Infrastructure for Crypto-Assets:

A Review by Infrastructure Providers

October 2018

Abstract
The purpose of this document is to raise awareness of the fact that the provision of services to participants in the crypto-asset markets – and not just the adoption of distributed ledger technology by market infrastructures to enhance their existing services - should be seen as a target market by major participants in the securities services industry.

The document does not focus on legal or regulatory issues raised by the emergence, growth and development of the crypto-asset markets. Regulation of crypto-assets is a major topic in the industry today. Many conclusions in this document are based on the current thinking of regulators and discernible trends in their treatment of crypto-assets. However, a detailed overview of the current legal and regulatory status of crypto-assets around the world as a whole, or even in specific jurisdictions, is outside the scope of this document.

Nor does this document focus on pre-trade and trade issues. Pre-trade and trade issues in the crypto-asset markets have received considerable attention already. While they will undoubtedly change and evolve further, it is ISSA's view that post-trade infrastructure must catch up with developments in pre-trade and trade before mass market adoption of crypto-assets can truly occur. It is the goal of this document to explore that particular problem. ISSA hopes that it will make a contribution towards the growth of the market in general and to the emergence of a safer and more efficient post-trade environment for the crypto-asset trading and investing, based on existing business and technical standards to the benefit of the whole industry and the investors.

Target Audience
The intended audience of this report includes custodian banks and payments market infrastructures (PMIs) as well as central securities depositories (CSDs) and central counterparty clearing houses (CCPs).

Acknowledgements
This report is the result of efforts by a team of experts drawn from ISSA Operating Committee members and other ISSA participating member firms. All participants supplied valuable market information. The names of participating firms are listed in Appendix 4. The ISSA Executive Board wishes to thank all supporters for their contributions as well as their firms having enabled their participation.

Disclaimer
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 listed in Appendix 4 of this report warrant the accuracy or completeness of the information or analysis contained in this report.

International Securities Services Association ISSA
c/o UBS Switzerland AG
EUR1 – EG2230, P.O. Box
CH-8098 Zurich, Switzerland
Contact +41 (0)44 239 91 94
issa@issanet.org

Table of Contents

0. Introduction

0.1 Preamble

Crypto-assets seem to be on a trajectory to establish themselves as a new asset class. Though they are the subject of a great deal of hype, speculation and price volatility, an interesting momentum is developing behind Initial Coin Offerings (ICOs) and utility, asset and asset-backed tokens, as a potential method of financing start-ups and small and medium-sized enterprises.

The challenge crypto-assets issue to established financial market infrastructures is this: How can we create a safe and efficient environment for investors in this emerging asset class? Since crypto-assets have a number of features in common with traditional financial assets - their novelty lies in the distributed nature of the blockchain-based networks they use rather than their investment characteristics – they are naturally of interest to central securities depositories (CSDs).

As a critical component of the networks of the financial market infrastructures that currently underpin the securities markets, CSDs have a clear responsibility to investigate the crypto-asset phenomenon and see where they might be able to help the market develop a safe and efficient environment for issuers and investors. The purpose of this paper is to contribute to the present debate and broaden the dialogue on crypto-assets to include post-trade interests.

Today, securities markets are organized and structured to mitigate the risks inherent to any financial market. Measures and institutions, including stock exchanges, central counterparty clearing houses (CCPs) and trade repositories (TRs) as well as CSDs, have evolved to reduce the risks associated with the issuers, the instruments and the intermediaries in securities markets and to ensure that transactions settle expeditiously and assets are held and serviced securely.

CSDs in particular guarantee the integrity of issues of securities and the elimination of risk in settlement through delivery against payment (DvP). They increase automation of post-trade processing through standard procedures, interfaces and messaging and provide regulators and investors with a reassuring degree of robustness and resilience. They also operate within a framework of laws and regulations which, between them, provide a trusted environment for investors.

In the crypto-asset markets, investors are looking for a comparably safe and trustworthy environment. It is likely that infrastructural components, not unlike the financial market infrastructures that service the securities markets of today, will be put in place over time. The emergence of crypto-asset exchanges and digital wallet providers indicates that this process is already under way. But this is just the start of a long journey.

Regulators are understandably concerned about the risks posed by crypto-assets and have yet to settle on the appropriate regulatory treatment. But the ready availability of infrastructural solutions may ease some of their concerns about investor protection, money laundering, financial instability and market integrity. The presence of infrastructural solutions could well become a condition of crypto-assets achieving regulatory acceptance.

Some of those solutions fall within the natural remit of existing market infrastructures. Many of the representatives in the market infrastructure space are running use-case studies to better understand whether, where, and how they could add value by making use of distributed ledger technologies (see Appendix 2). While market infrastructure roles and pieces of infrastructure in support of crypto-assets are likely to be different from those in today's securities markets, ultimately they will seek the same objective, i.e. creating a safe and efficient environment for companies to issue, investors to invest, marketplaces to provide facilities for trading and financial intermediaries to service these assets for their customers.

ISSA recognizes that the necessary solutions are not in place yet and that CSDs and the crypto-asset industry still have an interesting journey ahead of them, but ISSA welcomes the opportunity to play a part in shaping the probable future of this new asset class. It is ISSA's ambition to be an engaged interlocutor with regulators and policymakers and to collaborate with the crypto-asset and distributed ledger technology communities to develop resilient and robust solutions that can help the crypto-asset markets evolve and mature more quickly.

0.2 Executive Summary

The number of crypto-assets issued and traded now exceeds 1,800, with a total market capitalization of more than $200 billion. Crypto-assets vary but the four broad categories are those used to make payments ("crypto-currencies"), access applications or services ("utility tokens"), represent claims on assets or income streams ("asset tokens") or own an asset ("asset-backed tokens").

Crypto-assets are supported by a complex eco-system of exchanges, market-makers, digital "wallet" providers, crypto-asset registrars, smart contract verification services and a variety of consulting, legal and technological advisers which between them manage the issuance, trading, settlement, custody and servicing of the asset class.

The investors in crypto-assets are mostly confined to retail and other investors with a strong appetite for speculative risk. The issuance, trading, settlement and custody of crypto-assets is not surrounded by any agreed framework of regulation and law, and there is variation between jurisdictions on regulatory attitudes towards crypto-assets.

There is rarely any separation of duties. In most cases, the rules governing the distributed network on which the crypto-assets are issued and traded are set and implemented by the operator of the network. Crypto-asset exchanges, digital "wallets" and smart contracts have also proved vulnerable to cyber-attack, leading to misappropriation of assets.

Not all crypto-assets depend on blockchain or distributed ledger technology (DLT), but most do. This is because DLT offers the advantages of direct issuance into accounts on a single distributed ledger, direct settlement of transactions between accounts, simultaneous verification of transactions and registration of ownership and direct and automated payment of entitlements to accounts.

In the securities markets of today, these functions – issuance, settlement, registration, safekeeping and asset servicing – are performed by a range of centralized intermediaries, including central banks, banks, brokers, stock exchanges, CCPs, central CSDs, real-time gross settlement systems (RTGSs) and custodian banks.

This complex eco-system of market infrastructures and their users exists to provide a safe and efficient environment for issuers and investors active in the securities markets. It provides the necessary scale to allow for large increases in volumes and lowers the cost of transactions. But the members of the eco-system also operate within a framework of regulation and law which reinforces the trust of market participants.

Paradoxically, for an asset class which relies for the most part on a blockchain technology designed specifically to dispense with the need for trusted intermediaries, lack of trust in the integrity, safety and efficiency of the crypto-asset markets is a major obstacle to investment in them by institutional investors. High levels of price volatility reinforce this lack of trust.

Increasing the trustworthiness, safety and efficiency of crypto-asset markets is essential if they are to continue to grow and especially to attract institutional investors. Market infrastructures and their users are well-placed to foster favorable conditions because they have accumulated expertise in the securities markets in the mitigation and management of the obstacles to institutional investment.

Moving from a centralized to a decentralized market structure changes the form of the risks investors incur, but not their substance. Assets still have to be issued, transactions in them settled, tokens safe-kept and serviced, issuers and investors vetted and rules of behavior for all members of the distributed network devised, implemented and monitored for breaches.

Market infrastructures, one of whose responsibilities is to ensure that the number of securities in issue matches the number held by investors, could play a role to ensure that the number of tokens in issue and the number held by investors are perfectly aligned. This might be one of several market infrastructure roles in issuance, including the vetting of issuers, investors and crypto-asset exchanges.

Another core role of market infrastructures is the settlement of transactions by delivery against payment (DvP). At present, investors buying or selling tokens for fiat currency must pre-fund accounts and complete the cash leg off the ledger. Pending the development of central bank digital currencies (CBDCs), market infrastructures can reduce the costs by netting offsetting trades.

DvP settlement of transactions through market infrastructures is also how the securities markets achieve the irrevocable, simultaneous, final settlement that guarantees perfect legal title to cash or securities in multiple jurisdictions. Infrastructural services are not a substitute for legal certainty, but market infrastructures can already help create certainty around the ultimate transfer of ownership of the crypto assets by administering operational rules and contractual agreements that ensure effectual settlement finality.

In the securities markets, infrastructures increase the efficiency of their interactions with users via standardized interfaces and messages. Since distributed networks must co-exist with centralized infrastructures, necessitating reconciliations of data between them and creating legal and contagion risk, it makes sense to apply agreed rules to all interactions and maximize use of existing business and technical standards.

In theory, crypto-assets are held securely in digital "wallets". In practice, the private keys that are the sole guarantor of ownership are vulnerable to catastrophic loss. Market infrastructures and custodian banks can reduce the risk of loss by monitoring ledger-based registers of ownership, operating an independent register and providing physical custody services for private keys.

