures used to process financial instruments, with the overall aim of achieving interoperability and all the greater advantages this enables. The two identifiers will complement each other, in that the ISIN is the identifier for the reference data of the asset (i.e. the record of the specific financial or referential instrument), and the DTI will be the technical identifier of the token location (covering the nature of the digital token, how it is issued, in which blockchain,...etc). Potentially, also the Classification of Financial Instruments (CFI), Financial Instrument Short Name (FISN) codes and the Legal Entity Identifier (LEI) would also need to be considered for Crypto Assets.

This is also where the ISO 20022 standard for information exchange between financial parties comes into play. All ISO 20022 securities messages, whether for settlement, asset servicing and collateral management can include the above-mentioned ISO standards, including the DTI. In addition, other data elements needed in order to exchange information related to Crypto Assets have been adapted to deal with the specificities of Crypto Assets e.g. certain fields have been expanded to cater for blockchain addresses as well as quantities and balances with many fractional digits.

Furthermore, there is also the Financial Instrument Global Identifier (FIGI), an open data standard issued by Bloomberg and adopted by the Object Management Group (OMG). It is a 12-character, alphanumeric, randomly generated ID covering hundreds of millions of active and inactive financial instruments. The standard has been extended in 2021 to include Crypto Assets. Crypto-FIGI is a 12-character, alphanumeric randomly generated identification. The first two characters refer to the

certified issuer of the identification. The Registration Authority services are provided by Bloomberg and FIGIs can be found in a register.

A lesser known identifier for Crypto Assets is the ITIN, non-fungible and fungible DLT based cryptographic tokens maintained by the International Token Standardisation Organisation (ITSA). The ITIN has a pattern of 8-alphanumeric characters and a 9th check digit that are randomly generated.

ITSA also provides an International Token Classification (ITC), a framework for classifying cryptographic tokens according to various different dimensions (economic, technological, legal,...etc.) and an International Token Database (Tokenbase) with information on daily prices, market capitalization, trading volumes, etc.

4. Settlement

4.1 On-ledger Payment Models for Crypto Asset Settlement

The “on-ledger” settlement model, where both the Crypto Asset Token and the Payment Token are issued on the same DLT network or tokenisation platform – or at least on DLT networks or tokenisation platforms that are able to interoperate with each other – has a large theoretical advantage. It makes it possible to achieve Token versus Token (TvT) settlement on the DLT network or tokenisation platform itself, without the need for the buyer and the seller to move off the network to access fiat currency payments in central or commercial bank money.

In an ideal world, fiat currencies in central bank money would be available on DLT networks or tokenisation platforms in the form of CBDCs. Central banks across the globe and the BIS are exploring CBDCs. But at present no central bank has issued a CBDC for wholesale markets, primarily because of concerns about the impact on bank funding and lending if central banks compete with commercial banks for CBDC deposits.

The present alternative for “on-ledger” settlement are Stablecoins. These are a group of Payment Tokens that – as the name suggests – seek to overcome the price volatility of conventional crypto currencies by linking the Payment Tokens to a more stable store of value. The simplest structures make the Stablecoin exchangeable on a 1:1 basis with an equivalent amount of fiat currency held in an escrow account.

4.2 Types of Central Bank Digital Currencies (CBDC) and Stablecoins (SC) Useable in On-ledger Settlement

The ISSA paper Blueprint for Central Bank Digital Currencies in Post Trade Settlement (published December 2021) examines the question of how CBDC and SC may interact with settlement in a much greater detail, but quoting the summary is useful here for ease of comprehension:

“As the pilot schemes and experiments continue, changes to regulatory attitudes globally are enabling or envisaging the use of CBDC in the context of securities markets. The use of CBDC can provide several benefits including:

- *faster settlement finality*
- *liquidity and integrity³*
- *atomic settlement*
- *reduced operational work to reconcile between many different systems (including the possibility of aligning securities and cash on a single platform)*
- *programmability (e.g., to detect and call out on the potential of systemic liquidity gridlock,...etc)*
- *process and responsibility changes to reduce risk and increase efficiency.*

The use of CBDC may also present new risks for the ecosystem. In addition, in today’s environment, Central Banks control who is allowed to access to Central Bank money by tightly controlling access to the RTGS systems. For CBDCs the WG believes a similar control mechanism will have to be offered to the Central Banks.

The ISSA Working Group believes that the present market ecosystem is reasonably efficient and, in many instances, allows settlement in central bank money. There are opportunities to further improve efficiency and reduce risks, and some of these opportunities could be realised, potentially, through the introduction of technology including DLT solutions to improve the existing infrastructure. To maintain the benefits of true DvP1 settlement in central bank money, it is logical to conclude that a CBDC using DLT as the underlying technology would be an enabler for this.

*One of the potential opportunities for a transformation from the existing market structure to a CBDC-enabled securities settlement mechanism is that the roles of various parties in the ecosystem could be transformed as a result of their adoption and new roles, better adapted to the new technologies, could emerge. As well as new roles, the ISSA Working Group believes that changes to existing securities processes are required to allow meaningful progress to occur. The ISSA Working Group agrees with the statement within the Euroclear and Banque de France paper: *Experimenting settlement of French government bonds in Central Bank Digital Currency with blockchain technology* to quote:*

“Our experiment also highlighted that the full value of blockchain cannot be realized by simply replicating ‘as is’ the securities settlement operations processes. However, enabling direct access by end investors on the blockchain platform via their custodians and/or removing the current post trade processing breaks, would allow blockchain technology to significantly improve post-trade operations. This could then remove reconciliation processes, reduce the overall cost and increase the efficiency of the capital markets.”

³ <https://www.bis.org/about/bisih/topics/cbdc.htm>

To make the most of the potential efficiencies in cross-border transactions, the ISSA Working Group believes that Central Banks should consider the following CBDC attributes to prevent the fragmentation of market practices and approaches which currently bedevil the existing securities markets:

- *token standardisation*
- *designed for interoperability*
- *programmability*
- *designed for fast adoption (be that open source, using existing infrastructure and existing platforms, or other solutions)*
- *ability to auto-convert between CBDC in the currency of choice; i.e., not a “global” coin, but convertible coins.*

The ISSA Working Group’s view is that for the smooth functioning of the securities industry and the capital-raising capabilities of local companies, it is imperative that CBDC solutions are designed to be interoperable. This means interoperable not only between CBDCs, but also between existing securities platforms and ecosystems since a period of coexistence is likely. The ISSA Working Group would also support interoperability with environments (including SC platforms) which meet the appropriate prudential criteria.

A key finding of the ISSA Working Group is that the potential implementation of CBDC using DLT as the underlying technology within the wholesale securities markets will become the catalyst for the development of DLT adoption in securities ecosystems.

SCs (specifically those which meet the prudential standards and which are backed by a fiat currency) or CBDCs, can offer a useful method of progression to the adoption of digital crypto assets. To be genuinely useful, SC need to be regulated and offer both consumer protection and financial stability: i.e., be a store of value which is easily convertible. As yet, the regulation for SC is at an immature state, but that has not prevented a number of SC underpinning the Decentralised Finance (DeFi) environment.

The potential adoption of SC echoes the current environment where the activities of Settlement Banks have been superseded by Central Bank money for settlement over the decades. However, it should be noted that settlement venue regulations and rules rather than investor choice will govern the settlement venue’s appetite for SC.”

The degree of risk associated with Stablecoins varies by their structure and the type of asset they choose as backing. Some mix other assets (such as gold) with fiat currency. There are structures that reference a non-currency asset such as the price of a commonly traded commodity – oil, for example – without actually holding any of the commodity at all. The issuer might instead hold derivative contracts which pay out in the chosen fiat currency.

It is not unknown for Stablecoins to be backed by Crypto Assets, with over-collateralisation (“haircuts”) used to compensate for the increased level of risk. Some Stablecoins are not asset-backed at all. The so-called “algorithmic” Stablecoins, for

example, claim to maintain their value by restriction of supply alone. The supply of Payment Tokens, in other words, is expanded and reduced according to the dictates of a mathematical algorithm. Other Stablecoins have adopted a hybrid model, in which real asset backing is combined with non-asset-backed measures.

