REALISING THE INTERNET OF VALUE

A Multi-Asset Approach to Tokenisation

SETL

WWW.SETL.IO

AUTHORS

Anthony Culligan
Chief Engineer, SETL
Anthony.culligan@setl.io

Marjan Delatinne
Managing Director - Payments, SETL
Marjan.delatinne@setl.io

Dr Joshua Daniel
Director - Payments, SETL
Joshua.daniel@setl.io

Philippe Morel
CEO, SETL
Philippe.morel@setl.io

INTERVIEWEES

Sir David Walker

Chairman, SETL; formerly chairman of Barclays, Morgan Stanley International and Winton and an executive director of the Bank of England

Tony McLauglin

Emerging Payments & Business Development, Treasury & Trade Solutions, Citi

Ryan Marsh

Director Global Head, Distributed Ledger Technology & Digital Innovation, Securities Services, Citi

Henri Arslanian

Crypto Leader, Partner at PwC

Tom Zschach

Chief Innovation Officer, SWIFT

CONTENTS

1	Foreword	01
2	Preface	03
3	Introduction to Tokenisation	06
4	Tokenisation Thesis	08
5	The Topology of Value	10
6	The Technology of Tokens	18
7	Blockchains for The Public?	22
8	The Challenge of Interoperability	27
9	Identity Politics	32
10	A Roadmap	34
11	About SETL	38

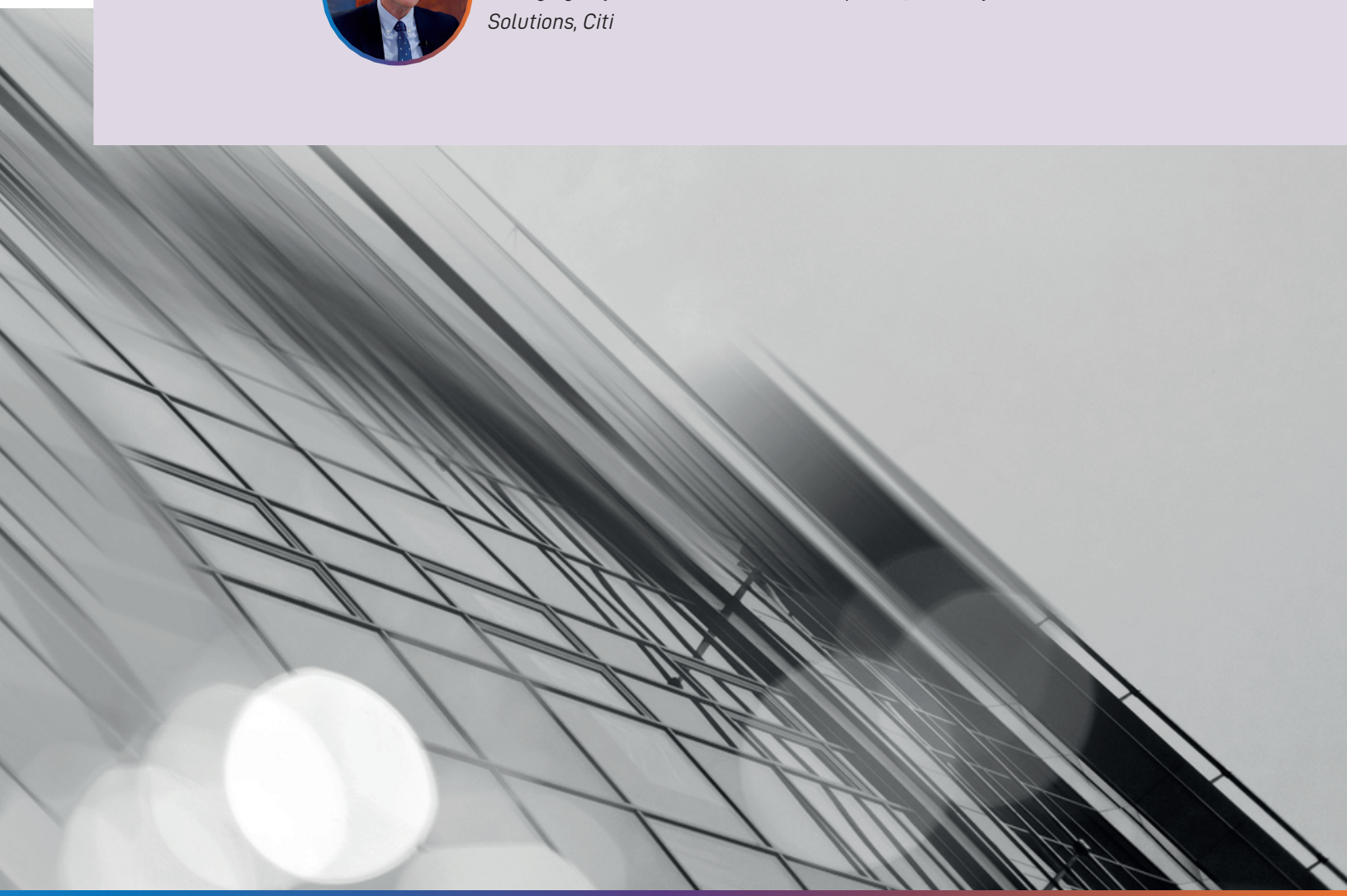
1

FOREWORD

"There is unnecessary confusion around the term 'tokenization'. It just means 'representation' in natural language. We can represent financial instruments with any arbitrary technology, say Lego blocks. Green blocks can be cash, red blocks can be bonds and equities can be yellow. Clearly, we will soon discover the shortcomings of representing financial instruments in physical Lego, so what if we want to utilise the digital domain? In that case it might be interesting to have a common platform that can represent any arbitrary asset. It may be useful to track the ownership of assets through chains of digital signatures using public key cryptography. Furthermore, it may be interesting to have a common programming language that can operate across this general digital asset representation technology. DLT is certainly better than Lego as a means of representing financial instruments. The history of technology is from the specific to the general. If we can develop a general way to represent and administer digital assets on common multi-party platforms, then that may represent a significant advance in financial technology."

Tony McLaughlin

Emerging Payments & Business Development, Treasury & Trade Solutions, Citi



2

PREFACE

The advent of tokenisation heralds the possibility of a new way of owning assets. A financial asset owned by one person is typically a liability of another. Our way of owning something is to pass that liability through a series of ledgers that stand between the issuer and the beneficial owner.

Wouldn't it be great if you could have a single technological layer where you could look at to see your cash and assets positions in real time, always on/24x7 and have them tradeable irrespective of the jurisdiction?

Cryptocurrencies have demonstrated that this is possible. However, for regulated liabilities and assets, the fragmentation of the value chain makes this impossible without tokenisation.

Tokenisation is a construct that allows you to interact with all types of assets and liabilities through a unified approach. DLT provides a secure means to do this, just like how double entry bookkeeping helped secure records on distributed paper-based records. Tokenisation enables a different relationship with 'store of value' and 'transfer of value', thereby enabling you to hold and manage a variety of value irrespective of its form such as CBDC, commercial bank money, e-money, stablecoins and all kinds of monies including a synthetic hegemonic currency if it were to exist.

However, this is not today's reality because appropriate governance and a framework for global compliance is missing. This leaves financial institutions without an ability to join a global public network and benefit from the key attributes of DLT. The regulation needed is not just on managing the technological risks but in helping build a global network that tokenises all kinds of liabilities and at the same time being governed by a transparent and regulated framework with global oversight.

Today's public policy discussion on DLT is limiting the ambition of financial institutions to interact with public blockchains without any exposure to their balance sheet. A shift in global conversation can make public blockchains not just public but also a public good by enabling financial institutions to safely tokenise liabilities on public networks. To this end, tokenisation on a private DLT may be the first step to allow regulators understand this shift while at the same time allowing financial institutions to reap benefits in efficiency and cost reduction in their global operations.