Cyber-attacks are a major threat, which centralized infrastructures mitigate with back-up facilities and recovery mechanisms. Although distributed ledgers avoid a single point of failure, exploiting of crypto-asset exchanges and smart contracts has occurred, and manipulation of data is possible. In a permissioned DLT environment, market infrastructures can vet and monitor members of a network, control access to data and certify the security of software.

Another security challenge distributed networks face is regulatory pressure to ensure crypto-assets comply with KYC, AML and sanctions screening obligations. The cost of duplication is significant, and the complexity of the rules means the risk of compliance failure is high. Market infrastructures could mutualize the cost of compliance and reduce the risk for the industry as a whole.

A final compliance risk is taxation. The novelty of crypto-assets has led to uncertainty and variation between jurisdictions over the taxation of transactions, capital gains and income derived from tokens. This deters potential investors. Market infrastructures, in collaboration with custodian banks, can help to solve this problem by preparing reports for tax advisers to investors.

These findings suggest that, while the distributed nature of the networks on which crypto-assets are issued and traded is rich in potential to create new forms of financing and ownership, it does require robust market infrastructure type roles and pieces of infrastructure to bring safety and efficiency to this market. In particular, distributed networks create a need for new forms of governance as well as operation.

Governance of a network needs to be separated from its operation. Deciding who is admitted to a network, who has access to which information on the network and how the activity of the network is policed, requires independent governance. Delivering it and the accompanying operational services, requires market infrastructures to adapt rather than metamorphose.

The services which market infrastructures and custodian banks can offer to distributed networks are confined to "permissioned" rather than public networks. They will also evolve in line with the development of laws and regulations governing the sector and the eventual availability of central bank digital currencies (CBDCs), but it is clear that these services can already help the crypto-asset markets to grow more quickly.

1. The Growth and Development of Crypto-Assets

1.1 The Size of the Crypto-Asset Markets

The range of crypto-assets available to buy and sell has expanded enormously in the last two years. Since the advent of Bitcoin in 2009[1], but especially since the beginning of 2017, the number of crypto-assets has grown rapidly. Exchanges have also emerged on which these assets can be traded. One widely followed web site now tracks 1,855 crypto-assets with a total market capitalization of $214 billion (see Chart 1, page 12) and monitors trading volumes on 214 exchanges[2].

An intricate eco-system is now in existence[3], in which a variety of financial assets, available in purely digital form and without any physical manifestation, are issued, bought, sold and serviced. Being financial assets, they are also issued by companies and traded and owned by investors, and they have a definable monetary value. They can be cancelled or terminated by the issuer too, in the manner of bond redemption or share buy-back. So they have features in common with securities, but also important differences.

The most common type of crypto financial asset is the crypto-currency, which aims to compete with fiat currencies as a means of payment. The best-known is Bitcoin. But other types of digital asset entitle the holder to an income stream, or to access a service, or confer part-ownership of an underlying asset. A useful term for all varieties of digital financial asset is "token", since they are all exchangeable for something, but they are not always backed by an issuer or property.

1.2 The Different Types of Crypto-Assets

Tokens are often lumped together as "crypto-currencies", but this is not correct. Only payment tokens, such as Bitcoin, are true crypto-currencies. They aim over time to compete with, or even replace, fiat currencies as a means of payment. Crypto-currencies differ from "utility tokens", which act as the currency in a network where investors can invest in digital applications coded by a member of the network and consumers can purchase a service provided by a member of the network. Using Ether tokens to invest in digital applications built on the Ethereum network is the best-known example.

"Asset tokens", on the other hand, represent claims on assets or income streams from assets, which can be on or off the network of investors. Holders of Lykke coins, for example, are invested in a company that aims to provide a trading platform for any asset – real estate, private equity, rental income, intellectual property rights, even freelance labor time - that can be digitized and traded against cash, a crypto-currency or another digital asset. An asset-backed token is easier to understand: It is, as the name suggests, a token which offers exclusive or joint or common ownership of an underlying asset such as gemstones or real estate.

Variations in the nature of the property rights inherent in a token alter the risks of investing in a crypto-asset in a way not wholly dissimilar to the risks of investing in a security. Just as the risks of investing in an equity are higher than the risks of investing in a bond, the risks of investing in one token are different from the risks of investing in

[1] Satoshi Nakamoto published the Bitcoin specification and proof of concept on 31 October 2008: *A Peer-to-Peer Electronic Cash System*, 31 October 2008

[2] https://coinmarketcap.com/

[3] See Chapter 1.6. for a detailed description of the crypto-asset eco-system.

another[4]. Table 1 below lists the four basic types of token – payment, utility, asset and asset-backed – and gives examples of tokens in issue.

Table 1: Types of Token in Issue

Type of Token	Characteristics	Examples
Payment	Synonymous with crypto-currencies that aim to compete with fiat currencies as a means of payment and have no intrinsic value, asset backing or links to other projects.	Bitcoin, Ethereum, Litecoin
Utility	Intended to provide digital access to an application or service.	Binance, Golem
Asset	Analogous to securities in that they represent entitlement to physical assets, companies, earnings streams, dividends or interest payments. They are sometimes treated as securities or debt obligations.	Modum, Daura C-shares, Lykke
Asset-backed	Provide absolute rights of ownership ("in rem") of an underlying asset, such as fine art, real estate, equity, fixed income, gold, or intellectual property.	Venezuelan Petro, Hello Gold, D1

In the end, a taxonomy as simple as that of Table 1 above cannot do justice to the sheer variety of token-based projects that are launched or being launched or soon-to-be launched. Accordingly, throughout this paper, all kinds of tokens are referred to somewhat inaccurately but collectively and conveniently, as "crypto-assets".

1.3 What is Unique About Crypto-Assets

However, while they vary considerably in detail, what they tend to have in common is a reliance on blockchain or distributed ledger technology. While it would be inaccurate to claim that all crypto-assets depend on blockchain technology, it is safe to say that the technology is well-suited to the issuance of crypto-assets. Its advantages include a distributed network of users, a single but distributed ledger to register assets and the ability to record and validate all transactions in those assets in chronological order in the same ledger.

Law and regulation have yet to catch up with the possibilities, but this combination in principle enables issuers to create exclusive – if not yet legally sound - property rights in

[4] Swiss law firm MME Legal, in *Conceptual Framework for Legal and Risk Assessment of Crypto Tokens: Classification of Decentralized Blockchain-based Assets*, 1 May 2018, classifies tokens by their so-called Blockchain Crypto Property, to distinguish between tokens that are backed by no legal counterparty against which a claim can be made (BCP Class 1), those backed by an individual or legal entity against which a claim can be made (BCP Class 2) and those which confer outright property rights in an asset. The BCP classification is an indication of the nature and extent of the rights conferred on investors by the various types of token. This is a measure of the legal risk assumed by investors in tokens, and by any entity claiming to act on their behalf. https://www.mme.ch/de/magazin/bcp_framework_for_assessment_of_crypto_tokens/

crypto-assets quickly and conveniently. Importantly, those rights can be created even in underlying assets that are intrinsically difficult to trade or sub-divide, such as real estate, precious metals or fine art.

By registering those property rights in a single distributed ledger and updating the ledger automatically every time the property rights are bought and sold, blockchain technologies also make it possible for members of the network to exchange the rights efficiently, peer-to-peer, between accounts on the network. In other words, unlike the modern securities markets, blockchains manage counterparty risk without going through a trusted and centralized third party.

Blockchains also facilitate the use of smart contracts, which automate the execution of contractual obligations – including the distribution and collection of entitlements, such as dividend payments – through software code operating to an "if-this-then-that" logic.

1.4 The Disruptive Potential of Crypto-Assets for Established Market Infrastructures

The potentially revolutionary implications of this combination – crypto-assets issued, traded, cleared, settled and safe-kept on a blockchain - for established financial markets, the instruments that are traded on them and the institutions that trade, settle, safekeep and service them, are obvious.

An extended infrastructural order of stock exchanges, central counter-party clearing houses (CCPs), central securities depositories (CSDs), automated clearing houses (ACHs) and real time gross settlement systems (RTGSs), plus networks of brokers and custodian banks to interact with them, exists today to do the same work in the securities markets: Issue, trade, clear, settle, safekeep and service financial assets.

In addition, far from being distributed, the financial markets of today are highly centralized. Central banks issue fiat currencies, which central governments underwrite. Domestic payments in fiat currencies are ultimately settled through centralized RTGSs operated or supervised by central banks. Cross-currency payments are settled via CLS, a centrally organized industry consortium. In the securities markets, trades are agreed on centralized stock exchanges or trading venues, confirmed via centralized matching engines, cleared through centralized CCPs and settled by delivery against payment in central or commercial bank money in centralized CSDs using existing business and technical ISO Standards such as ISO 15022 and ISO 20022.

In theory, a marketplace based on a single but distributed ledger powered by blockchain technology, has no need for this complicated set of inter-locking financial market infrastructures and institutions. This is one reason why central banks, RTGSs, CLS, stock exchanges, CCPs and CSDs are exploring the application of blockchain technologies to the roles they currently play, to explore whether a decentralized model can help them provide better/more efficient and new services at lower cost (see Appendix 2). But the challenge issued to existing market infrastructures reaches beyond the application of distributed ledger technology to existing services. Crypto-assets, like securities, have to be serviced. Transactions in crypto-assets have to be settled, purchases of crypto-assets safe-kept and entitlements collected.

In addressing the opportunity this represents, it is important to remember that current market infrastructures were not merely an expression of the technologies that existed when they were established. They were founded and continue to exist because they clear a major obstacle to growth in the volume of financial transactions, both domestically and across borders: They create a safe and efficient environment that instils trust.