But the most secure type of Stablecoin is not hard to depict. It would be issued by a commercial bank, a consortium of commercial banks, or a CSD with an FMI / banking licence against the fiat currency it holds in its reserve account at the central bank (see Table 1). In such a case, the central banks would almost certainly insist on regulating the DLT network or tokenisation platform on which the Payment Tokens were issued, in the same way that they regulate PMIs. This suggests that existing market infrastructures, such as PMIs or CSDs, or a consortium of commercial banks, are the natural choice as operators of such cash tokenisation platforms. An example of this approach can be found in the approaches outlined within SIX Digital Exchange’s Project Helvetia and its execution and settlement of bond trades.

There are extensive documents available addressing CBDC and Stablecoins. The ISSA Working Group would recommend the avid reader to avail themselves of [WEF Digital Currency Consortium - White paper series - Nov 2021](#) which covers the topic under three headings over eight individual papers. These topics are Regulatory Choices, Value Proposition for the Underserved and Technology Choices.

Description of the Payment Token	Issuers	Custodian of Collateral	Examples (in Development or Production)
Central Bank Digital Currency (CBDC)	Central banks	Central banks	Sveriges Riksbank E-Krona; Central Bank of the Bahamas’ Sand Dollar; Bank of Thailand; Eastern Caribbean Central Bank; Central Bank of Uruguay
Settlement asset backed by cash held in direct reserve accounts at the central bank	PMIs, CSDs, and / or a consortium of commercial banks	Central banks	Digitalised Singapore Dollar (Project Ubin); Stella project of the European Central Bank and the Bank of Japan; Finality International
Stablecoin based on cash deposits at a commercial bank	Commercial banks	Commercial banks	Bank Coin; Signet Coin by Signature Bank; JPM Coin by J.P. Morgan
Stablecoin issued by non-banks	Mainly crypto currency exchanges and related trust companies	Commercial banks	Gemini Dollar (GUSD); Paxos Standard (PAX); Huobi HUSD currency exchange; Circle and Coinbase’s USD Coin (USDC)

Table 1: On-ledger Payment Tokens useable in Settlement

Investors who want access to such a secure Stablecoin would deposit fiat currency with their commercial bank in their own books or in an account at a CSD with a banking licence and request it be converted on a 1:1 basis into Payment Tokens. The commercial bank or CSD would deposit the cash at the central bank and issue the Payment Tokens.

The fiat currency could be immobilised in an omnibus reserve account at the Central Bank or, if a consortium of commercial banks was used, in the account of the banking entity of the consortium at the central bank, with traceable links back to the commercial bank(s) which made the deposit.

The tokens can move independently across the DLT network or tokenisation platform. However, the number of Payment Tokens in issue and circulation will always need to be equal to the amount of immobilised fiat currency held at the central bank, so the owner of the Payment Tokens can at any time convert them back into fiat currency on a 1:1 basis. By doing so, the owner would reduce the amount of Payment Tokens in issue and, by extension, the amount of fiat currency immobilised in the omnibus account at the central bank (see **Figure 4**). However, the process might not be as simple as **Figure 4** suggests. The exact regulatory oversight and supervision of the operator of such a Stablecoin platform, as well as the reconciliation of holdings of fiat currency with the holdings of Payment Tokens, needs further research.

4.3 On-ledger Settlement on Multiple DLT Networks or Tokenisation Platforms

While a single DLT network or tokenisation platform that combines both trading and settlement is the simplest model, market forces are almost certain to create an ecosystem of competing DLT networks and tokenisation platforms. This implies multiple ledgers, some of which integrate issuance, trading and settlement, and some of which specialise in issuance or trading or settlement, or some other combination of the three. This will complicate the settlement process.

It is possible to foresee multiple trading ledgers supported by a single settlement ledger, akin to a CSD settling securities traded on multiple trading venues in the securities markets of today. It is also possible to envisage multiple settlement ledgers competing with each other for the business of multiple trading ledgers trading different Securities Tokens and settling them in the same Payment Tokens, or settling the same Securities Tokens in different Payment Tokens.

A number of pilot projects and feasibility studies have sought to demonstrate how a cross-ledger DvP model could work in practice. *Project Stella*, a study by the European Central Bank (ECB) and the Bank of Japan (BoJ), concluded that it would be possible to deliver two Securities Tokens on two separate ledgers by using “cross-chain atomic swaps.”⁴ More recently, the BIS Innovation Hub and Swiss National Bank’s *Project Helvetia* (run in conjunction with several private sector participants) investigated whether two separate, independent systems could coordinate the execution of certain technical steps to ensure that both the cash leg and delivery leg of a cross-ledger swap settle atomically (i.e., on an “if, and only if” basis). In such cases, the proposed arrangement is to link a tokenised securities platform with a tokenised payment system by deploying compatible smart contracts on each ledger and using a common interoperability protocol to coordinate each step in the DvP settlement flow across the two systems. **Figure 3** illustrates the flows of information between the various entities that are necessary to secure final settlement of transactions on a cross-ledger basis.

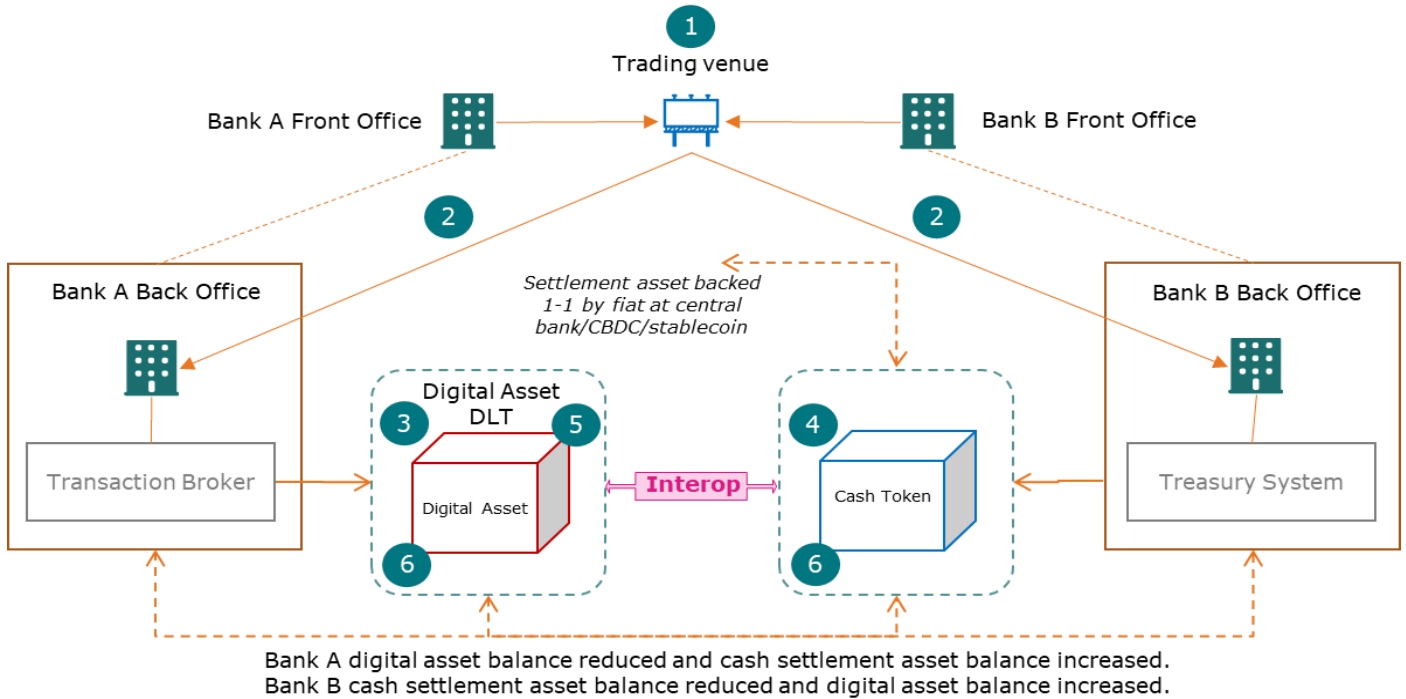
⁴ See European Central Bank, *BOJ/ECB joint research project on distributed ledger technology*, 27 March 2018, page 2 https://www.ecb.europa.eu/pub/pdf/other/stella_project_leaflet_march_2018.pdf

These and similar studies focused on two key areas of concern with this cross-ledger model: (i) that the proposed “hash time-lock” interoperability protocols used to connect the two DLT systems could not guarantee atomic settlement in all cases, for instance where an incorrectly set time-locking mechanism failed to prevent one party from running away with both legs of the trade and thus exposing its counterpart to a settlement risk in the full value of the trade; and (ii) a lack of industry-wide communications standards for the transmission of data between the two ledgers.