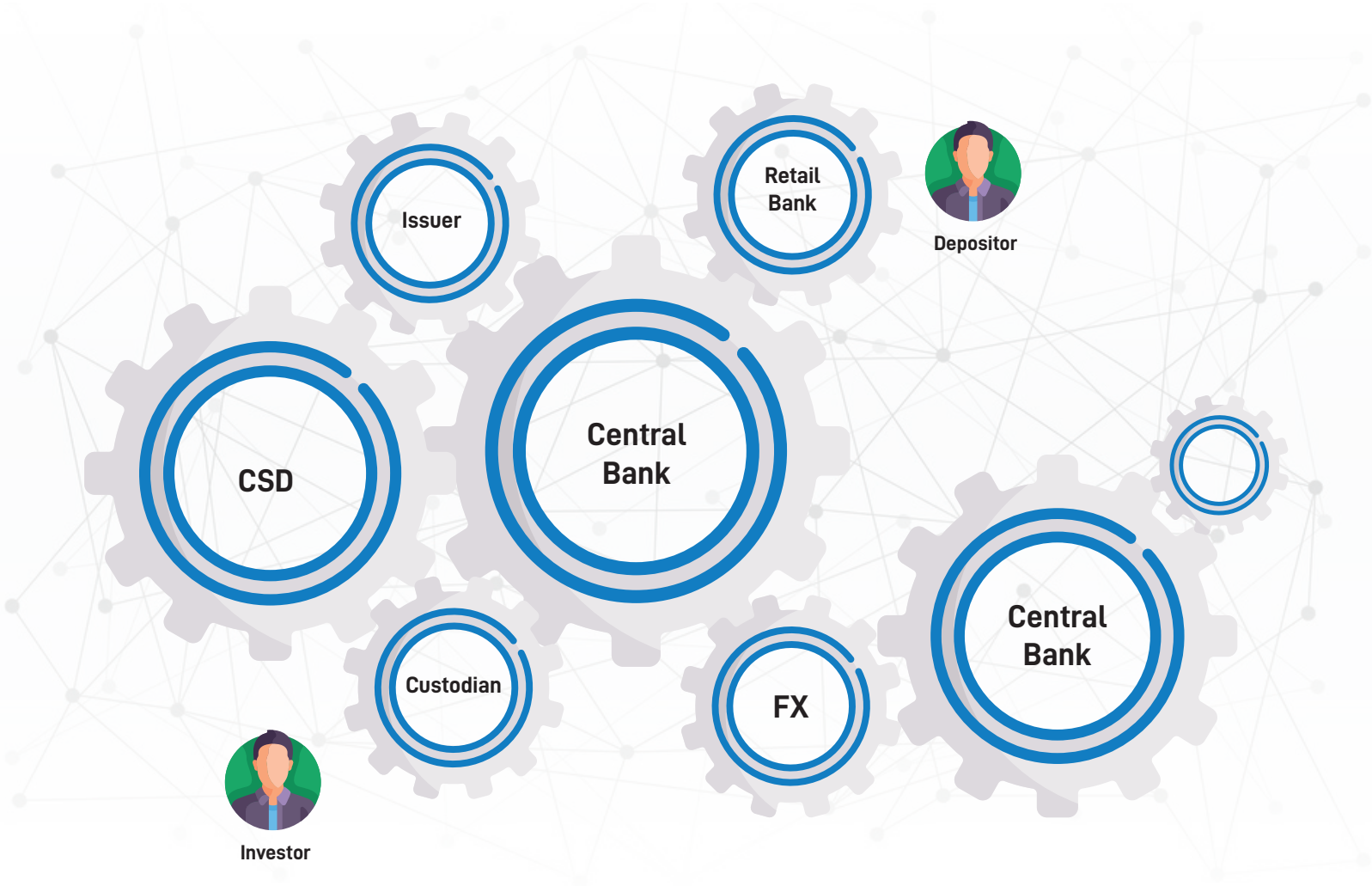
However, we would advocate a more ambitious approach to bringing public blockchains into the regulated space. This is much easier than most imagine. By making 'ledger updating' a regulated activity it would fall immediately into the current regime of AML and sanctions. This may well cause a regulated-fork but it would give financial institutions the ability to innovate and could marginalise bad actors in the space.

Given our concrete experience in tokenisation, and having developed a blueprint for a multi-asset ledger, we are confident that the vision of regulated internet of value is achievable and DLT technology is fitting for this purpose.

The impact of such frictionless finance could give rise to new forms of economic activity in the same way as the internet gave rise to new forms of social interaction. Micro assets, divisions of rights, specialist financing and peer to peer liabilities are all possibilities. As the OECD report [1] observes, tokenisation can improve liquidity and tradability, as it may deliver efficiency gains and bring inclusivity to all sectors of the market by removing the barriers to previously illiquid, unaffordable or insufficiently divisible assets.

[1] https://www.oecd.org/finance/financial-markets-insurance-and-pensions-report.htm

Network of Regulated Liabilities



This paper examines the proposition put forward in Tony McLaughlin's paper 'The Regulated Internet of Value' and considers the practical implications of a generalised approach to tokenisation of regulated liabilities. To map a practical way forward, the paper starts with where we are and looks at the landscape in front of us.

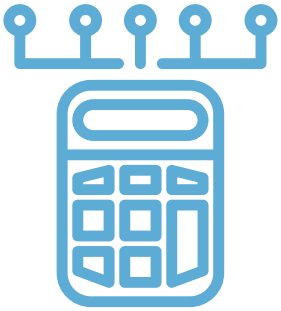
We have, throughout, polled several key influencers to comment on their experience so far and to give their perspectives of the path ahead. Our conclusions are added to theirs and we finish with a number of recommendations and points of guidance for those who have an interest in shaping the outcome in this important transformation.

3

INTRODUCTION TO TOKENISATION

Physical Token

A token is a representation of something else. A chit in a casino is a token representing an amount of money, for example. The token is often not valuable in itself but it can be more convenient to exchange than the thing it represents. Physical tokens have a particular property that makes them useful – they can be exclusively possessed. If a token is in my possession, it cannot be in anyone else's. This allows a very simple scheme for ownership and for the transfer of ownership of the underlying thing – if I possess the token, I own the underlying thing.



Digital Token

The creation of physical tokens turns out to be surprisingly hard to replicate digitally. If I send you a digital token comprising a collection of zeros and ones, it is a copy. You have no way to tell if I kept my copy and will use it in the future to claim ownership of the underlying thing. This is known as 'double spend' in the world of digital money.

To achieve a semblance of a physical token, there must be a place where we can register the existence and transfer of the digital token in a manner which is visible to everyone who has an interest in owning and transacting in that token and the related thing.

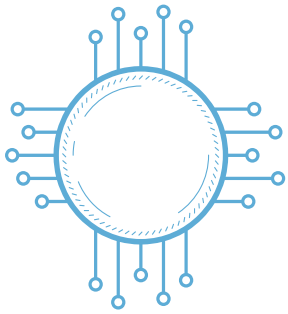
To do this, participants agree on the location of the ledger and how it can be updated.

4

TOKENISATION THESIS

In Tony McLaughlin's thought-provoking piece, 'The Regulated Internet of Value', a thesis emerges that sheds light on a potential path to reconciling the account-based economy with the emerging world of tokens. The paper proposes that, even if it is not obvious to most people, our sense of value is inextricably linked to a network of liabilities, or promises, that are made to us by banks and other organisations. A bank account or a balance with an e-money provider is just that. The role of regulation is to provide some oversight of those promises to promulgate trust – without which a network of liabilities could not scale. This is coupled with a legal system of enforceability that gives substance to those promises.

The thesis then goes on to consider how tokens are evolving and how they differ from regulated liabilities. It identifies two distinct kinds – those that look like liabilities and those that are intangible assets in their own right. In the first category lie stablecoins, bank issued coins and CBDC (Central Bank Digital Currency).