Trust increases transactional activity and reduces transaction costs. If a seller cannot trust a buyer to deliver the cash and a buyer cannot trust a seller to deliver the goods or services or securities, and either or both do not trust the environment in which they

trade, less business will be done at much higher cost because each counterparty will have to do their own due diligence on the other and on the wider trading environment.

A crucial lesson for the crypto-asset markets is that this trust is not wholly dependent on the market infrastructures and the technologies they deploy. Much also depends on the surrounding corpus of law and regulation. Blockchain technologies have so far developed outside the formalities of both law and regulation. Indeed, a large part of the attraction of blockchain technologies to the early enthusiasts was its promise to dispense with the need for trusted intermediaries operating within an agreed framework of law and regulation.

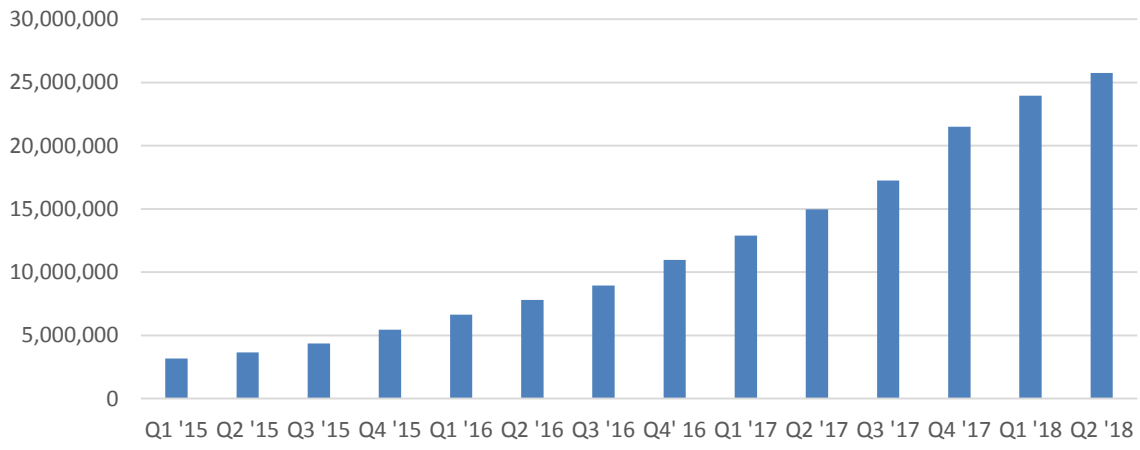
Instead, transactions are verified by participants in the network. They occur peer-to-peer, between payer and payee. In theory, this means they have no need for a middleman to check that counterparties are creditworthy, ensure that both parties are agreed on the terms of transactions, verify that sellers have securities and buyers have cash, deliver the securities against the cash simultaneously and solve the problems that arise when something goes wrong.

In theory, a blockchain of the classic variety obviates the need for any centralized intermediary or governing authority to police and facilitate transactions, by providing an immutable, digital audit trail of transactions that all members of the network agree is true. In short, evangelists for the classic version of blockchain argue that it eliminates the need for trust. As Satoshi Nakamoto put it in his original paper outlining how Bitcoin would work, "the main benefits are lost if a trusted third party is still required"[5].

1.5 Obstacles to the Further Growth of the Crypto-Asset Markets

Bitcoin and other crypto-assets issued onto public blockchain networks do rely on participants approving transactions in this "trustless" way. It works, in the sense that nearly 1,900 crypto-assets are now in issue and more than 25 million "wallet users" are invested in them (see Chart 1). Yet one recent survey found that two of the biggest obstacles to adoption of blockchain technologies, especially in interactions with third parties, are regulatory uncertainty and lack of trust among users[6].

Chart 1: Number of Blockchain Wallet Users



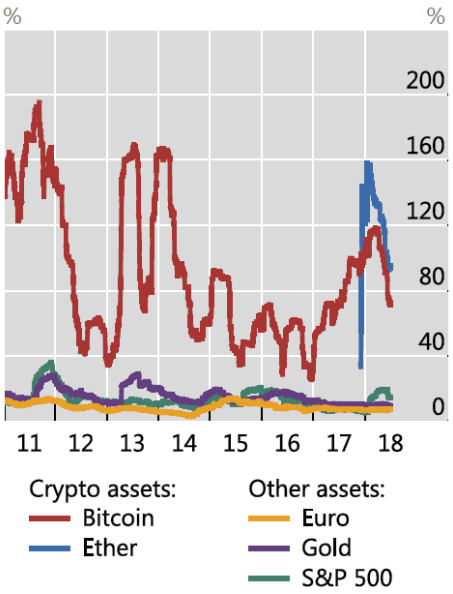
Source: Statista

[5] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 31 October 2008.

[6] PwC, *Blockchain is here. What's your next move?* PwC's Global Blockchain Survey 2018. https://www.pwc.com/gx/en/issues/blockchain/blockchain-in-business.html

This is a curious finding for a technology that was invented precisely to address the problem of trust. But it is not surprising. Hackers have stolen assets from crypto-asset exchanges and exploited vulnerabilities in the code of smart contracts. A number of initial coin offerings (ICOs) have proved fraudulent. It is understandable that, outside the ranks of the early adopters, potential users are concerned about the security as well as the reliability, speed and scalability of the blockchain technologies on which most crypto-assets depend.

Chart 2: Price Volatility



Source: Financial Stability Board, *Crypto-assets: Report to the G20 on work by the FSB and standard-setting bodies*, 16 July 2018. http://www.fsb.org/2018/07/fsb-report-sets-out-framework-to-monitor-crypto-asset-markets/

The market value of crypto-assets has also exhibited far greater price volatility than orthodox asset classes such as equities and gold (see Chart 2). The total market value of crypto-assets peaked in early 2018 at nearly $800 billion, but their value has since declined to a quarter of this amount (see Chart 3). This volatility primarily reflects a lack of trust in crypto-asset trading mechanisms and the risk of misappropriation, evident in the relatively small proportion of crypto-assets that are available for purchase and sale, as opposed to being held in digital wallets. This causes large price movements when an order to buy or sell is received.

Chart 3: Total Market Capitalization

Source: coinmarketcap.com

That lack of trust reflects the absence of an agreed legal and regulatory framework as well as a lack of market infrastructures to guarantee the safety of transactions and assets. This in turn deters institutional investors, reducing the flow of buy and sell orders that could dampen the price volatility of the crypto-asset markets. It also allows the few reliable trading, settlement and safekeeping services that support the crypto-asset markets to charge high prices, further inhibiting liquidity.

1.6 The Current Structure of the Crypto-Asset Markets

So it is not surprising that investment in crypto-assets is so far largely confined to private individuals, family offices and hedge fund managers comfortable with high levels of risk. The services they receive as investors are restricted to purchasing crypto-assets for cash through crypto-asset exchanges (such as Coinbase) and storing them in digital "wallets" supplied either by the issuer of the crypto-asset or a crypto-asset technology provider or a trading platform or an independent third party, which promise to store securely the private keys that govern their ownership of the token. The investors generally rely on the issuer to pay any entitlements due on the crypto-asset.

When it comes to trading crypto-assets, either in exchange for other crypto-assets or for fiat currency, investors or their intermediaries have to open an account at a crypto-asset exchange, which runs its own Know Your Client (KYC) due diligence process, which is not always adequate to detect counterparty risk or bad actors. Some of these exchanges also operate as market-makers to provide liquidity to buyers and sellers of crypto-assets, but market-making is not yet well developed in these new asset classes. An alternative to crypto exchanges exists in the OTC market, which has even fewer compliance controls and investor protection, but avoids third party risk raised by storing assets at the exchange.

Issuers are working with equally immature support services. They write their own prospectus, without clear direction from company law or regulation, but with input from lawyers, tax advisers and any one of a number of advisers on issues as various as blockchain technology, token structures, geo-blocking regulation, roadshows and public and press relations. Some issuers are hosted by incubators or accelerators which aim to turn ideas into viable products for sale.

Many issuers use their own developers or work with freelance developers. Issuers that use industry standard blockchain technologies (such as Ethereum) get the benefit of additional services for their investors, such as digital wallets and conversion into fiat currency. They can also join user groups to influence the development of the technology.

A number of crypto-asset registration services (such as CoinDaddy) have also emerged for issuers to register the name of their crypto-assets. Smart contract verification services certify smart contracts.

Chart 4: ICO Ecosystem

Source: Analysis of the ISSA Working Group

This complex eco-system of issuers, investors, trading platforms, governance mechanisms and service providers has evolved spontaneously in response to the day-to-day challenges of developing the markets in crypto-assets. As a result, it exhibits some conspicuous risks.

Issuers are not obliged to comply with disclosure requirements set by company law, such as those imposed on issuers of securities by the Transparency Directive of the European Union (EU). There is no separation between the entity responsible for establishing and monitoring the rules by which the network on which the crypto-assets are issued and traded are run and the operation of the network itself. In most cases, the roles of network governor and network operator are fulfilled by the same entity. This creates a conflict of interest.

Crypto-exchanges also assume counterparty and liquidity risks, but are not well-capitalized, or backed by defined resolution mechanisms. Several exchanges have been hacked and crypto-assets stolen. Digital wallets offer inadequate protection for the private keys which are the sole means of ensuring ownership of a crypto-asset.

Clearly, crypto-assets are on an evolutionary path. It is one that the securities markets trod before them, and which led to the development of a variety of services provided by an eco-system of financial market infrastructures and custodian banks to mitigate and manage the obstacles to widespread investment in equities and bonds.