Although much work remains to be done, progress is being made on both issues. In particular, a number of academic and private-sector initiatives are investigating new interoperability protocols as alternatives to hash time-lock contracts. These alternatives seek to avoid the problem identified by the ECB and BoJ in Project Stella by (for example), replacing time-out mechanisms with irrevocable technical commitments by which assets are technically earmarked pending either trade settlement or trade cancellation. Though such arrangements still involve certain trade-offs (i.e., by guaranteeing atomicity at the cost of some operational flexibility), they point the way toward a cross-ledger model that provides a genuine delivery-versus-payment capability in a PFMI-compliant way that central banks may be more likely to accept.

Likewise, various industry initiatives are working toward developing common communication standards to enable safe and reliable cross-ledger exchange of data.

Illustrative Flows: Delivery vs. Payment



1. Bank A and Bank B Front Office place an order at a venue; Bank A to sell digital assets, Bank B to buy.
2. Orders are matched, execution order with settlement details goes to all parties.
3. Bank A initiates the settlement. Digital asset ledger records earmark of Bank A's digital asset according to the terms of the settlement. A message is sent to the cash token ledger via interoperability framework.
4. Cash token ledger receives and records proof of earmark and initiates corresponding earmark of Bank B's cash token according to the terms of the settlement.
5. Digital asset ledger receives and records proof of earmark from cash token ledger via interoperability framework.
6. Proofs of earmark validated and recorded, signed digital asset order is executed on digital asset ledger, and signed cash order is executed on cash token ledger (settlement complete and final).

Figure 5: Settlement of Securities Tokens on multiple DLT networks or tokenisation platforms (Source: Fnality)

5. Asset Servicing - The Potential Benefits of DLT in Traditional Corporate Actions

In addition to posing novel challenges in terms of processing corporate actions on Crypto Assets, Distributed Ledger Technology (DLT) has the potential to streamline and improve corporate action information flows on traditional securities.

It could, for example, provide a decentralised database where issuers, CSDs and custodian banks could bring together their respective sets of information: the corporate action announcement, the holdings of investors in the securities at the CSD – and the holdings in sub-custodian bank accounts. This would make it easier to notify investors, obtain instructions and submit instructions on behalf of the underlying investors.

A DLT ecosystem of this kind could significantly reduce current frictions and inefficiencies, such as the duplicated layers of validating the same information throughout the chain of corporate action intermediaries.

6. Withholding Tax (WHT)

Tokenisation also has implications for tax reclaims. In the case of an Asset-Backed Token, the underlying securities are likely to be held by a trust company or Special Purpose Vehicle (SPV), which would be registered in a particular tax jurisdiction. However, the end-investors in the tokens are likely to have a different tax residence, or a variety of tax residences.

Depending on local tax regulations, an investor in a token may not be able to reclaim tax withheld in full under the relevant double taxation treaty if, for example, there is a mismatch between the location of the trust company or SPV and the tax country of residence of the investor. The parallel with the difficulties that can be faced by investors in other asset classes domiciled offshore, such as alternative investment funds, does not need to be laboured.

Payment Tokens, being an entirely new asset class, are likely to lack comparable precedents. Income events derived from Payment Tokens might necessitate new forms of income classification. If so, they are likely also to necessitate new tax rules.

However DLT can also provide a potential solution to the challenges of WHT. One example that the ISSA Working Group has found is described in a paper summarising a pilot project testing DLT by a group of governments and industry participants: *What happens when government, industry and investors seek common digital ground?*

https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/tax/tax-pdfs/ey-withholding-tax-distributed-ledger-report.pdf

To quote from the paper:

“As financial markets have become more globalized over the past 20 years, governments and industry have been grappling with a challenge that centres on cross-border investment, the practical application of tax treaties and withholding taxes (WHT) on passive income. Processing taxable events such as dividends and interest and determining the correct withholding taxes requires synchronized data collection and reporting across a complex network of financial intermediaries and tax authorities.

Although statutory WHT rates can be as high as 35%, they can be reduced or even eliminated by tax treaties or domestic law provisions if the investor meets certain requirements and provides the required evidentiary proof.

The withholding tax challenge is in proving that financial markets investors are entitled to tax treaty relief and making sure that the correct amount of withholding tax is paid can involve complicated, cumbersome, often inefficient paper-based manual processes with risk of human error and fraud. Coordinating the timely exchange of information across an extensive and complex network of intermediaries, while meeting contractual and regulatory requirements, is very difficult.

Without timely information being available, providing treaty relief at the time of the payment (relief at source) creates a risk for withholding agents and governments. As a consequence, treaty benefits are often provided after the payment has taken place, through a reclaim system that could result in administrative costs, opportunity costs and costs related to the time value of money. In certain instances, access to treaty benefits is unavailable in practice.”

Those familiar with the WHT tax challenge recognise this as a succinct summary of the challenges faced on a daily basis. The paper indicates participants in the group, who included Her Majesty’s Revenue and Customs (HMRC), the Netherlands Tax Authorities (NTA), Norwegian Tax Administration, EY, BNP Paribas Securities Services, Citibank, N.A., JP Morgan Securities Services, Northern Trust and with invited academics Vienna University of Economics and Business (Austria) and the Tax Administration Research Centre (TARC, University of Exeter), observers APG Asset Management N.V. and PGGM Investment Management and others, collaborated to formulate and test a solution.

“The project goal was to demonstrate, test and evaluate the feasibility of leveraging new technology for administering withholding tax that could:

- *Evidence cross-border investors’ entitlement to tax treaty relief.*
- *Help make sure the correct amount of tax is paid.*
- *Substantially lower the vulnerability to fraud.*

- *Provide a reliable, confidential and user-friendly way to share information and documentation on a (near) real-time basis across a complex network of intermediaries: registrars, transfer agents, local and global custodians, fund managers, distributors, withholding agents and tax authorities.*
- *Improve the sustainability of the process and reduce the carbon impact of the existing practices...*

...Distributed ledger technology as a solution to the WHT challenge is no longer merely a concept. This project has provided tangible evidence of a near future in which technology can assist industry and governments to reconcile legal and technical issues and also could flex to address different demands and requirements of taxpayers and tax authorities. With the potential for enabling a global solution, this could support the European Commission's proposal to begin building ...a common, standardized, EU-wide system for withholding tax relief at source."

The publicly available WHT paper which can be found on EY's Website is an excellent resource and should be read by all practitioners in its entirety, but the above selective quotes show the real opportunity in using DLT for tracking and processing a manually intensive and complex area of traditional finance using new technology solutions.

7. Safekeeping

7.1 Protecting the Private Keys of Investors from Loss

A challenge in paying entitlements to Crypto Asset investors lies in identifying beneficial owners. The soundest guide to beneficial ownership is possession of private keys: the cryptographic signatures that authorise the spending of crypto currency or the transfer of Crypto Assets.

In a public or "permissionless" DLT network, private keys are the only way to identify the owner of a Crypto Asset. Anybody who holds the private key to a public address (the DLT equivalent of a securities account and its standing settlement instructions) on a permissionless DLT network will enjoy full rights of ownership to that Crypto Asset. Being anonymous as well, Crypto Assets held in this way are comparable to bearer share and bond certificates.

Just as a loss of the bearer certificate is tantamount to a loss of the asset, so the loss of the private key to a public address is equivalent to losing the Crypto Asset. In fact, it is precisely because Crypto Assets are created and exist solely through a DLT network or tokenisation platform that institutional investors are wary of investing in Crypto Assets on permissionless DLT networks. Their concern is justified. In May 2019, for example, Crypto currency exchange Binance announced a data breach that resulted in the loss of US\$40 million in crypto currency.⁵

⁵ Hack Brief: Hackers Stole \$40 million from Binance Crypto Currency Exchange, Wired, 8 May 2019 <https://www.wired.com/story/hack-binance-cryptocurrency-exchange/>

To address this problem for investors in permissionless DLT networks or tokenisation platforms, technologies are being developed. Techniques such as the ERC 884 token allow for the burning and reissuing of Securities Tokens in the event of the loss or theft of the private keys. Holders of tokens on permissioned networks have the assurance of access to the “master keys” (sometimes known as “seeds” – see below) used to create all the private and public keys on the network.