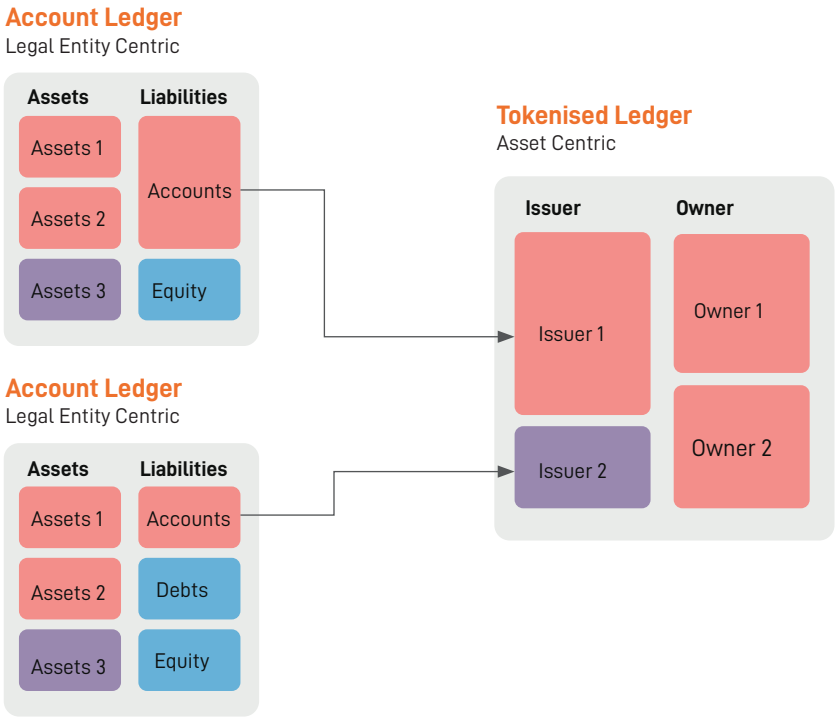
In the second, Bitcoin and Crypto Kitties. At least for the first category, there is a strong case for a unified approach which merges the strengths of regulation (trust and enforceability) with the advantages of emerging token technology – ubiquity, programmability, accessibility and functionality.

At SETL we envisaged this format war as described by Tony in his paper and therefore anticipate the transformation from account based to a token based ledger. We have already demonstrated that a token based multi-asset ledger has the capacity to enable a regulated internet of value from technology perspective.

ACCOUNT vs TOKENISED LEDGERS

Account Ledger

Account ledgers are legal entity centric. They chart all the assets and liabilities of a single legal entity.



Tokenised Ledger

Tokenised ledgers are assets centric. They maintain, for one or more assets, which legal entities are 'issuers' and who are 'owners'.

Single Location for Asset

Users know there is a location where their assets is recorded.

Direct Interaction

Users can interact directly with a token ledger.

Instant Settlement

A single message results in instant settlement.

5

THE TOPOLOGY OF VALUE

A Case for a Broad Approach to Tokenisation

Sir David Walker, points to a problem which is taxing those at Central Banks today.

"A concern for central bankers is that the introduction of CBDC could in itself erode the capability of commercial banks to assess, price and provide credit, which is a key element in our present financial system. Among possible processes and mitigants for consideration is a programme of tokenisation of corporate credit under which, for example, small and medium-sizes businesses might have access to a tokenised credit market comprising a taxonomy of credit types and qualities."

"The development of any new market will require establishment of a framework of trust and, in building this, it may be necessary to develop some form of guarantee scheme in relation to credit tokens. This could be significant in facilitating the development of commercial bank businesses around advisory as well as balance sheet credit products in a CBDC environment."

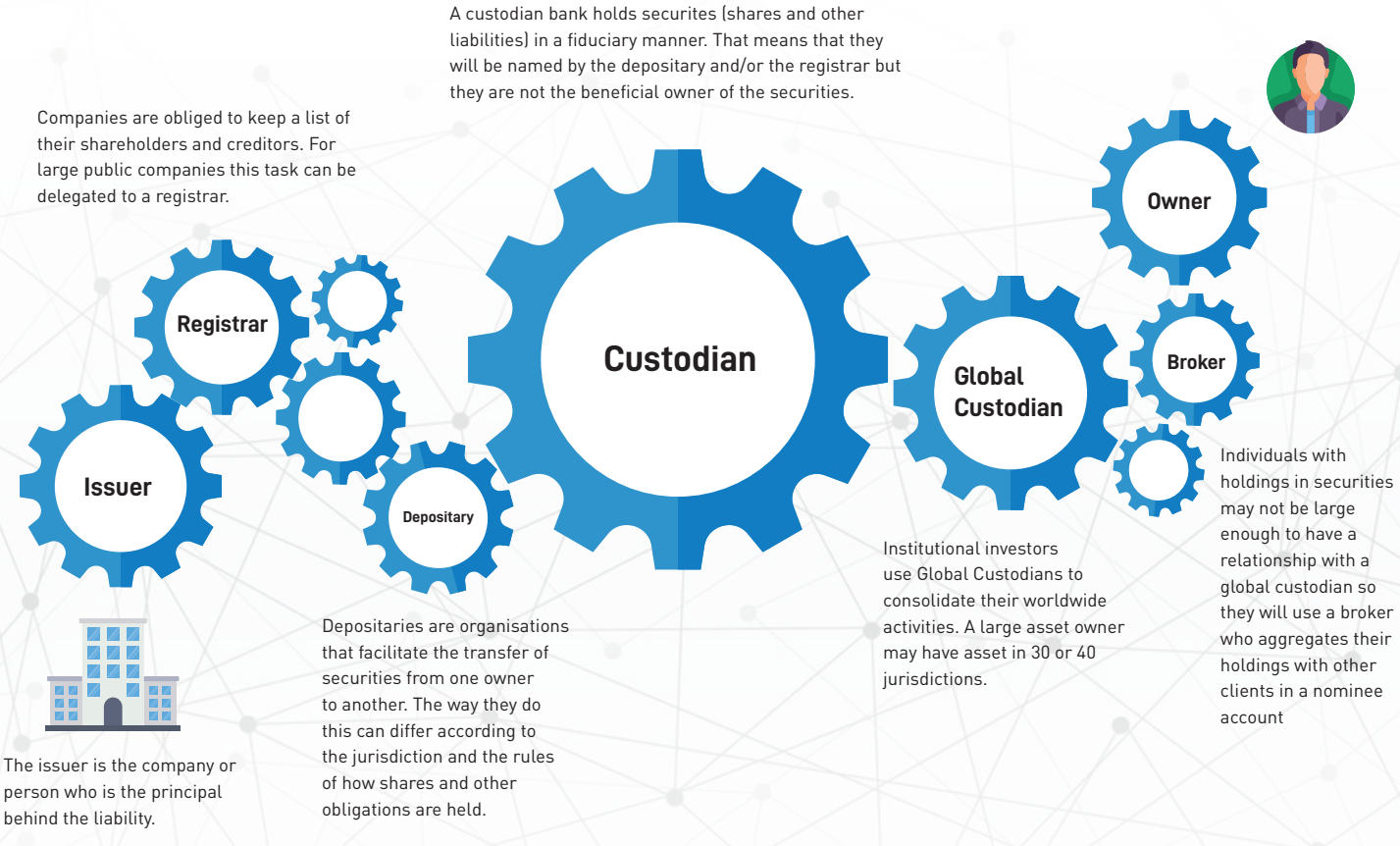
"We also need to be cognisant that the major free-market economies should be driving this innovation. The free movement of capital and developed systems of law and regulation fit well with this kind of digital innovation. It could prove to be very advantageous to open economies vs centrally-managed ones."

Owning a regulated liability

When I own an asset that is a liability of someone else, there can be a long chain of relationships between me and the obligation of the issuer. The intermediaries in that chain can be there for any number of reasons but it is important that, as an owner, I understand that chain and what rights and responsibilities each party in that chain has.

In tokenising regulated liabilities, it is important that the tokenisation does not interfere with the strength of any claim or the process by which the token holder can claim against the liability. Below we describe the two main ways that liabilities are currently held.