2. Creating a Safe and Efficient Environment for Investing in Crypto-Assets

2.1 Crypto-Assets are on the same Evolutionary Path that Securities Followed

Crypto-assets have developed outside the formal, regulated structures of developed financial markets. This is not unusual for new financial instruments. Equities were purchased by investors long before commercial law authorized the joint stock company. Eurobonds emerged to exploit the pool of stateless US dollars in Europe in the 1960s. In both cases, the earliest investors were not institutions such as pension funds or insurance companies, but retail investors. The same is true of crypto-assets.

The infrastructure necessary to facilitate the growth of a market in a new asset class tends to follow the initial success, rather than lead it. Eurobonds, which also developed outside formal regulation, are a case in point. Euroclear (established in 1968) and Clearstream (1970) were founded to solve the risks associated with the physical delivery of bearer bonds and especially the long delays in settlement, which created intolerable counterparty and market risks. The Eurobond market grew much more quickly in the 1970s and 1980s as a result, because the reduced risk attracted institutional investors.

So it is not surprising to find a vibrant market in crypto-assets has developed outside regulated financial markets and without the support of either an agreed legal regime or a market infrastructure to reduce the risks and costs of transactions. But it will be surprising if the crypto-asset market is able to continue to grow without developing a more sophisticated infrastructural underpinning. After all, financial market infrastructures exist in large part to underwrite investor confidence in any asset class by mitigating risk[7].

All the risks investors in crypto-assets face today are recognizable. Even though they arise in distributed networks of participants, rather than centralized marketplaces where participants meet to trade, the risks are in fact broadly the same as those which investors have experienced in other asset classes, including equities and bonds. They are different in form, but not in substance.

Like investors in securities, crypto-asset investors incur settlement, safekeeping and liquidity risks. Even those aspects which seem most unfamiliar (such as the use of private keys as the guarantor of ownership) are intelligible as risks comparable to those found in securities markets. It follows that, in mitigating them, existing financial market infrastructures and their users and owners (such as custodian banks) have a great deal of relevant experience to draw upon.

By applying that experience, market infrastructures and custodian banks can support their existing customers to invest in crypto-assets. This is because the principal reason why most of their institutional clients have yet to invest in crypto-assets is their lack of confidence in the ability of the current eco-system of issuers, exchanges and service

[7] See Regulation (EU) no 909/2014 of the European Parliament and of the Council of 23 July 2014 on improving securities settlement in the European Union and on central securities depositories and amending Directives 98/26/EC and 2014/65/EU and Regulation (EU) No 236/2012, which states that infrastructures "give market participants confidence that securities transactions are executed properly and in a timely manner, including during periods of extreme stress. Due to their key position in the settlement process, the securities settlement systems operated by CSDs are of a systemic importance for the functioning of securities markets. Playing an important role in the securities holding systems through which their participants report the securities holdings of investors, the securities settlement systems operated by CSDs also serve as an essential tool to control the integrity of an issue, hindering the undue creation or reduction of issued securities, and thereby play an important role in maintaining investor confidence".

providers to mitigate and manage the variety of risks they expect to encounter and the lack of relevant regulation.

Blockchain technologies have the potential to solve many problems and alleviate others. But moving from a centralized infrastructure to a distributed infrastructure does not eliminate the risks associated with the issuance of financial assets, the settlement of transactions in the assets, the safekeeping and servicing of the assets and the protection of the assets from fraud, theft and destruction.

However, the transition from a centralized to a distributed model does alter the form the various risks take. Settlement is contractual, rather than final and irrevocable. The safety of the assets depends not on an electronic register, but on holding alphanumeric keys to a digital wallet. Peculiarities of this kind require existing service providers to adapt how they help their users (and the customers of their users) to mitigate those risks.

2.2 Issuance

Issuance is one area where existing methods can be adapted. One of the core functions of a CSD is to record newly issued securities in a digital book-entry system and ensure that at all times the number of securities in circulation equals the total number in issue. In this way, CSDs guarantee the "integrity" of the issue, by making it difficult for issuers or third parties to damage the interests of investors by creating additional securities or reducing the number of securities in circulation.

This "notary function" is obviously vital to the maintenance of investor confidence and could be adapted to help ICOs attract institutional investors. After all, an ICO, in which the promoters of a new project raise funds by selling tokens for fiat currency or crypto-assets, is comparable to a new issue of securities. Most ICOs even issue a prospectus, akin to that of an initial public offering (IPO) of securities, or a private placement, in which the project, the scale of the investment and the likely returns are described.

Although there is a large number of respectable and successful ICOs, whose promoters offer legitimate investment opportunities for investors, some have proved to be fraudulent. This is not abnormal for a new fund-raising technique. Fraud remains an ever-present threat, even in the highly regulated markets of today, and most ICOs are currently launched outside any established legal framework or structure of regulation.

This is not because securities market regulators are unaware of ICOs. In all major jurisdictions they have taken a wide variety of stances towards them. Almost all have issued warnings about the speculative nature of the investments. Many have stated that securities regulations may apply to ICOs. China has actually banned them, and the Reserve Bank of India has effectively banned their use in the banking system. The challenge facing regulators is how to protect investors without losing the wider benefits of distributed ledger technologies. However, closer regulation of ICOs is now widely expected[8].

While market infrastructures cannot eliminate fraudulent ICOs or even vouch for the fact that an ICO is legitimate, they have an obvious role to play in a regulated ICO market. This is to adapt their "notary function" to obviate the "double issuance" risk in ICOs by matching the number of tokens in issue with the number of tokens held in the accounts on the distributed ledger.

Though they cannot do this by the same method as the consensus mechanisms used in public blockchain networks – namely using computing power to check the validity of every transaction added to the ledger – market infrastructures can eliminate the risk of "double issuance" in private permissioned networks, by acting either directly as the

[8] https://www.bitcoinmarketjournal.com/ico-regulations/

"governor" of the network or as the rule-setting authority that oversees a sub-group of members of the network whose only role is to validate transactions.

In a permissioned network, in which membership is not open to all-comers and some participants have privileged access to information, market infrastructures can set the rules by which the network operates and monitor participants and their activities for breaches of them. This is a governance role that market infrastructures play already in the securities markets.

CCPs, for example, set eligibility criteria and margining and other rules for clearing brokers and monitor their compliance with them. CSDs fulfill a similar role in the admission of issuers and custodian banks as account-holders. CLS also sets eligibility criteria for banks to join its foreign exchange settlement network. SWIFT has membership criteria too.

Similar tests of creditworthiness, technical competence and legal and regulatory status can be applied to members of crypto-asset networks, including issuers and exchanges. The due diligence process could include formal disclosure requirements by organizations applying to join a network as well as checking publicly available data about such organizations against official sources lodged with company registrars[9].

Applying measures and services of this kind, which market infrastructures have developed in the securities markets, will provide a degree of reassurance to investors holding accounts on crypto-asset networks. Eventually, market infrastructures, intermediaries or even networks could offer investors the opportunity to hold crypto-assets in a segregated account in their own name rather than in a commingled account operated by an intermediary.

2.3 Liquidity

Liquidity – or at least the lack of it, as measured by the large spikes in prices for what in many cases purports to be a currency (see Chart 2) – is a major issue in crypto-asset markets. Specialist market makers (such as Keyrock) have emerged with the ambition of providing round-the-clock liquidity in crypto-assets across multiple crypto-exchanges, which are thinly capitalized and suffer from high rates of failure and misappropriation.

A decline in the volatility of crypto-assets will be a consequence as well as a cause of increased investment by institutional investors and banks, which must at present allocate high levels of capital to support such a volatile asset class. But the immediate challenge to be met - at least until crypto-assets are accepted by a much wider range of merchants, adding natural liquidity to the market - is not making it easier to exchange one crypto-asset for another. It is to provide investors with the ability to turn a crypto-asset into fiat currency on demand.

Convertibility into cash, after all, is the best standard by which to judge the liquidity of any asset, and crypto-assets are no exception. Unfortunately, crypto-assets issued onto distributed networks cannot yet settle directly in fiat currencies, because cash is not made available efficiently for payments to and from account-holders.

Instead, investors which wish to buy or sell crypto-assets have to pre-fund cash accounts which can be turned into tokens that can be delivered to accounts on the network. The tokens are an imperfect solution. They can be used to settle the cash leg of a crypto-asset transaction only until such time as a counterparty wishes to turn tokens into fiat currency again. Alternatively, investors could segregate the movement of assets and the movement of cash and accept the settlement / counterparty risk. At that point, the traditional correspondent banking systems are required. In other words, reliance on the pre-funding of accounts and the use of off-ledger correspondent banks, creates

[9] See, for example, https://datarama.com/

liquidity risk and additional costs. Those costs take the form of interest (the need to borrow cash) or opportunities foregone (the inability to invest elsewhere).

Further real time gross settlement as typically done in DLT environments requires more crypto asset liquidity from the participants compared to batched netted settlements. This is because participants would need to either hold the crypto asset or borrow it for use in settlement.

The netting of offsetting transactions between account-holders would reduce these interest and opportunity costs. In the securities markets of today, CSDs settle transactions netted mostly through CCPs. Market infrastructures could apply a netting model that would reduce the liquidity needs of counterparties. Further market infrastructures could facilitate an environment in which purchasing power could be provided to participants on crypto networks without having to pre-fund cash accounts with the surety that net obligations are settled.

Availability of central bank digital currencies (CBDCs) for wholesale payment and settlement transactions on distributed networks could help increase settlement efficiency and reduce liquidity risk.

2.4 Settlement

Settlement finality is as vital to investor confidence in crypto-assets as it is in any asset class. It provides legally sound reassurance that the seller owns the cash and the buyer owns the crypto-asset, irrevocably and finally, irrespective of whether either party becomes insolvent or goes bankrupt. This ensures that, even if a counterparty fails, a liquidator cannot unravel the transaction.