However, the risk of loss of private keys leading to a loss of assets in permissioned DLT networks or tokenisation platforms is reduced mainly by governance and control measures. In fact, the most obvious risk mitigant is the fact that a permissioned network is a closed one. This means the ability to “write” information on to the ledger and create a consensus on the validity of transactions is restricted to a group of pre-approved members.

Another risk-reducing measure is that permissioned networks can apply an old-fashioned “maker-checker” or “four eyes” process that makes transfers less open to manipulation. A third risk mitigant is the fact that ownership of Crypto Assets can be recorded in “off-ledger” databases controlled by trusted third parties as well as “on-ledger”. Indeed, the operator of a permissioned DLT network or tokenisation platform can create new private keys to replace any that are lost.

Another service that can be offered is the custody of “Cryptographic Seed”. In a nutshell, blockchains are basically list of linked transactions lists, each one chained to the previous one through the use of cryptography. These solutions allow participants to deposit information in digital wallets whose access is controlled by asymmetric cryptography, which consists of a public key – usually used as an address or wallet – and a private key, equivalent to the password that allows authorization of transactions. In case of loss of the private key, it can be regenerated by applying a hash function on a sequence of ordered words that only the participant who owns the address knows. This sequence is known as “Cryptographic Seed”.

This Cryptographic Seed acts as a backup copy, and therefore must be stored safely. It can be guarded digitally and also physically. There are two ways to store this seed:

- Encrypted and stored digitally.
- Physical.

In both cases a trusted third party is required to custody this seed.

7.2 Insurance of the Crypto Assets

The digital asset custody insurance market remains nascent. This is a function of the novelty of digital assets compared to say life insurance. The Crypto Assets market capitalization is at nearly US\$2 trillion with equivalent insurance coverage estimated between US\$6–8 billion notional, delineating the paltry coverage of today’s Crypto Assets.⁶ The volatility of Crypto Assets prices, complexities of pricing affordably for market participants, regulatory uncertainty in key jurisdictions

⁶ Blockdata report <https://www.blockdata.tech/>

and some high profile and non-trivial losses within the sector contribute to the difficulty in provision of sufficient insurance coverage. Further, the universe of talented actuaries who understand the insurance sector, Crypto Assets and cybersecurity risks is a very small one.

The resultant insurance protections that are offered are either offered at a very high price or for relatively trivial amounts compared to the notional value at risk, particularly for digital custodians at the start of their businesses' existence. Regulated custodians are perceived to be lower risk prospects and are likely to have larger coverage for lower premiums, though it seems, most Crypto Assets firms remain under-insured.

The ISSA Working Group expects to see the situation improve over the longer term as the industry matures, potentially improving its risk profile and as the length of loss history increases and the underwriting premiums fall. In response to the US\$40 million Binance hack, the group recently announced a US\$1 billion Binance Secure Asset Fund for Users (SAFU) which acts as an effective safeguard as well as protection for users.⁷ The SAFU does not cover the whole potential exposure if there was a catastrophic event but is an essential element of the “waterfall” of exposure mitigation. Evertas, a Chicago-based Crypto Assets insurance company, licensed in Bermuda, became the first cover holder at Lloyd's to specifically cover digital wallet products and write policies on behalf of Lloyd's syndicate member Arch Insurance, which also served as sponsor of the Evertas cover holder application.⁸ Various committees within the U.S. Congress and regulatory bodies as well as the European Union's Markets in Crypto-Assets (MiCA) are also considering regulatory requirements for Crypto Assets service providers to implement insurance policies (albeit these will be potentially costly at the present time).

7.3 Cyber Security & Security of the Crypto Asset and Ransomware Risks

As Crypto Assets evolve into increased mainstream adoption, inevitably, so do cyber hacks, ransomware and cybersecurity risks. Chainalysis estimates crypto-related crime may be at an all-time high whereby scammers took a record US\$14 billion in 2021, the lion's share of which are related to DeFi related hacks, smart contract vulnerabilities and scamming.⁹ Although the vast majority of Crypto Assets crime was related to DeFi scamming, the growth (estimated at 912% in 2021) and legitimate uses of DeFi are a welcome addition to the financial markets and all nascent markets attract fraudsters – as was seen with the widespread adoption of cheques/checks in the last century.

NFT thefts and hacks in 2022 have been seen as the highest vulnerability with examples such as OpenSea and other platforms having experienced varying degrees of NFT thefts caused by user errors on Metamask, scamming / phishing emails and smart contract code vulnerabilities.

⁷ Binance Builds up US\$1 billion Insurance Fund amid Crypto Hacks, Ben Bartenstein, Bloomberg, 31 January 2022

⁸ Crypto Insurance Firm Evertas Wins Lloyd's of London Approval, Ian Allison, Coindes, 03 February 2022

⁹ Crypto Crime Report 2021, Chainalysis

White hat hackers within the crypto community have formed bug bounties and groups like Immunifi work to communicate, highlight and track various hacks, thefts, code vulnerabilities across the entire ecosystem, with a good deal of communication happening on Twitter and / or chat groups.

According to Gartner, criminal cryptocurrency transactions are predicted to drop by 30% by 2024. The reasons cited include: blockchains are more transparent than fiat payment networks, the emergence of sophisticated blockchain intelligence market including CipherTrace (a Mastercard company), Chainalysis, TRM Labs, Merkle Science etc to help track the ‘bad actors’, government prioritization of cybersecurity efforts including Crypto Assets issues and finally, jurisdictions which have implemented Financial Action Task Force (FATF)’s Travel Rule guidance for VASPs (Virtual Asset Service Providers, including exchanges) demonstrate most VASPs are not likely havens for criminal activity versus self-hosted wallets and non-VASP venues for trading.¹⁰

7.4 Safekeeping the Crypto Asset itself

The discussion above makes it surprising to find private keys routinely identified as the principal asset in need of safekeeping when it comes to investing in Crypto Assets. Of course, custodians or CSDs providing safekeeping services to investors in Crypto Assets must offer assurance that private keys are held securely. But if private keys are all an independent custodian holds in custody the service amounts to little more than a digital version of locking a paper security in a vault. The custodian is in no position to protect the actual Crypto Asset or prove that instructions to transfer it are valid. It is little more than a useful back-up service for investors who lose their private keys.

If an investor requests a custodian or CSD to safekeep the private keys only, the custodian or CSD has no right to access the Crypto Asset. The investor retains control over access to the Crypto Asset, in much the same way that a bank client retains control of access to an item in a bank vault. A custodian or CSD that safekeeps private keys only is in no position to guarantee the safety of the actual Crypto Asset or to validate that any transfer instructions originated from the investor. The Crypto Asset could in principle be transferred to anyone by anyone who knows the private keys.

The safekeeping of the actual Crypto Asset by the custodian or CSD is a more secure alternative, which better reflects the reality of service offerings in the market. In this case, the investor transfers the Crypto Asset to the digital wallet address of the custodian or CSD, along with the ability to directly access and transfer the Crypto Asset. The private keys are held by the custodian or CSD only. The digital wallet provided by the custodian or CSD can also offer segregated wallet addresses (in which the Crypto Asset is held in the name of the investor) or omnibus wallet addresses (in which the Crypto Assets of multiple investors are commingled).

¹⁰ Predicts 2022: Prepare for Blockchain-Based Digital Disruption, Gartner article, Avivah Litan, 14 January 2022

Clients can buy and sell Crypto Assets by using existing authentication mechanisms to access the systems of the custodian or CSD and issue transfer instructions. Authentication can be bolstered by a variety of established techniques adapted to the digital age. They include threshold signatures (in which the ability to construct a signature is divided across multiple devices, in the same way that two factor authentication works) and multiple signatures (where it takes multiple private keys to authorise a transaction).

In order to gain traction, it will require Custodians and CSDs to work with and interoperate with the execution venues where digital assets are traded to allow assets to be transferred on and off the execution venue. This will allow them to support customers who want to be able trade and settle on multiple venues.

7.5 The Varieties of Digital Wallets

Digital wallets come in three varieties, each of which strikes a different balance between safety and liquidity.

A **“hot”** wallet remains connected to the internet, and so is vulnerable to being hacked, but means the Crypto Assets are available online for immediate transfer.