Figure 1. Owning a Corporate Liability – A Chain of Custody Between the Issuer and the Owner:

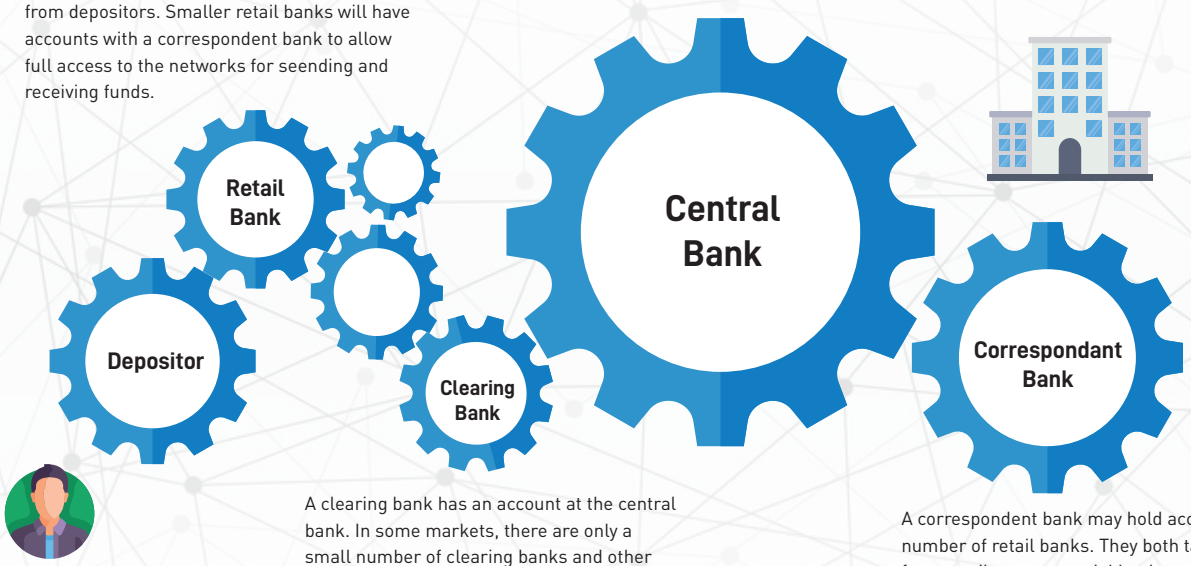


Each element of the chain of custody from the issue to the beneficial owner needs to ensure that the obligations and liabilities of the issuer flow legally to the beneficial owner, however many steps there are in between. The owner needs to understand whether an intermediary has a liability to the owner and, if so, what the nature of that liability is and if it interferes with his claim on the issuer.

Figure 2. Owning Cash – A Chain of Obligations between a commercial bank and a depositor

A central bank is the issuer of money in it's own domain - The Bank of England is the issuer of GBP, the Fed is the issuer of USD. Unlike the chain of custody described above, the depositor does not have a claim on the central bank. Each intermediate entity legally stands between its customers and the next one up the chain.

A retail bank has accounts to accept money from depositors. Smaller retail banks will have accounts with a correspondent bank to allow full access to the networks for seending and receiving funds.



A clearing bank has an account at the central bank. In some markets, there are only a small number of clearing banks and other banks need to have an account at a clearing bank to operate effectively.

A correspondent bank may hold accounts for a number of retail banks. They both take deposits from retail or commercial banks and act as their messenger for sending funds to other banks.

The depositor is like the beneficial owner of securities. However, unlike the beneficial owner there is no legal relationship between the depositor and the central bank - the issuer. Instead the bank makes a promise that it will deliver central bank notes (i.e. cash) on demand.

Regulated Internet of Value:

Understanding The Tokenisation Thesis

The legal structures and regulations that exist within global financial services have been created from the combined and long experiences of the participants – each financial disaster, failure or bankruptcy contributing to a structure that mitigates the effect of any repeat incident. In building a system of tokenisation, it is important that none of this experience is lost or diluted.

With a tokenisation approach, one can imagine a general purpose network where participants can assert a promise into the network or become the beneficiary of another's promise with instantaneous effect.

To understand the necessary ingredients of the tokenisation thesis, let us break it down into a set of problem statements that it must address:

Problem 1: Investor safety is ensured when there are clear records of ownership supported by legal frameworks that have been reliably tested. Safety drives investor confidence, which is a necessary foundation for growth in markets.

This fundamental need for safety has meant there is a stark difference in one's relationship with money in comparison to assets. The chain, that connects you with an issuer as **illustrated in Figure 2**, is a cross section of an individual's value map in a world of many such individuals.

A transfer of ownership of an asset or cash, therefore, requires each of the entities in the chain of value to interact all the way up the chain. An investor is free to choose a bank or a broker of their choice and hence to speed up the process of transfer of value each type of liability has its own settlement infrastructures to reflect the change. Such a network of value exists today and is complex. The complexity grows when you factor in a variety of assets that would have been issued across a range of jurisdictions that an investor may hold.

Need 1: Creating a single view of state of net value held by an individual across the globe. A single place to instruct the transfer of asset or cash.

Solution 1: Tokenisation creates a common technical infrastructure that connects an issuer with a holder through a record. The various entities in the chain of value can all be recorded and linked directly on a tokenisation ledger. This simplifies the process of drawing up a balance sheet and instead the tokenisation ledger can provide a realtime view of their net value without needing to synchronise across the intermediaries.

Problem 2: To enable safe exchange of value - transfer of assets and payments needs to be synchronised. The construct of a DVP or a PVP ensures settlement finality as is defined by law. However, a DVP across jurisdictions can have exposure to Herstatt risk or a PVP across jurisdictions can be exposed to settlement risk, this is purely due to the difference in the definition of settlement finality in each jurisdiction.

Need 2: Being able to carry out a DVP or a PVP on the same ledger can alleviate this risk with atomic settlement

Solution 2: A DLT based tokenisation platform provides Atomic settlement. DLT platforms that enable synchronised state management enables this via the form of smart contracts. A DVP or a PVP implemented using a smart contract can execute simultaneously without any such settlement risk. SETL has demonstrated this with their experiment with the Banque de France to purchase and redeem fund units with cash on the same ledger.

Problem 3: Every asset and liability has a siloed existence today. This makes innovation very cumbersome and inefficient especially when settling complex or multi-asset trades. A healthy market requires an ability to support novel instruments and maintain liquidity.

Need 3: To break the siloed model of asset lifecycle management and support multi-asset interface that is programmable. Programmability helps one create asset or client specific workflows to automate lifecycle of complex and novel activities.

Solution 3: A DLT based smart contract is also extensible to allow for a multi-asset multi-party DVP/PVP to be executed simultaneously. With smart contracts orderbook, trade, exchange applications can plug into a single common ledger and complex orders executed involving multiple assets and cash.

A clear record of ownership also allows for client servicing activities to be carried out on the DLT ledger in an automated manner. These can include dividend delivery, stock split or an interest payment on deposit/ CBDC.

Problem 4: Ensuring market safety is the responsibility of market regulators. They ensure open and efficient markets while preventing any illicit activity. This need however has caused siloed distribution of assets and liabilities into various markets across jurisdictions, thereby creation liquidity fragmentation. A healthy and vibrant market needs to pool all the liquidity it can.