But settlement finality is not achieved in the same way in transactions completed on distributed networks. In non-permissioned distributed networks that use proof-of-work to achieve consensus, settlement is not final but probabilistic: It simply becomes more final the more times the transaction is committed to the ledger.

Typically, a public blockchain requires multiple blocks to be confirmed to the ledger before a transaction can be considered practically (though not legally) final. This process can take from a few seconds to several minutes, depending on the consensus algorithm employed. It means a transaction might be committed to the ledger after bankruptcy proceedings were commenced against one of the parties. In such a case, the insolvency laws of the jurisdiction in which the counterparty failed might require the transaction to be reversed.

Clearly, this falls short of the security offered by legal definitions of settlement finality in the securities markets, such as that contained in the 1998 Settlement Finality Directive of the EU. That legislation was of course passed specifically to eliminate variances between legal jurisdictions in their treatment of property in insolvency proceedings at a time when cross-border transactions were increasing.

Distributed networks, both public and permissioned, operating across borders, now face the same difficulty: How to achieve settlement finality, especially amid multi-jurisdictional legal uncertainty.

While legal uncertainty is not an obstacle that market infrastructures can clear directly, they can help create certainty around the ultimate transfer of ownership of crypto assets by administering rules and contractual agreements that ensure transactions on them not only become irrevocable once they are settled but are also legally final.

Operational rules could insist, for example, that sellers always have the crypto-assets visible in their account on the ledger and buyers always have the fiat currency or crypto-asset visible in their account on the ledger. Contractual agreements between counterparties transacting on the network could already help make the settlement legally final to a high degree of certainty.

While it is difficult to provide the same protection to counterparties settling on distributed networks until legislators in multiple jurisdictions define a legal framework for DLT settlement finality or agree on a common definition, a rules and contracts based settlement framework of this sort can help to instill confidence in the network participants and drive institutional adoption.

It ensures that crypto-asset transactions settle in broad compliance with the highest standards of settlement finality in the securities markets of today. Without it, the inability to provide irrevocable and final settlement will act as a constraint on the growth of crypto-assets, particularly among institutional investors.

2.5 Inter-Operability

Crypto-assets are currently issued onto multiple distributed networks that are not linked to each other, so selling assets on one to buy assets on another entails multiple transactions. In addition, the distributed networks on which crypto-assets are issued and traded will co-exist, for the foreseeable future, with the existing centralized trading, clearing and settlement market infrastructures. It follows that distributed networks will have to inter-operate both with each other (there are several different types) and with legacy infrastructures.

This is already the case with payments, where investors wanting to convert crypto-assets into fiat currency must make use of the existing networks of correspondent banks and payments market infrastructures. As institutional investors start to invest in crypto-assets, they will expect the custodian banks they appoint to settle any purchases or sales and to safekeep the assets they choose to hold. This means that custodians will need to interface with distributed networks[10].

There are a number of obstacles to this. One is that in distributed networks issuance, execution, clearing and settlement are collapsed into a single process, so there is no need for intermediaries to collect, exchange and reconcile information about transactions. But reconciling holdings of crypto-assets by market participants in both legacy systems (where anomalies can be resolved by adjusting positions) and distributed networks (where records are immutable and changes require a new transaction) will still be necessary, yet problematic.

The differences between distributed networks and centralized systems will attract the attention of regulators if solutions are not identified, since they increase the complexity of the financial system and widen the potential sources of contagion. The failure, for example, of a major participant in a distributed network, or of the provider of the underlying technology, will spill over into any legacy systems with which the network inter-operates. This risk will become progressively more acute as crypto-asset values and transaction volumes increase.

If contagion risk does materialize, resolving it will be further complicated by legal risk. While jurisdictional differences are a feature of the financial markets today, assets are not held nor are transactions completed in more than one jurisdiction: In a centralized system, both occur within a single infrastructure in one legal jurisdiction. But in a distributed network, crypto-asset holdings and transactions will span multiple jurisdictions, each of which might take a different view of the legal status of the same asset or transaction.

[10] According to one recent study, they have so far failed to do this. See Thorsten Ehinger, Promila Gurbuxani, Jonathan Klein and Matthias Voelkel, *A calm surface belies transformation in securities services*, McKinsey & Company, March 2018. https://www.mckinsey.com/industries/financial-services/our-insights/a-calm-surface-belies-transformation-in-securities-services

This legal risk is accentuated by the use of smart contracts. The automatic execution of contractual obligations makes it difficult to reverse mistakes, while the uncertain legal status of smart contracts provides an unsure foundation for doing so.

In the absence of a sound, internationally agreed legal and regulatory regime governing the activities of distributed networks, the best practical solution is a network governor to set clear rules to govern the behavior of all participants in a distributed network, including when they inter-operate with other distributed networks and with legacy market infrastructures. The governor can monitor the operation of the rules for breaches and resolve disputes when they occur.

Governance arrangements could also establish rules to resolve regulatory inconsistencies between distributed networks and legacy infrastructures. In the EU, for example, the imposition by CSDR of fines and mandatory buy-ins on counterparties which cause matched transactions to fail to settle is difficult to apply to distributed networks in which settlement takes place directly between the accounts of the buyers and sellers on the blockchain.

What is also essential to inter-operability is standardization. By implementing business and technical standards, market infrastructures make it easier for their users to access multiple markets without having to build a bespoke interface to each one. In the same way, a standardized interface for multiple crypto-exchanges makes commercial sense. The cost of bespoke interfaces would otherwise multiply by the number of exchanges. Re-using existing communications channels and existing authentication mechanisms will be much cheaper.

It would also be sensible to base the standardized interfaces on existing message standards (such as ISO 20022) because these are already used and fully endorsed by market participants to link their systems to market infrastructures[11]. Existing business and technical standards should appeal to the crypto-exchanges as well, since this enlarges the reach of the assets traded on their platform to encompass the established investors and trading platforms in the securities markets.

A key success factor for an industry solution targeting the clearing and settlement of crypto-assets is the development of common standards. Those standards should be created from a set of common business rules and technical specifications based on the existing business standards under the auspices of standards bodies and open source initiatives to ensure that distributed platforms are fully interoperable at a business and technical level. The securities industry should collaborate to evolve and adapt the business standards that will be required for DLT to take its place in the securities services value chain and business processes with minimum disruption and rework. This will support an easy integration with existing automation technology such as messaging gateways, standard middleware and standardized APIs. A standardized input to the shared ledger that defines the data set and the format provided to participants to create, confirm or reject an entry. The standard includes among many data elements certainly a common time stamping model that distinguishes the creation time of an entry from its booking time or its value time.

[11] A study of ISO 20022 in fixed income securities trades on distributed, blockchain-based networks concluded they would enhance inter-operability (see SWIFT, Information paper, *Distributed ledgers, smart contracts, business standards and ISO 20022*, September 2016) https://www.swift.com/insights/press-releases/swift-examines-application-of-financial-business-standards-to-distributed-ledger-technology-and-smart-contracts and a separate study of proxy voting on distributed networks also concluded that ISO 20022 would be helpful (see ISSA, *General Meeting Proxy Voting on Distributed Ledger*, Product Requirements v2.1, November 2017) https://www.swift.com/insights/press-releases/swift-examines-application-of-financial-business-standards-to-distributed-ledger-technology-and-smart-contracts

2.6 Safekeeping

Crypto-assets, issued and traded on a distributed ledger, serviced through smart contracts and held in cryptographically secure digital wallets, are often said to have no need of traditional safekeeping services. However, the safety of assets held in digital wallets depends on asymmetric keys which are vulnerable to loss. They combine the use of a public key (which allows the ledger to encrypt the information) and a private key (which allows the owner to decrypt the information).

The reliance of distributed networks on embedding information about ownership in the digital asset itself in this way is akin to the physical custody of securities. In fact, custody services have emerged that offer so-called "cold storage" of private keys in secure vaults. But these exemplify the risk of catastrophic loss. Just as destruction of a physical bearer certificate used to erase all knowledge of ownership, so does loss of private keys today. The loss becomes irreversible. In reality, the loss of the private keys is tantamount to the loss of the crypto-assets.

Yet the methods for keeping private keys safe are not reassuring for investors. They include locking a hard drive or USB stick in a safe, storing the key in physical form, or just storing it in a digital location that is not connected to the Internet. Hardware Security Modules (HSMs), which are designed to protect cryptographic keys, combine these features, by using certified hardware, specialized operating systems and minimal Internet access to hide and protect private keys.

All these forms of safekeeping are not unlike the asset safety measures that characterized the securities industry until the 1990s: Physical custody. Paper share and bond certificates were simply locked in a large safe at a bank, where they remained vulnerable to theft or destruction. CSDs have provided a less cumbersome solution. At first all paper certificates were immobilized at the CSD, and then they were dematerialized, or reduced to digital registers of ownership only.

These digital registers protect the assets, because they can be backed up, and changed in cases of theft or misappropriation or error. This is not an option in distributed networks, which collapse the registration function into the record of transactions maintained on the digital ledger. Yet market infrastructures, which often act as the register of owners of securities, are in good position to monitor the updating of the ledger as crypto-assets are bought and sold.

In fact, providing a registration monitoring function independently of the distributed network would provide a valuable degree of reassurance to investors. Relying on crypto-exchanges to update their own ledger ignores a conflict of interest. Further, relying on them to safekeep private keys is clearly unsafe, since hackers have already penetrated their defenses and stolen assets. In this context, outsourcing the management of the risk to a trusted third party will appeal to investors.

Market infrastructures, perhaps working in collaboration with custodian banks and technology providers, could provide an independent safekeeping service for private keys. They would need to decide collectively on the most secure method of storing private keys in terms of physical protection. They might also wish to create an audited reserve to back any liability they incur to compensate investors for losses.