“Cold” wallets, on the other hand, keep private keys offline in physical form (usually paper) or in devices which are not connected to the internet. The Hardware Security Module (HSM), or hardware wallet, is a way of storing private keys which ensures they never leave the physical device. All functions requiring access to those keys are then executed directly on those devices, complemented by additional security features such as two factor authentication, personal identification numbers (PINs) and the “four eyes” principle. Because transactions are always signed within the separate device, the private keys are never exposed to hackers. However, transfer of Crypto Assets from “cold” wallets of this kind is inevitably more cumbersome and time-consuming and inhibits immediate liquidity.

In addition to “hot” and “cold” digital wallets there are hybrids known as **“warm”** wallets. The most popular of these can receive Crypto Assets from any public address but can transfer Crypto Assets to a restricted list of (generally “cold”) wallet addresses only. Their operation is akin to a retail deposit savings account whose contents can only be transferred to a retail checking account held by the same investor. This provides a degree of liquidity while reducing the risk of fraudulent transfer to unspecified parties.

The risk of being hacked is not, of course, specific to assets issued and held on DLT networks or tokenisation platforms. Securities held in digital form at CSDs and custodian banks are equally vulnerable to being stolen by hackers.¹¹ That said,

¹¹ See Cyber Risk Management in Securities Services, a report by the ISSA Working Group on Cyber Risks in Securities Services, October 2018 https://issanet.org/e/pdf/2018-10_ISSA_Cyber_Risk_in_Securities_Services.pdf

Crypto Assets do create novel risks. Smart contracts, in which contractual obligations are fulfilled automatically, making mistakes hard to reverse, is one example, exacerbated by the legal uncertainty of smart contracts.

But in practice DLT networks or tokenisation platforms create few genuinely unprecedented risks. And despite the novelty of the terminology, the purpose of all the safekeeping measures – private keys, “hot”, “cold” and “warm” digital wallets, Hardware Security Modules and threshold and multiple signatures – associated with Crypto Assets, is deeply familiar.

Custodians and CSDs between them fulfil two vital responsibilities in the securities markets. The first is to protect investors against the risk of the loss of their assets and the entitlements that belong to those assets. The second is to ensure that they retain ready access to them when they wish to sell or pledge collateral. They are well-placed to fulfil the same responsibilities in Crypto Asset markets.

After all, securing good title, and ensuring that transfers are valid and fully authenticated, are techniques custodians and CSDs have combined to deliver to investors in securities for a long time. More importantly, their fulfilment can also help investors in Crypto Assets comply with extant laws and regulations which apply as certainly to Crypto Assets as they do to securities.

8. Shareholder Transparency Requirements

However, there is one emerging aspect of safekeeping in which DLT networks or tokenisation platforms appear to offer an advantage over familiar methods. This is shareholder transparency or, more broadly, the improvement of communications between issuers and investors. The intention is that investors play a more significant role in the strategies and behaviour of the companies they own, and issuers engage investors more in their decision-making processes.

Today, communications between issuers and end-investors are intermediated by five or more layers of service provision, including asset managers, CSDs, global custodian banks, sub-custodian banks, proxy voting agencies and others. Direct contact between issuers and investors is infrequent. The processes of collecting and updating shareholder information, communicating it to investors and collecting their voting preferences are complex and time-consuming.

In theory, Securities Tokens issued on to DLT networks or tokenisation platforms can shorten this extended chain of intermediation and bring issuers and investors directly into contact with each other on a single network, where safe custody and asset servicing can also be provided directly. Even a more limited application of DLT, such as using the technology to support a parallel platform that maintains an updated list of shareholders per issuer based on settled positions provided by custodians, could make existing processes more efficient. The same system could then be used to facilitate communications between issuers and investors.

The issue is topical because regulators in a number of jurisdictions are encouraging richer and more frequent dialogue between issuers and investors. In the European Union (EU), for example, the second iteration of the Shareholders Rights Directive (SRD II) imposes obligations on custodian banks to improve and accelerate proxy voting services and make it quicker and easier for issuers to identify their shareholders. The use of DLT networks and tokenisation platforms should be explored for these purposes alone.

9. Network Management Requirements

Under various legal frameworks across the globe, there is a requirement for the custodian to perform due diligence on third parties who are providing services on behalf of the end clients. Historically this due diligence has been performed on many, but certainly in the low hundreds, of sub-custodians. These due diligence assessments are carried out using highly defined models for assessing the strength and viability of agent banks and FMIs, and their compliance with key investment and client money regulations.

New models need to be developed which cover the emerging requirements. These need to cover both the new risks which come from the safekeeping of digital assets but also potentially the greatly increased number of due diligence assessments to be made.

10. Law and Regulation

10.1 The Legal and Regulatory Status of Crypto Assets is Evolving

The issuance, trading, settlement and safekeeping of securities is well-defined in both law and regulation in every jurisdiction with an active capital market. The extension of these legal and regulatory frameworks to ecosystems based on DLT networks or tokenisation platforms is settled in a few jurisdictions and not yet settled in many others. It is however prudent to always assume that securities laws and regulations apply to Securities Tokens. It is also reasonable to expect existing securities laws and regulations to be extended and adapted over time to accommodate Crypto Asset ecosystems, not least because many regulatory authorities around the world are working to achieve this.

Nevertheless, issuers and investors in Crypto Assets are currently operating in an environment in which the legal and regulatory status of these new instruments is still evolving. In these circumstances, the techniques developed by the securities services industry to comply with laws and regulations governing the issuance, settlement, custody and servicing of securities provide valuable insights into how investors in Crypto Assets can be protected and the integrity of the markets maintained.

So what are the continuing challenges for regulators in this space that mean they have not been able to provide a stable and transparent regulatory environment?

1. There is an inability to agree on a standard set of taxonomy for different Crypto Assets on a global basis. This is because there are many different factors at play that need to be taken into consideration, whether risk profiles, different underlying technologies, continued evolution of the Crypto Asset landscape itself and the historic challenges of defining a security. A key example of this would be in relation to Stablecoins which can have significantly different risk profiles depending on their issuer and their underlying assets that support them.
2. There is a recognition by regulators that the emerging Crypto Asset market will need to interact with existing financial markets. This requires an understanding of where existing regulatory perimeters can be applied to Crypto Assets and where new regulation is needed. The difficulty is determining where the key gaps are and applying new rules in a proportionate manner.
3. Although many governments are keen to see innovation thrive in their jurisdictions, DLT and related products being a particular area of focus, regulators are wary of allowing the growth of the crypto market to a point where it becomes a risk to financial stability. Criticism following the 2009 crisis, has understandably driven a conservative approach to a new market that has the potential to introduce new risks.
4. There is a perception that DLT technology is intrinsically linked with the Crypto Assets themselves and the governance around them; i.e., by utilising distributed architecture there is not one body or authority that is accountable when things go wrong. In a regulatory environment that focusses on holding institutions and individuals to account, this is difficult to reconcile. There is a desire amongst many in the regulatory community to apply a *same activities, same risk, same rules* approach, but this can be difficult to apply if it is not clear that the activities and risks are the same as in existing markets.
5. Linked to the governance point, there is a perception that the distributed nature of the technology is a threat to operational resilience rather than it being a positive development that has the potential to reduce single points of failure and reduce complexity in post trade processes. Regulators are looking for the industry to explain exactly how the technology can withstand cyberattacks, cloud outages...etc.

Over the last two years it could be recognised that the debate around Crypto Assets, being classified as securities, was often overlaid by the discussions around Stablecoin arrangements. In the latest FSB progress report [Regulation, Supervision and Oversight of “Global Stablecoin” Arrangements \(fsb.org\)](#) on the implementation of the FSB High-Level Recommendations, it has been noted that:

“Jurisdictions have taken or are considering different approaches towards implementing the high-level recommendations. As the stablecoin landscape is evolving rapidly and as regulatory and supervisory policies are being developed, the differences among regulatory approaches and classifications could be increasing. For example, certain jurisdictions are seeking to implement the recommendations through the adoption of new rules and regulations, while others have amended or plan to amend existing rules and regulations in such a way that these are applicable to Stablecoins. Other jurisdictions have relied largely on existing regulatory, supervisory and oversight regimes to address the risks associated with Stablecoins or with entities that are part of the stablecoin arrangement.”