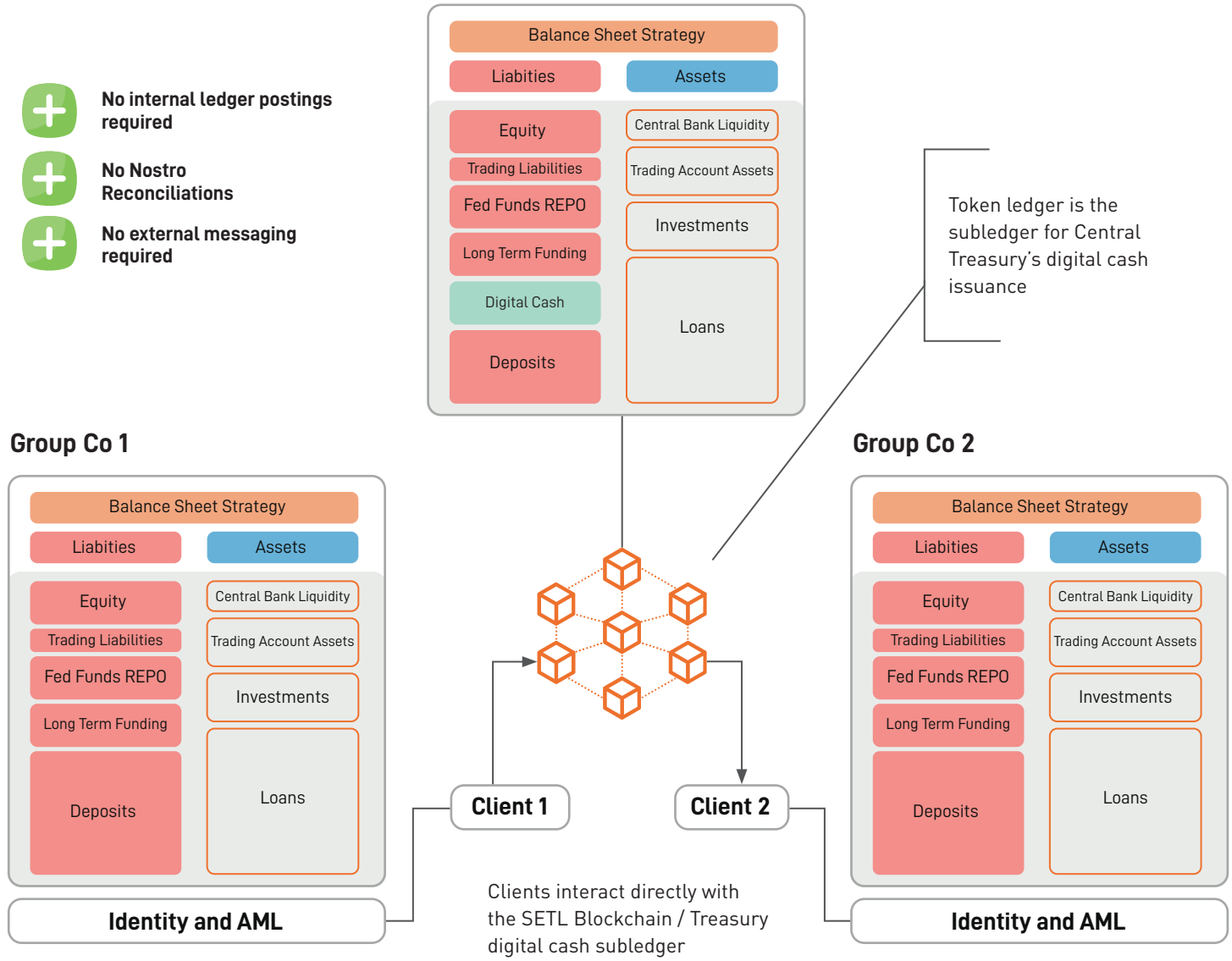
Need 4: Just as CLS has created a safe way to execute PVP for FX transactions safely for 18 currencies, an equivalent is required to enable a global multi-asset multi-liability ledger. This technical infrastructure needs to support multiple assets and liability with DVP or PVP, irrespective of their jurisdiction.

Solution 4: Tokenisation on DLT infrastructure allows creation of a common technical ledger infrastructure on which multiple issuers can issue assets and liabilities irrespective of their jurisdiction. Therefore, with an appropriate governance of the issuers on their use of the ledger, a global multi-asset multi-liability ledger can be a reality. A DLT based tokenisation ledger would also provide the ability to assure the integrity and availability of the infrastructure without disruption from cyber threats while adhering to any data residency requirements. Combined with the advances in digital identity such as verifiable credentials, both KYC and AML requirements relating to the jurisdiction of the issuer can also be ensured and audited.

Building the Regulated Internet of Value

At SETL we have developed a blueprint to enable a regulated internet of value in collaboration with key market participants and infrastructures. We have also been busy building evidence to showcase that such an infrastructure can exist today and deliver a better client experience globally, as demonstrated most recently in the publicly published experiment with Banque de France in collaboration with Citi on a live DLT infrastructure.

To understand how we can build a regulated internet of value on a tokenised multi-asset ledger, we must begin by looking at the balance sheet of the issuer. A balance sheet is structured to have liabilities represented on one side and assets to the other, while on a tokenisation ledger, it is the issuer liability that is represented on one side and the holder on the other side.



Therefore, a tokenisation infrastructure must have two primary roles, firstly that of an issuer and secondly of a holder. The tokenisation process is the reflection of the liabilities of an issuer onto the ledger. When the issuer is a regulated institution, the tokens then represent a regulated value on the ledger.

Since the ledger itself is agnostic to what is being issued, a variety of regulated tokens can co-exist. An issuer can tokenise multiple liabilities as separate tokens e.g. CBDC, commercial bank money, e-money, stablecoin and other assets. The multi-asset ledger also supports issuers in creating tokens of assets (e.g. securities, NFT, land).

Such a ledger will allow a holder to concurrently own multiple tokens, be they liability or asset based tokens. Every holder and issuer are uniquely identified by the globally unique cryptographic signature (backed by a public-private key) on the multi-asset ledger.

Whilst it is likely that the issuer will still be required to hold the records of its holders, the multi-asset ledger allows for the issuers to use this tokenisation ledger as a unifying golden source of record that is kept up to date in real time. Therefore, the ledger would allow for any transfer or exchange of liabilities and assets to be settled directly on the same multi-asset ledger 24x7 and 365 days a year.

This model removes the need for double-entry book keeping and alleviates the need for nostro-vostro reconciliation and internal ledger postings. Pooling of assets and liabilities onto a common ledger improves the liquidity with dynamic liquidity allocation from multiple issuers by breaking the siloes and providing a common infrastructure for record keeping and settlement.

6

THE TECHNOLOGY OF TOKENS

New Tech Leads to New Opportunities

Ryan Marsh, Global Head of DLT and Digital Innovation, Securities Services at Citi is potentially at the epicentre of a securities tokenisation trend.

"We have always been a client-centric organisation. Part of that is anticipating our clients' needs in the face of accelerating technical change and tokenisation is the result of fast-emerging new technology. We see three pillars all evolving independently but which are complementary to one another, 1: digital infrastructure and networks, 2: digital assets, and 3: digital forms of payment.

While the technology has broadly given rise to new forms of assets such as cryptocurrencies, it can also be used to create digital representations of existing assets. Digitization can also lead to fractionalisation of physical assets such as hotels and office blocks.

"The technology allows for a more granular approach to ownership which would not be practical without the automation that it brings. That is, not only splitting by value but splitting assets into their constituent rights such as coupons and principal or dividends and voting.

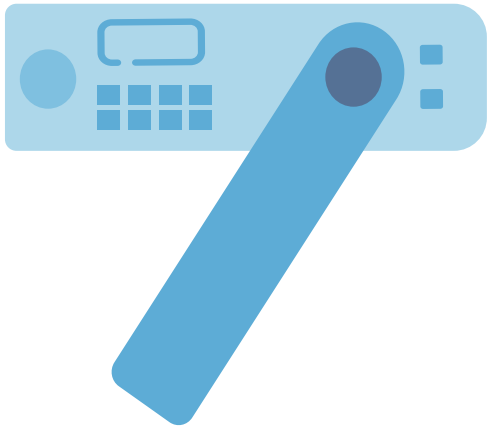
Dividing assets in this way can allow the component rights to be transferred separately without impacting the integrity of the instrument itself.

"For a complex and large organisation like Citi there are many things to consider. When launching a new product or service we undertake a huge amount of due diligence to ensure that we understand and manage the various risks. Forward thinking traditional banks such as Citi are going through this analysis with regard to digital assets right now."

On public blockchains, Ryan comments, "They are establishing themselves as alternative financial infrastructure. Some features of these networks, such as distributed decision making, pose practical and legal challenges for firms operating within regulated, centralised networks and these are elements that must be considered carefully as part of a firm's due diligence."