2.7 Cyber-Security

Centralized market infrastructures mitigate the risk of losses by building secondary and tertiary recovery sites that replicate information in real-time and sometimes use different software to increase the level of protection. Distributed networks mitigate the risk by avoiding a single point of failure at the primary, secondary or tertiary level. Instead, multiple copies of the same sets of information are distributed throughout the network.

However, hacking of crypto-asset marketplaces is not uncommon. Distributed networks, particularly of the public, non-permissioned variety, are vulnerable to manipulation of the data by any group capable of controlling more than 50 per cent of the "hash rate", or computing power, of the network[12]. The attackers are able to prevent new transactions from being confirmed, allowing them to halt payments between some or all users.

Distributed networks share code as well as data – and this vulnerability is true of private permissioned networks as well as public, permission-less ones, though the risk of bugs being added to software is obviously higher in a network without formal control of access. Distributed networks will also, for the foreseeable future, have to interact with legacy networks, which creates further points of vulnerability.

The codes of smart contracts, which are used to automate the execution of contractual obligations, are, as a recent report pointed out, a particular risk, because they are subject to constant change and inter-operate continuously with other systems[13]. This creates a degree of dependence on the software writing and testing capabilities of all other members of the network, creating room for malicious actors to embed code that puts the ownership, purchase and sale of crypto-assets at risk.

These risks can be mitigated, at least in private, permissioned networks, by the appointment of a governor to vet applications for membership and the quality of the software members of a network are obliged to use, including that written to underpin smart contracts.

In the securities markets, market infrastructures already maintain clear membership criteria and auditable processes and procedures to control access to data and changes to software code. They also draw up and regularly update detailed plans itemizing the actions to be taken in the event a cyber-attack is detected.

In addition, as market infrastructures have been judged by regulators to be of systemic importance, and therefore open to cyber-attack by nation-states, criminals and so-called "hacktivists", they have to invest heavily in cyber-security measures (e.g. the Customer Security Programme launched by SWIFT). By providing additional assurance to investors, market infrastructure can accelerate institutional investment in crypto-asset markets.

2.8 KYC, AML and Sanctions Screening

The early growth and development of crypto-assets was hampered by the conviction that they were useful mainly to criminals engaged in illicit purchases, the financing of terrorism, tax evasion or money laundering. This reputation, which has also infected ICOs, has proved hard to dispel. A report prepared for the European Parliament this year estimated that the misuse of crypto-assets probably exceeds €7 billion and argued that the principal problem to be addressed is the anonymity of the users[14].

The fifth version of the European Anti-Money Laundering Directive (AMLD5), which came into force on 9 July 2018, addresses the issue directly. It includes a definition of "virtual

[12] A mining pool or group of colluding mining pools that controls 51 per cent of mining power can potentially append false transactions to a public blockchain. Private, permissioned networks do not use "miners."See ISSA, *Distributed Ledger Technology: Principles for Industry-Wide Acceptance*, Version 1.0 Report, June 2018, at https://www.issanet.org/e/pdf/2018-06_ISSA_DLT_report_version_1.0.pdf

[13] Deloitte, *Six Control Principles for Financial Services Blockchains*, October 2017. https://www2.deloitte.com/ie/en/pages/technology/articles/blockchain-control-principles.html

[14] Professor Dr Robby Houben and Alexander Snyers, Directorate -General for Internal Policies, *Cryptocurrencies and blockchain: Legal context and implications for financial crime, money laundering and tax evasion.* Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, July 2018.

currencies" and subjects virtual currency exchanges and digital wallet providers to customer due diligence requirements of the same kind that now apply in the established financial markets. Crypto-asset issuers and exchanges in Europe are now under a legal duty to report suspicious transactions to the authorities, who can share the information with the tax authorities.

This means that distributed networks on which crypto-assets are bought and sold are now under a legal obligation, at least within the EU, to

- Collect and analyze basic identity information;
- Check it against public records such as passports, identity cards, and certificates of incorporation;
- Match names against lists of "politically exposed person" (PEPs) and black-listed investors;
- Define how they might be expected to transact in the assets; and
- Monitor their actual transactional behavior against the definition.

Building an effective and efficient Know Your Client (KYC), Anti-Money Laundering (AML) and sanctions screening process of this kind is a complex and expensive undertaking. The Financial Action Taskforce (FATF) recently published an updated version of its methodology for assessing compliance with its own recommendations for reducing money laundering, whose length and complexity is considerable[15].

It follows that the risks of non-compliance by distributed networks is high. This is one reason why there are frequent suggestions that markets develop centralized services[16]. So there is a clear opportunity for crypto-currency issuers and exchanges to avoid the costs and risks of duplication of their KYC, AML and sanctions screening due diligence processes by outsourcing the work to a third party.

Market infrastructures are one candidate for this role. They already run extensive due diligence checks on every individual and organization that opens an account with them, and on the transactions they settle, and they cover different jurisdictions. A group of market infrastructures, organised on a regional or global basis, could also pool KYC, AML and sanctions screening information for the use of crypto-asset issuers and exchanges.

2.9 Taxation

The tax treatment of crypto-assets is still evolving and varies widely by jurisdiction. Some governments treat them as a commodity, others as a currency, and some as a security. The tax treatment varies according to the classification of the asset and the tax code of the jurisdiction in which the investor is based. What is clear is that using crypto-assets to pay for goods and services does not exempt the payer from value added taxes, receiving crypto-assets as payment does not exempt the payee from income taxes and that any appreciation in the value of crypto-assets will be subject to capital gains taxation where applicable[17].

This uncertainty about the tax treatment of crypto-assets in different jurisdictions is one of the largest deterrents to investment by institutional investors in the asset class,

---

[15] FATF, *Methodology for Assessing Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems,* updated February 2018, at http://www.fatf-gafi.org/media/fatf/documents/methodology/FATF%20Methodology%2022%20Feb%202013.pdf

[16] Such as that being developed by the Central Registry of Securitization and Asset Reconstruction and Security Interest in India (CERSAI).

[17] See, for example, the policy statement by the US Internal Revenue Service at https://www.irs.gov/pub/irs-drop/n-14-21.pdf

because it is one of the biggest risks they face. They cannot be certain about the size of any tax liability on a successful investment and even which tax authority is entitled to payment. While they are not interested in the complexities of tax treatments, especially across borders, they do not want to be taxed twice, and they want tax relief granted and paid as fast as possible.

In the securities markets, institutional investors generally outsource this work to third parties, including global custodian banks, accounting firms and specialist advisers. No comparable entity is yet providing a similar service to investors in crypto-assets, though crypto-exchanges are developing services for retail investors[18]. There is an opportunity to encourage institutional investors to take an interest in crypto-assets by developing a service to help them settle questions such as value at acquisition and sale, beneficial ownership and tax jurisdiction.

Market infrastructures, in tandem with global custodians, could develop a data consolidation service for investors, giving them a view of all of their assets and liabilities across multiple networks, markets, asset classes and jurisdictions. This would be useful to third-party accounting firms and tax advisers to investors, not only for tax compliance and reclaims, but in enabling them to offer advice to investors on how to hold crypto-assets in a tax-efficient way.

[18] For example, Coinbase, a platform for buying, selling, transferring and holding crypto-assets, is providing its users with information about their purchases and sales to help them complete their tax returns.

3. Summary and Conclusion

3.1 The Relevance of the Experience of the Securities Markets

A large part of the attraction of crypto-currencies and crypto-assets, for investors as well as issuers, is the prospect of a financial system that operates without intermediaries, including market infrastructures and custodian banks. But there is a secondary attraction in blockchain technology which is easily forgotten. This is that it *distributes* as well as *disintermediates*.

In theory, information about financial assets and transactions no longer has to pass through centralized institutions. Indeed, information about financial assets and transactions no longer has to be controlled by anyone at all. In short, there is no need for anyone to *govern* the issuance, trading, clearance and settlement of financial assets.

The experience with crypto-assets so far falls some way short of this ideal. Value and activity in crypto-assets is highly concentrated among a small class of crypto-currencies and tokens that control the bulk of the necessary computing power. The number of ICOs that failed to deliver viable projects is extremely high. Thefts of crypto-assets are a frequent occurrence.

Yet it would be a mistake to believe that these problems invalidate the opportunities crypto-assets create to provide new forms of financing and ownership and to reduce costs and risks. The challenge is to find ways and means of solving or reducing the size of the problems in order to eliminate the deterrent they represent to the engagement of institutional investors in crypto-asset markets.

In meeting the challenge, the experience of the securities markets is relevant. Much of the early enthusiasm for distributed networks was based on the power of the technology to bypass the need for law and regulation. But the securities markets have found that market infrastructures and financial institutions, operating within a framework of law and regulation, are essential to growth and success.

In the securities markets, market infrastructures and custodian banks ensure that transactions settle promptly, even in stressed markets. They help to safekeep assets, chiefly by maintaining accurate records of ownership and help investors to claim their entitlements. They also ensure that the number of securities held by investors always matches exactly the number in issue.

They fulfill these various roles in a highly regulated environment, based on law. Market infrastructures are regulated directly themselves and all of the entities with which they interact – exchanges, brokers, banks, custodians, registrars, fund administrators and central banks – are also regulated directly. The networks to which they belong are, to borrow a phrase from crypto-asset culture, "permissioned".

3.2 Successful Distributed Networks Need Good Governance as well as Efficiency

One clear finding of this paper is that market infrastructures and their users are less likely to have a prominent role in public distributed networks but a great deal to offer "permissioned" distributed networks. That is precisely because the *operational* services they offer to crypto-asset issuers and investors cannot sensibly be analyzed in isolation from the *governance* of the networks on which crypto-assets are issued, traded, settled and safekept.