Differing regulatory classifications and approaches to Stablecoins at jurisdictional level could give rise to the risk of regulatory arbitrage and harmful market fragmentation.”

That said, “Authorities have identified several issues relating to the implementation of the recommendations that may warrant further consideration and where further work at international level could be useful. These include: conditions for qualifying a stablecoin as a “global stablecoin”; prudential, investor protection and other requirements for issuers, custodians and providers of other global stablecoin functions (e.g. wallet providers); redemption rights; cross-border and cross-sectoral cooperation and coordination; and mutual recognition and deference.”

The Global Blockchain Business Council (GBBC) issued a comprehensive paper [Global Standards Mapping Initiative 2.0](#) with input from many organisations, including ISSA. This paper addresses many of the regulatory points in the following section (and more in addition) in far greater depth. It is a very helpful survey of the current status of regulatory efforts across the globe.

10.2 The Current Regulatory Status of Crypto Assets

Amid these uncertainties and concerns, one legal and regulatory issue is paramount for custodians and CSDs. Clarity over the regulatory standing of a Crypto Asset is a prerequisite for adoption by issuers, investment by investors and support from service providers since it has implications for the legal soundness of the investment and the legal status of the entities servicing such assets and the services they provide. Moreover, the legal status of a Crypto Asset also influences its accounting treatment.

The key distinction to be established in regulation is whether a Crypto Asset is a security or a payment or something else. The criteria by which a Crypto Asset is judged to be a security varies between jurisdictions, complicating any assessment of the risks Crypto Asset service providers incur in different jurisdictions – or at least forcing service providers to make judgments on a jurisdiction-by-jurisdiction basis. Additionally, the emergence of Crypto Assets illustrated, that assets may be issued fitting into one category, but throughout the lifecycle of their existence may change their characteristics and fall into a different category. The prime example for this is Bitcoin. Initially issued with the intention to serve as a payment medium, it is now primarily used as an investment vehicle.

Some regulators assess Crypto Assets on a case-by-case basis but others use fixed criteria. Some jurisdictions, such as the United Kingdom, have come up with guidance frameworks to categorise Payment Tokens, Utility Tokens and Securities Tokens. Other jurisdictions have provided frameworks to help market participants assess whether securities law applies to particular Crypto Assets. In the United States, for example, the Securities and Exchange Commission (SEC) “Framework for

‘Investment Contract’ Analysis of Digital Assets” uses the Howey test.¹² In France, the Autorité des Marchés Financiers (AMF) has used the PACTE (Action Plan for Business Growth and Transformation) Law to support the development of specific types of Crypto Assets.

The ISSA Working Group recognised that some jurisdictions have built or are in the process of building a legal framework for Crypto Assets to create certainty for the financial markets. Some authorities are updating existing frameworks while others build new frameworks on top of the existing ones. A few examples:

European Union

On 24 September 2020, The European Commission (EUComm) adopted a digital finance package, including a digital finance strategy and legislative proposals on Crypto Assets and digital resilience, for a competitive EU financial sector that gives consumers access to innovative financial products, while ensuring consumer protection and financial stability. With regard to Crypto Assets, the EU differentiates between those Crypto Assets already governed by EU legislation and other Crypto Assets. The former will remain subject to existing legislation but the EUComm proposes a pilot regime for market infrastructures that wish to try to trade and settle transactions in financial instruments in Crypto Asset form. This should enable market participants and regulators to gain experience with the use of DLTs exchanges that would trade or record shares or bonds on the digital ledger.

For previously unregulated Crypto Assets, including ‘Stablecoins’, the EUComm proposes a bespoke regime (“Markets in Crypto Assets, MiCA”). The proposed regulation sets strict requirements for issuers of Crypto Assets in Europe and Crypto Asset service providers wishing to apply for an authorisation to provide their services in the single market. Safeguards include capital requirements, custody of assets, a mandatory complaint holder procedure available to investors and rights of the investor against the issuer. Issuers of significant asset-backed Crypto Assets would be subject to more stringent capital requirements, liquidity management and interoperability requirements.

Currently (October 2021) the different draft proposals are discussed and negotiated in the triologue discussion between the EU institutions. Expected entry into force is most likely not before 2023.¹³

Germany

The draft law for the introduction of electronic securities (Electronic Securities Act, eWpG) was adopted by German Parliament on 6 May 2021 and entered into force on 10 June 2021. The law addresses key considerations from the

¹² The Howey Test, created by a Supreme Court judgment in a case of 1946 (SEC v. Howey), stipulates that an investment is a security if money or other assets are invested; the investment is expected to yield a profit; the investment is made into a common enterprise; and the profit is generated not by the efforts of the investor but by the efforts of a third party. It forms the basis of the “Framework for ‘Investment Contract’ Analysis of Digital Assets”, published by the Securities and Exchange Commission (SEC) to help market participants decide if a Crypto Asset is a security or not.

¹³ - DLT Pilot Regime: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0594&from=EN>
- DLT Pilot Regime presentation: https://ec.europa.eu/info/sites/default/files/business_economy_euro/banking_and_finance/200924-presentation-proposal-market-infrastructures-pilot-regime_en.pdf
- MiCA: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0593&from=EN>
- MiCA presentation: https://ec.europa.eu/info/sites/default/files/business_economy_euro/banking_and_finance/200924-presentation-proposal-Crypto-Assets-markets_en.pdf

Blockchain Strategy (published in 2019) by introducing a new category of “electronic securities” that are equivalent to traditional securities issued by means of a physical certificate. The requirement for a physical certificate is replaced by an entry in an electronic securities register. The new law classifies electronic securities as “moveables” within the meaning of the German Civil Code.

On 5 August 2021, The German Federal Ministry of Finance published its joint draft bill with the Federal Ministry of Justice and Consumer Protection for an ordinance on electronic securities registers (eWpRV).¹⁴

Switzerland

In Switzerland, an amendment to the Financial Market Infrastructure Act (FMIA), which is part of bill 19.074 to “adjust Swiss law to the developments in the area of distributed ledger technology” came into force on 1 August 2021, introducing the DLT Trading System as a new license category for the trading of security tokens. While this step indeed removes regulatory obstacles which have so far prevented establishing effective secondary markets for security tokens, it cannot be ignored that the requirements for operating a DLT Trading System will be similar to those of traditional exchanges.

Already on 1 February 2021 the first part of the DLT framework law came into force, introducing ledger-based securities; such securities are created by entry in a securities ledger and can only be exercised and transferred via this securities ledger. The securities ledger must satisfy the requirements mentioned and characterized in the Swiss Code of Obligations. The registration agreement creates the constitutive link between the right and the entry in the ledger. Ledger-based securities have the same functions as a physical order or bearer instrument (certificated securities), especially the functions of transparency, evidencing of title and protecting commercial transactions.¹⁵

There nevertheless remains considerable legal uncertainty at this stage as to the regulatory status of Crypto Assets in many jurisdictions, including in some cases within the same jurisdiction. In general, however, regulators tend to prefer a substance-over-form approach, in which a Crypto Asset which has the same characteristics as a regulated security is then regulated in the same way.¹⁶

¹⁴ - Law: Bundesgesetzblatt Teil I Nr. 29 (bundesfinanzministerium.de)
- Blockchain-Strategy: Federal Ministry of Finance - German government adopts blockchain strategy (bundesfinanzministerium.de), https://www.bundesfinanzministerium.de/Content/DE/Pressemitteilungen/Finanzpolitik/2019/09/2019-09-18-PM-Block-Anlage.pdf?__blob=publicationFile&v=3

¹⁵ Federal Council Press Releases:
- <https://www.admin.ch/gov/en/start/documentation/media-releases/media-releases-federal-council.msg-id-84035.html>
- <https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-81563.html>

¹⁶ European regulators, such as the European Banking Authority (EBA) and the European Securities and Markets Authority (ESMA), seem to apply a “substance over form” approach (i.e., if a Securities Token has the same characteristics as a financial instrument regulated under the Markets in Financial Instruments Directive (MiFID), it should receive the same regulatory treatment). International Financial Reporting Standards (IFRS) also require a “substance over form” approach.

11. Interoperability

The BIS defined interoperability in financial services as:

“The technical or legal compatibility that enables a system or mechanism to be used in conjunction with other systems or mechanisms. Interoperability allows participants in different systems to conduct, clear and settle payments or financial transactions across systems without participating in multiple systems.”