The Ledger

One of the powerful elements of tokenisation is that it establishes different norms to the prevailing topology of liabilities. A company ledger is legal entity centric while a token ledger is asset centric. It need not be a legal entity at all but simply a collection of issuers on one side (assets) and owners on the other (liabilities). Blockchain ledgers are typically distributed copies of a single source of truth. That is to say, they exist on multiple servers which all record an identical copy of a state.



A way of Asserting to the Ledger

A global distributed ledger can have multiple points of ingress. It is the ledger technology which ensures that transactions asserted anywhere on the network are corralled and applied in a consistent way everywhere. The ledger tech makes sure each copy of the ledger has identical discrete states and identical transformations.

The Rules of Acceptance

Each ledger should have rules of acceptance. Typically a transaction must be signed by parties who have authority to move tokens.

Smart Contracts and Flows

Another powerful feature of tokenisation is the separation of token balance from functionality. Tokens are typically simple things – a token name, a token balance and ticker symbol, for example.

There are two ways that the lifecycle of a token can be managed. A smart contract is functionality which exists on the ledger and can be referenced as part of the process of moving from state to state. For example, a smart contract could increase token balances automatically with each state to reflect interest payments. This can be a wasteful way to do things if you have thousands of tokens all requiring the same treatment.

A flow is code outside of the ledger that acts upon a ledger. It is more like an automated agent. A flow can more easily interact with data and functionality outside of the ledger – for example a flow can be used to create interoperability with SWIFT messaging systems.

The Elusive Decentralized System of Tokens

Since blockchain has become a theme in financial services, there has been a hint that tokens could be moved between owners without there being a common reference ledger. Somehow, I should be able to pass you a digital token which you could pass to someone else and tokens could circulate freely in a completely decentralised way.

It is a tempting vision because it mimics physical tokens. It is ultimately made impractical by the double spending problem. When public blockchain systems talk about being 'decentralised' it still relies upon a common ledger – what is decentralised is the storing of that ledger – i.e. there is no single server where the ledger is kept. Second, as we discuss below, the decision making on how to move from one ledger state to another can be structured so as not be in the hands of a single party – i.e. decision making is decentralised.

7

BLOCKCHAINS FOR THE PUBLIC?

Regulated vs Unregulated

The prevailing distinction between a public and private blockchains rests in who has the right to move the ledger from one state to another. In a private blockchain, that function is undertaken by appointed parties who control access to the blockchain. A public blockchain is open to all to use. Movements on the ledger are typically controlled and approved by members of the public using some kind of proof of work mechanism, or voting open to individuals or entities 'staking' their ledger-native tokens.

The attraction of the public model is that it appears to provide a sense of directness and fairness. Any participant can be a user and part of the decision-making group as well. The issue with this approach, however, is that it does not fit within the regulated system of liabilities. Oversight by regulators benefits the public as a whole by, for example, ensuring that companies keep sufficient assets aside to meet their promises. Regulators have authority to intervene if activities are for criminal or terrorist purposes. This approach can carry across easily in a private blockchain and, though it requires more thought for public blockchains, we can envisage that this could be achievable.

In fact, large public blockchains are often controlled by a small number of private entities. Taking Bitcoin as an example, there are fewer than a dozen organisations that, between them, actually define the rules of Bitcoin and keep the ledger of who owns Bitcoin. They literally, between themselves, could freeze accounts, refuse transactions and even change balances. They are identifiable commercial operations with owners and directors who are as susceptible to regulation as any bank or company.

Refusing transactions, moreover, is entirely consistent with the Bitcoin scheme. When a miner wins the right to add a block of transactions to the ledger, there is nothing in the protocol which defines which transactions he must or must not include. When a user submits a transaction, they can include a higher than normal fee to incentivise a miner to include their transaction. Miners could equally be motivated not to include certain transactions by interested regulators or law enforcement organisations.

Finally, the rules of Bitcoin and other cryptocurrencies were not passed from the heavens. Nor are they constant. They are really in the hands of the private entities which in practice control them. There are any number of ways that national or supra national authorities could involve themselves in the protocols of ledger updates. There is certainly no technical, moral or philosophical bar to their involvement.

So why are public blockchains growing in popularity? If the analysis above is correct, users are embracing systems where they have fewer protections. There are, no doubt, some who actually use the lacunas in oversight to avoid scrutiny but, for most, it boils down to utility. Public blockchains have the following attractive characteristics.

Attractive Attributes of Public Non-Regulated Blockchains

Instant and permissionless wallets

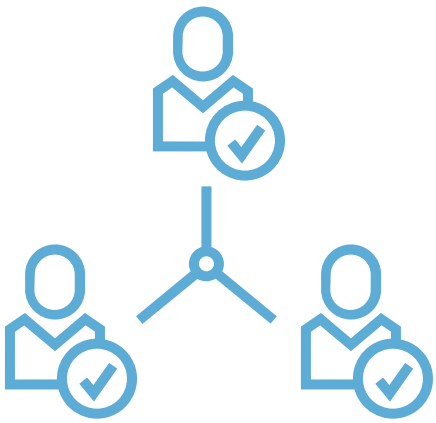
It is easy and permissionless to open an account. An account on a public blockchain is simply a wallet which contains cryptographic keys and has the functionality to sign things. I can download software from the internet, set up an online wallet or buy a hardware wallet. There are no forms, no ID, and the process can be completed in seconds.

Having an account allows you to interact with ledgers – it does not give you any money or assets. The equivalent in traditional banking would be like buying a Visa card or MasterCard card before you chose your bank.

Crucially, you own your wallet and your accounts – they are not the property of the blockchain or the bank.

Always on Everywhere

As Henri Arslanian commented, 'My bank does not process international payments on a Sunday. Why? It's not like the payment system has to go to church!' Public blockchains are always on. They are robust, resistant to attack and reliable in their operation.



The Same Process for Everything

Once you get up the learning curve – which can require a rethink of some basic processes you might be used to – the blockchain approach is pretty much the same regardless of what asset or token you are working with. You use your wallet to sign some action into the ledger and watch it happen.

Not So Attractive Attributes of Public Blockchains

Having said that, public blockchains can alarm experienced regulators – and for good reason, as we list below. Regulators are adept at spotting schemes which conceal risks behind ease of use. Every generation is subjected to schemes which take advantage of a lack of knowledge or understanding. Regulators are there to both inform and protect the consumer – a service which creates trust and expands the capital markets.

Promises, Promises

A token is a promise. It is not 'the thing', but it is instead a promise of 'the thing'. A liability is a promise of a thing. Promises are the lifeblood of any modern economy. Everything from supply chains to mortgages depend upon society being able to judge the worth of a promise. We all do it tens (if not hundreds) of times a day. We rely upon a communal trust framework comprising brands, laws and regulators because we do not have the time to individually evaluate every trust decision we need to make.

A promise made on a public blockchain can benefit from the communal trust framework but not submit to the rules that support it. Those rules include the regular audits, capital requirements and regulatory registration.

Legal Uncertainty

Many contracts and tokens on public blockchains are poorly documented or have no documentation at all. Without specific agreements in place, it is hard to know how to exercise rights or litigate disputes.

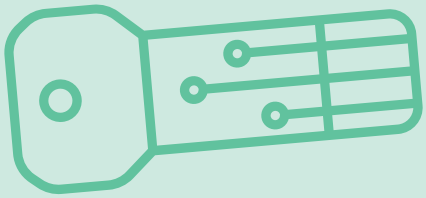
Lose My Key, Lose My Asset

The question that everyone should ask before they participate in a public blockchain is 'What happens if I lose my private key?' Mostly the answer will be 'Don't, because you will lose your asset'. This creates an unworkable conflict in that I need my private key to be accessible to do transactions, but I need it to be protected from loss or theft, the consequences of which are catastrophic.

The situation is exacerbated by custody arrangements. A class of digital custodians are emerging with business models predicated on looking after private keys. These arrangements rely upon technical solutions that use both hardware and software to reduce the probability of loss or theft.