Obviating *issuance* risk in crypto-assets, for example, entails matching the number of tokens in issue with the number of tokens held in accounts on a distributed network. To fulfill that role, a governing authority must join the network to vet applications to open

accounts and to validate transactions, either directly or by supervising other participants that perform the same function, i.e. the network governor defines the operating rules including the membership and a network operator implements them.

Likewise, improving liquidity in crypto-assets means overcoming the costs and inefficiency in today's crypto-asset world by e.g. ensuring safe settlement (delivery of crypto vs cash payment) and providing netting efficiency. Today's practice of prefunding and of payments outside the blockchain environment, traps liquidity and proves costly and inefficient. A trusted network participant like a market infrastructure can play a role to ensure purchasing power is made available to the network and net obligations are settled.

In helping distributed networks achieve settlement finality in crypto-asset transactions, market infrastructures could help create certainty around the ultimate transfer of ownership. Its relevance even increases in cross-border crypto transactions by effectively mitigating the impact of handling different jurisdictions with different conceptions of settlement finality. Comparable to the current market practices around delivery versus payment and linking markets, market infrastructure could not only ensure irrevocable but also legally final settlement in the jurisdictions involved.

Achieving *inter-operability* between distributed networks of different kinds with each other, and with legacy market infrastructures and their users, such as custodian banks, creates a series of operational, reconciliation, legal and contagion risks. These can be mitigated by the design, implementation and supervision of rules of interaction, as well as by wider use of existing business and technical standards and interfaces for the exchange of information.

Enabling investors to take secure ownership of crypto-assets depends on assessing the accuracy of the records of transactions on the digital ledger. Retaining ownership hinges on the *safekeeping* of private keys. Market infrastructures, working in collaboration with technology providers and custodian banks, can develop combinations of supervision and custody services that ensure that title transfer on a distributed network is secure and which provide safe custody for private keys.

The vulnerability of crypto-assets to breaches of *cyber-security*, which is exacerbated by the sharing of code as well as information between members of the distributed networks, is best reduced by market infrastructures vetting applications being released to the network, certifying the robustness of software codes and drawing on their experience of preparing detailed plans to respond to cyber-attacks.

With crypto-asset issuers and exchanges and providers of digital wallet services coming under pressure to check the identity of their customers and monitor their behavior for signs of illicit activity, the risk of compliance failure is rising. Market infrastructures can help mutualize the cost of compliance in distributed networks by supporting KYC, AML and sanctions screening services on an outsourced basis.

Another area rich in compliance risk for issuers and investors active on distributed networks is the *taxation* of transactions, capital gains and income derived from crypto-assets. By working with global custodians, which already offer tax reclamation and relief-at-source services to investors, market infrastructures can provide tax information to investors and their tax advisers.

3.3 The Need to Strike the Right Balance Between Innovation and Risk

Clearly, the long-term success of crypto-assets depends on both good governance and operational efficiency, but these functions can and should be separated. In fact, shifting from a centralized environment to a decentralized environment makes the separation of the governance of distributed networks from their operation even more important. Who is admitted to a network, who has access to what information on the network and how

bad behavior is discouraged on the network, are of paramount importance in distributed networks. Managing these issues successfully demands independence to the benefit of the industry and its community.

However, as independent as they are, existing market infrastructures will not solve all the governance and operational challenges which the crypto-asset markets now confront. In addition, there is a strong logic for them to work with financial intermediaries such as custodian banks and also technology providers as well as regulators to help the crypto-asset markets accelerate their progress towards a higher level of safety and efficiency. This is because, as Table 2 illustrates with some examples, many of their existing services are easily adapted to the needs of the crypto-asset markets today.

Table 2: Examples of Possible Roles (Actively Pursued for Existing Asset Classes) and Future Roles of Market Infrastructures

	Existing Asset Classes	New Crypto-Asset Classes
Possible Roles	Custody/settlement and trading of existing securities on distributed ledger.	Due diligence on issuers of Security Token Offerings (STO) or governing a network that hosts STOs
Potential New Roles	Provide pre-issuance platform (origination, syndication and distribution) to issuers, dealers & investors.	Safekeeping of private keys by providing key management wallet services

In adapting to distributed networks the services they have developed in the securities markets, today's market infrastructures will be mindful of the need to solve problems without crushing the ingenuity and innovation which has driven the growth of the markets in crypto-assets, or raising transaction or compliance costs to burdensome levels.

This paper identifies different areas where market infrastructures could play an important role in ensuring safety and efficiency of crypto markets, i.e. monitoring issuers, facilitating the settlement of crypto-assets versus cash, providing settlement finality, encouraging the use of standardized interfaces, existing business and technical standards and message protocols, safekeeping private keys to digital wallets and supporting oversight and services to minimize the risks of cyber-attack and KYC, AML and sanctions screening and tax compliance failures.

In playing a role that supports the evolution of the crypto markets, existing market infrastructures are steered by an agreed set of principles set by the regulators, which include the maintenance of financial stability as well as investor protection[19]. While regulatory treatment of crypto-assets is fragmented - the French regulator is working on a legal framework for ICOs[20] and Malta[21] has already defined one, while the United

[19] Committee on Payment and Settlement Systems and the Technical Committee of the International Organization of Securities Commissions, *Principles for financial market infrastructures*, April 2012. https://www.bis.org/cpmi/publ/d101.htm

[20] https://www.amf-france.org/en_US/Actualites/Communiques-de-presse/AMF/annee-2018?docId=workspace%3A%2F%2FSpacesStore%2F57711a6c-4494-4215-993b-716870ffb182

[21] https://www.chambersandpartners.com/article/4008/malta-approves-crypto-acts-and-creates-a-regulated-framework-for-icos-and-exchanges

Kingdom has encouraged experimentation via a regulatory "sandbox"[22] – there is measurable regulatory interest everywhere in devising policies for the management of crypto-asset risk.

At bottom, the challenge in creating a safe and efficient environment for investors in crypto-assets does require a suitable framework of law and regulation. However, in the long term as well as the short, it would be a mistake to dispense with current ways of managing and mitigating risk and with existing rules and rule-makers. The better solution is to bring them both into closer alignment with the nature and power of distributed ledger technology.

That alignment will not be a one-way street. Wherever the risks and costs of maintaining trust between buyers and sellers in intermediated, centralized systems outweigh the costs and risks of maintaining trust in an un-intermediated, distributed system, there is no case for persisting with the status quo.

Issuers and exchanges, and the other members of the crypto-asset eco-system, ought to welcome this prospect rather than deplore it. The involvement of market infrastructures in a variety of governance and operational roles can only increase the trust of investors, by raising the quality of the infrastructure which underpins the new asset class. By that means, market infrastructures will help crypto-asset markets to grow more quickly.

[22] https://www.fca.org.uk/firms/regulatory-sandbox/regulatory-sandbox-cohort-4-businesses

Appendix 1: Glossary of Terms

APIs. An Application Program Interface (API) allows two applications to exchange data with each other and present the data in any format required.

Crypto-asset. A crypto-asset is a tokenized asset that does not necessarily derive its value from the chain and whose application is not necessarily payment. It includes crypto-currencies, utility tokens, platform tokens and tokenized securities. A crypto-asset shares the characteristics of a digital asset (see below) and, in addition, allows for issuance, termination, ownership and transfer of ownership to be guaranteed via cryptography.

Distributed ledger platform. As defined in the ISSA paper on distributed ledger technology[23], a distributed ledger technology (DLT) platform is a distributed, automated, shared database of information and business rules, combined with a methodology for cryptographic protection and guaranteed integrity of digital data and transactions.

Digital asset. An asset in binary form that comes with a right to use, that has clearly defined notions of issuance, termination, ownership, and transfer of ownership, a definable monetary value, which may be between specific counterparties, and which may be based on right to use, or may be based on the principle of limited supply.

Digital wallets. These are provided by companies for users to store their tokens in a given crypto- asset in a secure manner.

Hardware Security Module (HSM). A physical device designed to protect cryptographic private keys by using certified hardware, specialized operating systems and minimal Internet access.

Hash rate. The speed at which a computer is completing an operation in a crypto-currency code. The faster the hash rate, the greater the chance of a "miner" finding the next block and claiming the reward.

ISO 20022. ISO 20022 is a recipe for a universal financial industry message scheme, and includes:
- a syntax neutral business modelling methodology
- syntax specific design rules
- an industry led development/registration process
- a financial repository on www.iso20022.org

Issuer. The company that issues crypto-asset tokens in exchange for fiat currency or crypto-assets.

Miner. The individuals who create blocks of validated transactions and add them to the ledger by solving complex mathematical puzzles. They are rewarded with crypto-assets.

Network operator. The entity that manages a distributed network on a day-to-day basis and implements rules laid down by the network governor, including admission to the network. Often synonymous with the issuer.

Network governor. The entity that devises the rules and policies by which a distributed network is run, including admission criteria. Often synonymous with the network operator.

Node. A computer connected to a distributed network, which receives a copy of the single, distributed ledger.

Permissionless/Public distributed ledger networks. Many blockchain-based networks, like Bitcoin and Ethereum, are characterized by the anonymity of their users

[23] https://www.issanet.org/e/pdf/2018-06_ISSA_DLT_report_version_1.0.pdf

and the complete lack of any centralized service that is required to run the network. Those solutions are also referred to as "public" or "permission-less" networks.

Permissioned distributed ledger networks. These are characterized by a strong membership authentication mechanism and depend on the availability of centralized services to run the network. They were developed partly as an answer to the scalability issues and the high power consumption necessary to run a public or "permission-less" network, but also to accommodate the need of sophisticated institutions to protect their data and reduce risk by restricting membership of the network.

Politically exposed person (PEP). A PEP is a person who has been entrusted with a prominent public function, or an individual who is closely related to such a person.