In the context of DLT, this would mean that such technical or legal compatibility would refer to different blockchain systems and protocols being able to communicate with one another without the need for an intermediary, permitting the sharing, accessing and transferring of value across different blockchain systems. It should be highlighted that such interoperability could and where possible, should also allow such compatibility with existing systems too.

So why is this important and where is the ISSA Working Group seeing a need for interoperability?

As the DLT environment gains momentum and the industry sees greater opportunities for adoption, there are some clear areas where interoperability is rapidly becoming a necessity in order to see wider take-up and therefore the realisation of such opportunities.

1. **Payment approaches for digital asset settlement.**
2. **DvD:** digital asset vs digital asset trading and settlement of across chains. This can be key in the repo or securities lending space.
3. **Open DLT networks:** digital products transacted across different non permissioned or public networks.
4. **Permissioned networks:** digital products transacted across governed networks with controlled access.
5. **Permissioned to open networks:** digital products transacted between permissioned and non-permissioned networks.
6. **Value-added services interacting with DLT networks:** e.g., digital asset wallet storage and its interaction to DLT network.
7. **Interoperability between new DLTs and legacy:**
 - a. Payments on existing rails vs digital asset platforms.
 - b. Payments on DLTs vs existing securities platforms.

So, it is clear that the concepts and approaches for DLT adoption have a heavy reliance on interoperability.

11.1 Interoperability Between DLT and Existing Networks is Making Progress

Effective governance of interoperability between DLT networks or tokenisation platforms, and between DLT networks or tokenisation platforms and legacy networks, is essential, because the different systems will co-exist for the foreseeable

future. Unless DLT networks or tokenisation platforms can interact successfully with existing services, there is a risk of fragmentation and loss of efficiency. Lack of interoperability is also one of the main reasons why DLT has yet to be widely adopted.

Interoperability between open or non-permissioned DLT networks or tokenisation platforms is feasible. This is still a work-in-progress, but there have been significant advances in recent months. One example is DAML 2.0 which allows the creation of business processes which are blockchain agnostic; for example, the processes built will run on either Corda or Hyperledger and do not need to be rewritten. DLT has a generic capacity to allow for the exchange of information between separate networks simultaneously. Interoperability between separate digital wallet providers is facilitated by the fact that all such systems use the same cryptographic techniques. Digital wallet providers have found they can support Crypto Assets running on almost any non-permissioned DLT network.

Permissioned DLT networks, whose membership is controlled, have made little progress in inter-operating with each other and even less in interoperating with their non-permissioned counterparts. Inter-operability between DLT networks or tokenisation platforms of both the permissioned and the non-permissioned variety and legacy infrastructures has made virtually no progress at all.

Although initiatives do exist – SWIFT, Liquidshare, ASX – achieving compatibility between DLT networks or tokenisation platforms and existing services remains a distant ambition. To the extent that this interoperability can be accomplished without adding complexity, multiplying risks, restricting access and undermining the value of innovative technology, it will enable issuers and investors to reap the benefits of Crypto Assets.

11.2 Interoperability Depends on Standards

The key to efficient interoperability is standards. The securities industry has long made use of standards to automate exchanges of information between the various parties involved in post-trade processing. Standards have cut costs and risks throughout the industry. But these benefits have been hard-won. Securities markets have spawned multiple proprietary formats, and it has many costly migrations and substantial re-engineering of processes to converge on common standards, and the industry is not even now fully aligned. The translation and transformation of the differing existing standards creates risk for the clients and the industry, as variations in payloads or syntax can create errors.

Something similar to the early days of the securities markets is visible in the Crypto Asset markets. There are competing protocols, such as Ethereum, EOS and Bancor. New standards are being developed for digital wallet services, such as “hierarchical deterministic wallets” (HD wallets), which can be shared across DLT systems.

This paper addresses “instrument” data standards in Section 3 above. However there are additional standards that need adoption within the crypto industry to allow efficient interoperability.

Crypto Assets are a computer program represented by and in smart contracts. These smart contracts can contain all the information of the asset they represent. This provides the potential to store immutable information about the instrument, which facilitates and gives confidence in due diligence to both investors and regulators. Although this represents a great advantage, it brings a challenge: standardizing the information it will contain, and the format in which it will be stored.

DLT networks and tokenisation platforms are publishing their own standards for tokens. There are several initiatives in train to create universal token standards, including the Token Taxonomy Initiative by Enterprise Ethereum Alliance, which aims to create a DLT-neutral token definition. Ripple is building an Interledger protocol designed to facilitate token transactions between separate DLT networks or tokenisation platforms. R3 has developed a system that allows applications built on its platform to interact seamlessly with other DLT systems.

In recent years, these efforts have resulted in a number of DLT tokens standards reaching widespread adoption throughout the DLT space, including:

Body	Objectives	Achievements
ISO/TC 307	Standardisation of blockchain technologies and Distributed Ledger Technologies.	Limited standards published around glossary and taxonomy. Nothing on interoperability.
W3C	Lead the World Wide Web to its full potential by developing protocols and guidelines that ensure the long-term growth of the Web.	DID Standard published, no specific DLT standards. Nothing on interoperability.
Token Taxonomy Standard	Define a common language, behaviours and properties for a token of value that can be used or exchanged.	Co-ordinated different industry groups to produce a shared taxonomy. Useful foundational standard for interoperability.
Ethereum Enterprise Alliance	Drive the use of Enterprise Ethereum and Mainnet Ethereum blockchain technology as an open standard.	Client specification published. Interoperability working group established, mainly focussed on Ethereum to Ethereum chains.
IEEE P3205	Standard for Blockchain Interoperability.	Unknown.
Interledger Protocol	An open and inclusive payments network that puts humanity first.	Abstracts payment for multiple chains. Limited to payments.

Figure 2: Standard-Setting Bodies, Objectives, Achievements to Date

However, the proprietary nature of many of these initiatives remains an obstacle to interoperability between DLT networks.

Although a number of different solutions have already proven the possibility of cross-DLT interoperability, what is lacking is a common framework based on common standards for the safe and resilient implementation of these solutions. As the European Central Bank noted in a recent paper on the use of DLT in post-trade processes, *“as industry participants are presently building their own DLT-based systems, there is a risk of incompatibility between the different systems, potentially leading to fragmentation. Standardised rules are needed and can be ensured by adopting pre-determined standards and common rules for smooth interactions.”*¹⁷

What should these standards aim to achieve? Current links between FMIs are designed primarily to ensure that each leg of a securities transaction is settled on a DvP basis. This key objective should be reflected in standards for DLT-based settlement infrastructure. It is therefore clear that in the specific context of DLT, the market requires a common set of technology-neutral and protocol-neutral operational standards that enables DvP settlement, along with clear expectations that the legal and governance arrangements underlying each DvP link ensure compliance with the global benchmark standards set by the PFMI.

To meet these objectives, a common set of standards should mandate that any link between two DLT-based settlement arrangements or a DLT system versus incumbent system apply the recommendations of interoperability. These are fully described in the earlier paper (page 53) and maintain their relevance. The most notable development in the intervening years has been the continued adoption of ISO 20022 and the opportunity for this to facilitate DLT interoperability.

It should also be recognised that interoperability is not just a requirement for Delivery versus Payment, but it can also be a requirement at execution level (the ability to trade the same product across multiple platforms – DLT or legacy) and at asset servicing level with certain activities being processed on different platforms such as proxy voting on DLT. The ability to interoperate in these areas also requires standards to ensure the best choice and capabilities for consumers.

The International Organisation of Standardisation (ISO) Technical Committee (TC307) has published a number of standards documents over the last three years, including the ones addressing privacy, taxonomy, smart contracts interaction with DLT and Security Management of Digital Asset custodians.

11.3 A Potential Role for ISO 20022

One way forward is to align Crypto Assets with ISO 20022, the standard that defines the development of financial messaging standards. Messaging standards describe formally the content of business messages exchanged by market participants to complete business processes, such as settling transactions or issuing corporate action notifications and instructions. They also describe the roles played by the different links in a transaction chain and the message flows required to complete a particular transaction.