The problem is the liability. Banks have used HSM's for years to protect their private keys used in signing SWIFT instructions. The main purpose of this is to ensure the integrity of their instructions. To elevate the use of this kind of technology to the point where the loss of a key would result in the loss of an asset is to put it into a completely different risk framework. Making a promise to customers that you will keep their keys safe is the same as standing as principle and creates a contingent liability on your balance sheet. In the world of regulated liabilities this necessitates capital.

Ownership, Possession and Private Keys



In a modern replay of John Locke, you can ask 'when do I actually own a Bitcoin?' John Locke's labour theory of property chimes well with the Bitcoin proof of work. Where public blockchains diverge from his and other theories of property is that they do not distinguish between possession and ownership. Private keys are a means of possession not ownership. Ownership is a legitimate recognition that a person has a right to possession. Ownership passes by some form of conveyance that is generally wilful on the part of the existing and prospective owners.

High profile ransomware attacks are a case in point. It is public and obvious that possession of Bitcoin has changed from the victim to the perpetrator. However, even if every participant in a public blockchain, including those participating in consensus, knows this and recognises the rightful owner, there is no mechanism in the protocol for them to restore possession to the rightful owner. In reality, public blockchains are possession ledgers, not ownership ledgers.

Private blockchains with identifiable parties responsible for evolving the ledger can more effectively maintain ownership ledgers. Ownership and the mechanisms for changing ownership are at the heart of financial services. On a private blockchain, the ledger proves ownership, and the private key is the mechanism by which an owner exercises their right of possession.

Bad Actors

The perceived lack of regulation and the pseudo anonymity offered by public blockchains attracts bad actors. Every transaction and money system has some element of vulnerability to bad actors. Public blockchains, however, offer little functionality to mitigate their involvement.

The Best of Both Worlds?

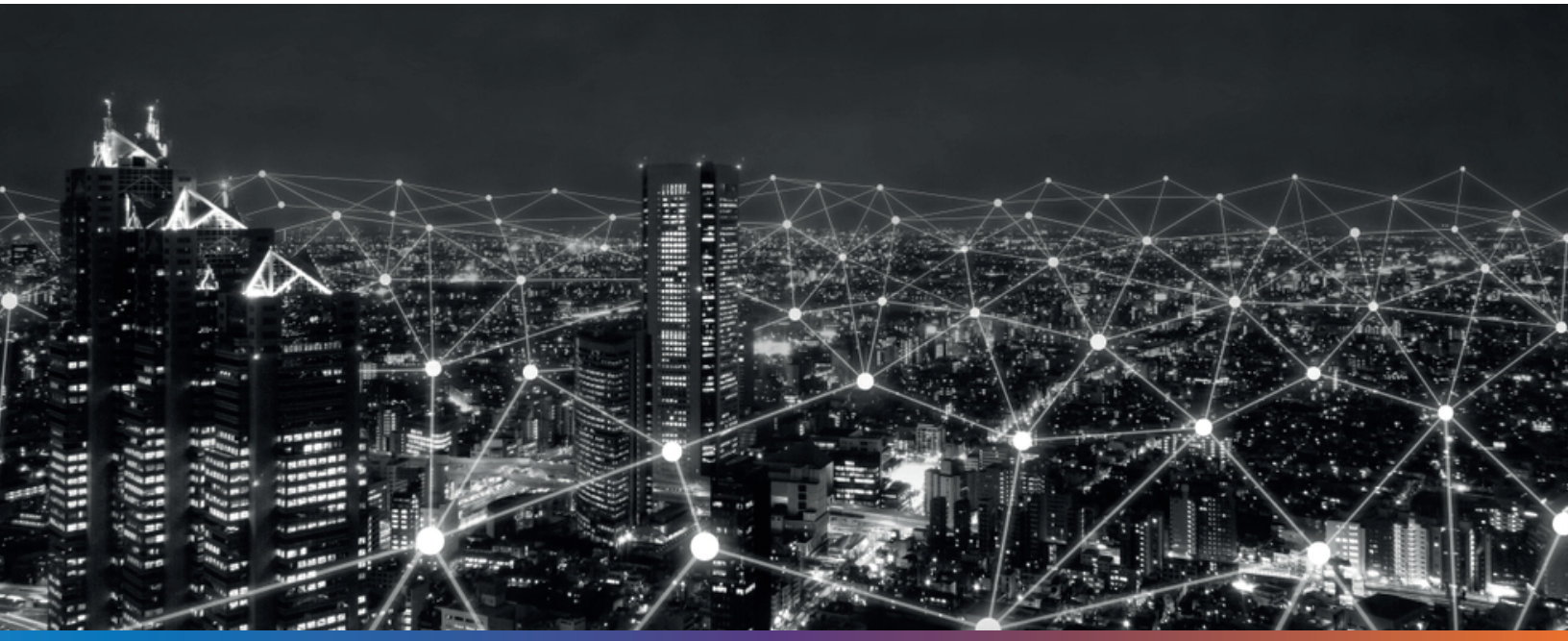
So, could the utility of public unregulated blockchains exist within a framework that offers the same good governance as private blockchain? It would seem there are a number routes:

- Find a way to create a new global network which is accessible to everyone and is subject to some form of acceptable governance
- Steer the public blockchains into a more acceptable form of governance
- Encourage and enable private companies to innovate in a way that realistically competes with the public blockchain model

All options face some significant challenges. Common to the first two is a need to define a governance model – a non-trivial international effort. The third option is typically how markets respond and there is continuous evidence that this process is underway. FinTechs are successful when they attract users through a better experience.

Successful private innovation which can compete with the ubiquity of public blockchains, however, will need a level playing field and some standards to allow them to interoperate. The level playing field requires regulators to take a thoughtful approach to the innovation that is happening in unregulated blockchains and to find ways to ensure that regulated firms are not unduly excluded from new technology and new approaches.

Standards are also likely to play a big part in private innovation. Where private initiatives lack a central planning authority, they can flourish with interoperability. Interoperability is based on standards – but that is not the whole story as we discuss below.



8

THE CHALLENGE OF INTEROPERABLITY

If we want to implement a general scheme of tokenised regulated liabilities, there will be a need for parties and systems to be interoperable. We discuss, below, the challenges of having various blockchains interoperate but also the need for regulatory and legal harmonisation.

The Will

As Henri Arslanian observes, "The difficult element of interoperability is not the technology, it's the geo-politics. Moving to a common platform involves giving up some element of control - and that is not an easy thing for nation states nor for their central banks."

This is a perennial issue. Money is ultimately linked to the norms and politics of a state. Exchange controls, for example, have often been used to pursue a particular local policy which could be undermined by large capital inflows or outflows. Long standing trade imbalances can be the result of restrictive policies which inhibit equilibriums that might otherwise have been reached. Both of these scenarios make interoperability practically difficult.

The Way

Assuming the will exists, interoperability is a networking problem. Sir David Walker notes, "A token system that cannot effectively interoperate is like a telephone company that won't let you call the customers of other telephone companies." So how is interoperability achieved?

Standards

Financial services have successfully embraced technology standards for many decades because there is such a direct link between standards and operational efficiency. SWIFT has been pivotal to the adoption of message standards, but they have also provided a lot more to their members over that time. In particular, they initially provided physical infrastructure before the internet, and they continue to provide a Public Key Infrastructure (PKI) that allows banks to reliably identify the source of any message they receive via SWIFT. More lately they are the body responsible under ISO for the curation of the ISO20022 standard of messaging – the next generation of financial messaging standards.

Evolving standards and interoperability is a complex task in the face of continuous innovation. Backwards compatibility is key to interoperability in financial services. Not all participants move at the same speed, so they must be able to operate during complex transitions. Tokenisation therefore will need to be a staged process with clear governance to support such innovation at scale.

The community model has worked well so far in finance. Taking CLS as an example, they have accounts at 18 central banks and are overseen by the G20. It is laudable that stable coins such as USDC are now turning over $25bn a day, but CLS today settles $6trillion a day with its membership model.