Registration services. Trusted third parties which register the existence of a crypto-asset.

Smart contracts. A smart contract is a computer code that executes the terms of a contract automatically. A blockchain-based smart contract is visible to all users of the network in question. A smart contract can vary according to the role of each node, even though every node is part of the same network.

Smart contract verifiers. Service providers that certify the quality of the code in which a smart contract is written.

Appendix 2: What Market Infrastructures are Doing with Blockchain

Country/ Region	Organization	Use Case
Abu Dhabi	Abu Dhabi Securities Exchange	Implemented an e-Voting platform using blockchain technology.
Australia	Australian Securities Exchange	Using DLT to record shareholdings and manage the clearing and settlement of equity transactions, ASX will replace its current settlement and clearing system known as the Clearing House Electronic Sub register System (CHESS) in partnership with Digital Asset Holdings.
Argentina	Caja de Valores	Announced the implementation of a proxy voting project and digital input center for the distribution of issuers and equities information.
Chile	Chile Santiago Exchange	Implementation of a blockchain application for the short selling system for securities lending. The technology aims to improve transaction management, reduce costs and provide Chilean institutions with greater information integrity.
USA	CME Group	Launched bitcoin futures contracts in December 2017. Partnered with the Royal Mint to test a blockchain-based platform for trading gold.
EU	Deutsche Börse AG	Deutsche Börse and the Deutsche Bundesbank have collaborated to present a prototype for the blockchain technology-based settlement of securities. The solution is designed to provide the settlement of securities in delivery-versus-payment mode for centrally-issued digital coins or digital securities. Four international CSDs under the Liquidity Alliance will develop a blockchain prototype based on the Hyperledger Fabric blockchain to provide a solution for faster and more efficient mobilization of collateral transfers.
USA/Global	DTCC	Developing an industrywide DLT platform for a Trade Information Warehouse for cleared and bilateral credit derivatives in partnership with IBM, Axoni and R3.

Country/ Region	Organization	Use Case
EU	Euroclear	Partnered with Nasdaq, ABN AMRO Clearing to develop an end to end blockchain solution for the processing of collateral with securities to cover margin calls.
EU	Euronext	Launched LiquidShare for SMEs improving the transparency, speed and security of post-trade operations using blockchain.
Republic of Korea	Korea Stock Exchange	Launched a blockchain solution called the Korean Start-up Market within the blockchain-based market place where equity shares can be traded. The blockchain technology was implemented in November 2016, provided by Blocko Inc.
Italy	London Stock Exchange Group	Partnered with IBM to build a blockchain-based platform to digitally issue private shares of small and medium enterprises in Italy.
USA	NASDAQ	Announced the LINQ platform that allows private companies to record private securities transactions. Partnered with Citi on an integrated payment solution to record and transmit payment instructions. Complete Proof-of-Concept (PoC) that provides an efficient 24/7 securities collateral solution, according to a press release published Tuesday, June 19. See Euroclear re. securities collateral solution.
Russia	National Settlement Depository	Partnered with Sberbank, an education platform LevelOne and the Bank of Russia to develop a blockchain platform for compliant, regulated ICO issue and token custody based on Russian central bank-backed Masterchain DLT. Adopted Hyperledger Fabric 1.0 and smart contracts to carry out the settlement of transactions for commercial bonds.
India	National Stock Exchange of India	Testing blockchain technology for Know Your Customer (KYC) data. The solution allows participants to access the KYC data in real time.
Singapore	Singapore Exchange Limited	Currently exploring the use of blockchain in making trading and settlement of fixed-income trading cycle more efficient. Partnership with Cobalt, a firm using DLT streamline post-trade settlements.

Country/ Region	Organization	Use Case
Switzerland	SIX SIS AG	Announced the launch of SIX Digital Exchange (SDX) to enable the tokenization of existing securities and non-bankable assets. It will be the first market infrastructure in the world to offer a fully integrated end to end trading, settlement and custody service for digital assets. PoC: Partnered with Digital Asset Holdings to test a new bond issuing solution which covers the entire bond lifecycle, from issuance to settlement. Partnered with NASDAQ to test blockchain technology for SIX's OTC structured products unit.
Hong Kong	Stock Exchange of Hong Kong	Announced the launch of a blockchain powered private market, aimed at helping early-stage and smaller firms obtain financing.
South Africa	Strate	Partnered with NASDAQ to deliver an e-Voting Solution based on blockchain technology.
Canada	TMX Group	Collaboration with the Bank of Canada and Payments Canada in a proof-of-concept project to explore the settlement of netted and novated trades on DLT using tokenized fiat money and securities.
Japan	Tokyo Stock Exchange	In agreement with IBM to test a trade confirmation prototype for trading and settlement in low liquidity markets.

Appendix 3: Current Crypto Asset Market Roles

Service Group	Stakeholder	Service Offering
Investor Services	Investors	Private individuals, family offices, hedge funds etc. buying crypto-assets for the purpose of pecuniary benefit or to make use of a service associated with the crypto-asset purchased.
	Wallet providers	(Usually) companies providing solutions for users to store their tokens for a given crypto-asset in a secure manner.
Issuer and Corporate Services	Issuers	Issuers receive crypto-assets or fiat currency in exchange for the tokens they issue. They are responsible for the whitepaper on a given crypto-asset and for the development of any services associated with the crypto-asset. Issues the native tokens with funds being raised in either fiat currency or in a crypto- currency.
	Advisors	Industry and technology practitioners and influencers advising the issuer and providing trust to the company.
	Incubators and accelerators	Ecosystem of various service providers assisting the company to turn the whitepaper, PoC or the prototype into a viable product.
	Issuance providers	Pre-sale offerings Allocation services such as geo, cap and other forms
	Registrars of token holders	Registrar services provide issuer information of token holders, access to them and offer servicing of the assets.
	Sales, marketing and communications providers	Integrated with the issuer or outsourced. Provide services such as roadshows, promotions, documentation, website, etc. Advisors play a significant role in this area.
	Advocacy groups	Connecting the community to shared resources and know-how, e.g. Enterprise Ethereum Alliance, Anchors on Stellar, Tokenomica and Basics Fund on Waves
Certification and Authorization Services	KYC providers	Regulatory and legal function necessary for creating trust in and compliance for the crypto-asset.
	Registration providers	Registration of the crypto-asset within a trusted party. Furthers the compliance to regulations.
	Legal services providers	Legal services detailing the corporates' role and responsibilities, defining the relationship between the issuer and investor and legal clarification on the nature of the crypto-asset. Enhances the trust of the issuance and its lifecycle and is instrumental in providing the white paper.
	Tax authorities	Guarantor for tax compliance

Service Group	Stakeholder	Service Offering
Infrastructure and Technology Services	**Infrastructure providers Ethereum, Waves, Stellar, NEO etc.**	**Providers that do not only offer their platform but provide additional products and additional services such as multi-currency wallets, fund raising abilities, tokenization etc.** **Included are activities and roles for token generation, payment, fiat conversions, exchange trading enablement, etc.**
	DLT System designers / providers	May be an individual designing its own DLT on which a given crypto-asset operates, or it may be a pre-established system such as Ethereum, Waves, Stellar, NEO etc.
	DLT node operators	Individuals or companies that provide processing power to run the DLT system on which a crypto-asset is based on. These may be private individuals or corporations. In some cases, they receive remuneration for the operation of the node (i.e. currently bitcoin miners are paid for providing the mining service).
	Network operator	In charge of the day to day management of the network. Implements and enforces the policies established by the network governor. Manages membership of network based on the operating rules of the network. Provides, or arranges for, support for problems encountered by the business network's users. Reports to the network governor.
	Developers	Developers of the systems such as smart contracts.
	Smart contract verifiers	Providers of compliance to and certification of developed smart contracts. One major aspect is to enhance trust in the crypto-asset and its IT setup.
	Fiat gateway providers	Providers of a technical gateway between coins/tokens to and from fiat systems.
	Exchange infrastructure providers	Usually based on centralized online locations with wallets across various crypto / fiat networks, that can be used by users to exchange one crypto-asset for fiat cash or tokens of another crypto-asset. Market making can be one of their main activities.
	Derivatives trading providers	Offering of derivative contracts on crypto underlying assets
Governance	Network governor	In charge of the strategic management and governance policies of the network. Accountable for the implementation and enforcement of those policies. Defines the legal and regulatory basis on which the business network operates. Determines how the network will be operated and by whom. The roles of network operator and governor can be fulfilled by the same organization.

Appendix 4: Working Group Members

Working Group Member	Organisation
Alexander Chekanov (Stream Lead)	NSD Russia
Urs Sauer (DLT Working Group Lead)	SIX Securities & Exchanges
Henri Bergström	Abu Dhabi Securities Exchange (ADX)
Ana Casalla	Caja de Valores SA, Argentina
Marina Leontari	Clearstream Banking
Claudio Calderon	Deposito Central de Valores S.A. Chile
Nardeo Ganesh	DTCC
Daniel Thieke	DTCC
Glen Fernandes	Euroclear
Walter Verbeke	Euroclear
Rok Sketa	KDD Central Securities Clearing Corporation, Slovenia
Dace Daukste	Nasdaq
Andreas Lundell	Nasdaq
Nadezhda Lukasheva	NSD Russia
Dmitrii Zakharov	NSD Russia
Georg Imboden	SIX Securities & Exchanges
Alex Faugeras	SLIB, France
Philippe Juanola	SLIB, France
Tanya Knowles	Strate Pty Ltd
Anne Njoroge	Strate Pty Ltd
Johan Pretorius	Strate Pty Ltd
Charles-Raymond Boniver	SWIFT
Cécile Dessambre	SWIFT
Stephen Lindsay	SWIFT
Jacques Littré	SWIFT