¹⁷ The Use of DLT in post-trade processes, ECB Advisory Groups on Market Infrastructures for Securities and Collateral and for Payments

Messaging standards draw on reference data standards whenever possible, to minimise ambiguity in a financial message. Reference data standards define universal codes for all the common data elements in a financial message, such as the currency (using shorthand codes such as EUR and USD), the securities (using International Securities Identification Numbers, or ISINs) and the counterparties (using Bank Identification Codes (BICs) or Legal Entity Identifiers (LEIs)). There is no reason why the same reference data standards cannot be used by operators of DLT networks or tokenisation platforms.

The principal value of a DLT network or tokenisation platform lies in the fact that the same data is shared automatically with all parties to the transaction. Financial messages, by contrast, are passed from point-to-point and reconciled by each link in the transaction chain. Like reconciliation, point-to-point financial messages are redundant in DLT-based markets, such as those in Crypto Asset Tokens.

However, the semantics – the meaning of the business terms – that underpin existing financial messages can be re-used for DLT networks or tokenisation platforms. The business layer of the ISO 20022 standards is designed to fit the business process rather than the technology on which it is implemented, so it is in principle adaptable to DLT networks or tokenisation platforms.

In other words, the business layer of the ISO 20022 standard can be used to guide definitions of DLT-based products and services such as smart contracts. ISO 20022-compatible application programming interfaces (APIs) could also be used to facilitate communication between different DLT networks or tokenisation platforms.

However, much of the content required for financial business transactions already exists in a standardised way, so there is no need to reinvent the wheel. Existing business standards describe financial data and how to interact with it to execute the business of finance. Specifically, reference data standards define identifiers for common data items like currencies, countries, assets and market participants. Semantic standards define common business concepts and the relationships between them, providing a common vocabulary and data model for business information. Transactional standards define the steps required to complete a transaction – who is responsible at each step, what data is exchanged, etc.

ISO 20022¹⁸ already includes semantic and transactional definitions covering business processes as diverse as retail and wholesale payments, foreign exchange, securities lending, repo transactions, collateral management, securities settlement, asset reconciliation, trade finance, cards transactions, regulatory reporting and more.

ISO 20022 was conceived to harmonise the fragmented financial messaging standards landscape, but inherent to its design is an architecture that also makes it a future-proofed standardisation methodology for blockchain transactions and APIs. There are two key aspects to ISO 20022. It is a methodology: a “recipe” to be followed to standardise financial transactions. And it is a machine-processible repository of content: the definitions of messages, business concepts, processes and

¹⁸ www.iso20022.org

everything else required to describe those transactions. ISO 20022 is an open, global standard. It is not controlled by a single interest and is open to anyone in the industry who wants to participate. It is platform and technology agnostic and free for anyone to implement in any business or software environment or on any network.

12. Conclusion

Since the last edition of this paper in 2019, the DLT landscape has continued to evolve. We have seen the whole industry, both incumbents and new entrants, increase their adoption of the technology and the products that utilise it. There have been an increasing number of high profile projects whether live or in test phases that have borne out the benefits that such products can bring to the market in terms of efficiency and transparency (see The Value Exchange and ISSA 2021 survey on DLT adoption). It is clear that Crypto Assets in their many forms are here to stay. However, the industry is still not at a point where it can realise the full benefits of this new market. It is clear that the following are needed to really allow the market to expand:

- A concerted industry wide effort to finalise taxonomy across the Crypto Asset space. This work has begun but as this paper has demonstrated, there are many different players working to an extent in isolation developing different taxonomies and standards. It is critical that the industry identify who is working on what and bring their efforts together to consolidate an approach. This will in turn aid regulators in determining the best way to regulate the space in a harmonised way that is critical for a cross border global market.
- Increased education on the different elements of DLT, its uses, its benefits and its risks. Papers such as this need to be circulated across the industry including the policy maker and regulatory community to aid them in understanding the landscape. Furthermore, it is vital that those who are adopting and experimenting with DLT should look to share learnings as this will aid in broader adoption across the industry. This will all help in developing a coherent and efficient marketplace rather than replicating fragmented and siloed markets that currently exist in the traditional space.
- A greater focus on developing open interoperability standards within the Crypto Asset marketplace to allow different types of DLT platforms to interact and to support the different aspects of the issuance, trading, clearing and settlement lifecycle. Only by doing this will an efficient playing field emerge that will allow greater access for all players.
- A greater focus on developing interoperability standards between the Crypto Asset marketplace and traditional markets. In order for financial institutions to develop and grow the new marketplace, it is critical to determine exactly how the marketplace will interact with traditional finance. Both markets will co-exist into the foreseeable future, so without that interaction, the overall financial marketplace will become more fragmented and inefficient, not less. This will have a negative knock on effect for all players within it as regards costs, revenues and profits.

- Greater support for the regulators who are trying to create the right regulatory environment for the new marketplace. The industry has an opportunity to further educate and help regulators in drafting and implementing legislation to cover this market. The quicker regulators can introduce a globally coherent regulatory environment that has the capability to pivot as the market continues to evolve, the sooner institutional financial players can access and grow the marketplace, creating the necessary post trade products to support clients.

Crypto Assets issued on DLT networks or tokenisation platforms will not leave the present order in post-trade securities services unchanged. Securities Tokens and Payment Tokens have the potential to make a number of existing services more efficient, extend the range of asset classes that are investable and liquid and widen the number and type of providers that are engaged in servicing issuers and investors. They also promise to introduce entirely new products and services and unprecedented ways for service providers and their clients – and issuers and investors – to interact as members of networks.

The settlement and safekeeping services that currently support the securities industry will have to evolve and adapt to manage the threats and seize the opportunities that Crypto Assets represent. New roles, of which network governance and / or operation is the most obvious, will emerge and develop. New ways of completing old tasks, such as smart contracts, will be adopted. But the essential responsibilities of the custodian banks and CSDs that provide safekeeping and settlement services will remain unchanged: the protection of investors and the preservation of the integrity of the capital markets.

The form may change, but the substance will remain the same, is also the attitude adopted by policymakers and regulators. They are encouraged by the possibilities of innovation – increased market size, greater liquidity and lower transaction costs – and seek to foster it. But they will need to adjust laws and regulations to continue to protect investors and preserve the integrity of markets. If a Securities Token exhibits the characteristics of a security, it will be regulated in a manner equivalent to a security. If a Payment Token has the characteristics of cash, it will be regulated in the same way as cash.

Custodian banks and CSDs are well-advised to monitor both national and international policymaking and regulatory bodies for material changes to the legal and regulatory status of Crypto Assets. For now, however, substance-over-form provides sufficient legal and regulatory certainty for issuers, investors and service providers to continue to experiment with Crypto Assets, albeit within the confines of individual jurisdictions. Legal and regulatory differences between countries make it too difficult to internationalise Crypto Asset issuance and investing yet, although awareness and collaboration can help to evolve global standards over time.

The technology behind DLT networks and tokenisation platforms is at an early stage but maturing, and custodian banks and CSDs are proceeding – understandably – with caution anyway. Several operational issues remain unresolved. On-ledger settlement is not yet superior to simultaneous delivery versus payment (DvP) in the securities markets. Safe custody of private keys and financial assets that back “non-native” Securities Tokens both need technical, legal and regulatory

refinement. The standards that will enable DLT networks to interoperate with each other, and with legacy systems, are not yet developed.

The best way to overcome these challenges is to collaborate. Every participant in the Crypto Asset industry – issuers, investors, regulators, CSDs, custodian banks, CCPs, FMIs, vendors and FinTechs – will benefit from collaboration. By working together, agreement can be reached on the definitions of Crypto Assets, the legal and regulatory frameworks which govern them, and the business and technical standards that will allow all the ecosystems to interoperate. It is the measure of agreement on those issues that will determine the rate of growth of the Crypto Asset markets.

Appendix: Working Group Members

The following individuals have contributed significantly to authoring the final report:

Working Group Members acting as Authors	Organisation
Vic Arulchandran	Nivaura Ltd
Urs Sauer	SIX
Claudio Calderon	DCV Chile
Jack Cameron	Brown Brothers Harriman
Giles Elliott	TATA Consultancy Services Limited
Angus Fletcher	Finality International
Francesca Frigerio	UBS
Alexia Kazakou	Citibank
Katrin Koller	Accenture
Robin Leary	Citibank
John Andrew O'Brien	Citi Europe Plc
Jennifer O'Rourke	DTCC
Colin Parry	International Securities Services Association
Ioulia Petti	Clearstream
Sandra Ro	Global Blockchain Business Council
Ian Salmon	R3
Angela Walker	R3