The blockchain industry is no stranger to the benefit of standards. Tokens issued on the Ethereum public blockchain quickly coalesced around the ERC20 standard [2]. This standard determined that a token should have 9 specific functions that could be called and would produce 2 standard events. The standard determines the name and parameters of each function but leaves the implementation to the author (ref Appendix 1).

Since then, other token standards (such as ERC721 for Non Fungible Tokens) have emerged.

The definition of these standards allowed developers to build wallets which would work with those standard tokens and for token exchanges to emerge which allowed users to give the exchange permission to move tokens to settle trades.

Whilst the ERC20 and ERC721 standards are an interesting start, they are several orders of magnitude away from what is required for a truly functional institutional token market. The scale of a financial services standardisation project can be observed by looking at the ISO20022 standard and ISDA's Common Domain Model for derivatives. Both define an important common language in their specific areas covering everything from simple account details to complex event servicing.

The challenge for the blockchain industry, if it wants to create interoperability between technologies and with existing institutions, is to leverage the significant effort which has gone into these two projects and others in financial services. Reinventing the wheel is unlikely to be productive.

[2] The ERC20 standard

```
function name() public view returns (string)
function symbol() public view returns (string)
function decimals() public view returns (uint8)
function totalSupply() public view returns (uint256)
function balanceOf(address _owner) public view returns (uint256 balance)
function transfer(address _to, uint256 _value) public returns (bool success)
function transferFrom(address _from, address _to, uint256 _value) public returns (bool success)
function approve(address _spender, uint256 _value) public returns (bool success)
function allowance(address _owner, address _spender) public view returns (uint256 remaining)

event Transfer(address indexed _from, address indexed _to, uint256 _value)
event Approval(address indexed _owner, address indexed _spender, uint256 _value)
```

Layering and Frameworks

On a technology level, the discourse in the blockchain world has been 'my blockchain is better than yours'. Whilst each technology boasts some unique features, they often share the same basic building blocks – e.g. cryptographically signed assertions and discrete states built around Merkle trees.

What has emerged from the first few years of testing, implementing and experimenting has been a collection of blockchains in production and a number embedded within innovation labs. It does not look like there will be a 'winner takes all' technology – nor would that be normal in a highly innovative environment. This has led to a demand for products which can simplify the process of access across and between different blockchain technologies.

The challenge in this area is to simplify the approach for the user while not obscuring the underlying technology. In particular, abstracting too much could result in valuable features and innovation at the blockchain layer being inaccessible to the user.

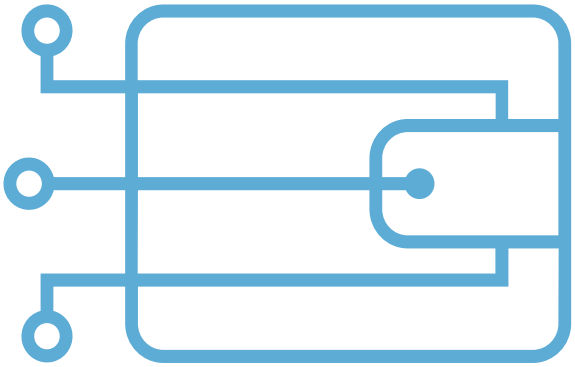
Users, Wallets, Keys and Nodes

One of the challenges of interoperating is projecting consistent permissions across different blockchain technologies. Permissions in institutional finance are complex. A legal entity can have multiple accounts and relationships, and there may be multiple people within and outside of that legal entity that have limited authority to act on behalf of that legal entity – managers, administrators and custodians, for example.

Different blockchains take different approaches to this. Some equate a legal entity to a full node while some have no particular structure other than a key pair being a permissioning entity. The concept of a 'wallet' as a collection of keys introduces a hierarchy or identity above the key level – but what does a corporate wallet look like?

Similarly, blockchain frameworks can take different approaches to trust boundaries. Some take a fundamentalist approach that privacy is defined by a security boundary – i.e. data is only private if it is on a computer within my security boundary – excluding the possibility that I may have private data held in trust.

A coherent interoperability scheme needs first to address how to manage a corporate identity across these different technology approaches. Simplistic approaches that just present a 'party' to a transaction will run out of steam in real applications.



Simultaneous Settlement

When financial institutions undertake large transactions involving an exchange of assets it is important that both sides of that transaction settle simultaneously. This is because of the risk that one of parties to the transaction may declare insolvency. In such a case, if only one half of the transaction is complete, the liquidator of the insolvent party owns what they have received but may default on what they have not paid – famously demonstrated in the bankruptcy of the Herstatt Bank.

This problem breaks down into two related elements – legal and technical. The most important is that this is a legal exposure. The risk derives from what a liquidator can and cannot do legally in an insolvency. The legal solution is settlement finality. Each jurisdiction defines the rules that bind the liquidator. Those rules are extremely specific as to when a trade is settled and when it is not. A useful reference point in time is when a particular ledger is updated – which is where the technical element comes in.

What happens when one side of the trade is on one ledger and the other on a different ledger. In the case of Herstatt Bank, Deutschmarks were recorded at the Bundesbank while US Dollars were on a Fed ledger. Each jurisdiction having its own definition of settlement finality meant that it was possible for the bank to fail after the Deutschmark were finally settled but before the Dollars were finally settled.

The solution is (and was in response to Herstatt) that such trades should be structured to take place in a way made settlement finality simultaneous – leading to the creation of CLS. Participants in CLS deliver their element of the trade to CLS but finality only happens when the book entries for both transactions are made in CLS. For this to work, it needs each participating jurisdiction to reference the same event as the legal point that the two transfers become irrevocable by a liquidator. It is in this final point that the complexity of CLS is to be admired.

This points to how blockchain simultaneous settlement needs to work. In particular, two co-operating blockchains need to generate a single event which can be referenced to be legal finality for both. What's more, that needs to either in a single jurisdiction or be subject to the same kind of multi-jurisdictional regime that CLS has implemented.

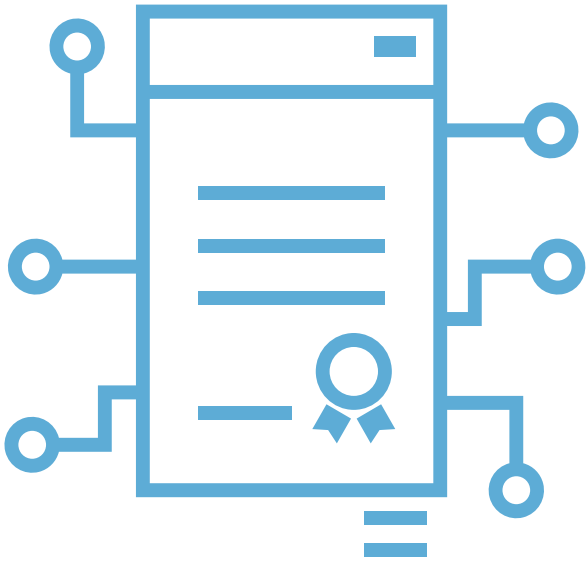
The technology surrounding this is important but secondary. Essentially it needs to stop either one of the participants having access to both sides of the trade at the same time.

9

IDENTITY POLITICS

Owning liabilities through tokens is dependent upon our having a reliable way of connecting a public key to a person. The benefit of digitisation cannot be fully realised if identity remains paper-based.

The major divergence between public and private blockchains is their approach to identity. Public blockchains seek to divorce identity from transactions. This is because transactions are public, so privacy depends upon the public not being able to tie a specific key to a real person or company. The current legal environment poses a challenge to public blockchains. Money laundering rules require those who maintain ledgers to proactively identify transactions and participants that might be related to criminal activity and make reports to the regulator. Second, operators of nodes of public blockchains will need to comply with data protection regulations. These include strict provisions of where they can store and send data, the right to be forgotten and the obligation to keep people's data private. The fact that these provisions are antithetical to the scheme of public blockchains is not a valid defence.



In private blockchains, the ledger is not on public view, so a different approach is possible. Private blockchains can choose where to store data, can insist on strong KYC and identity checking and can maintain schemes of privacy that are compliant with legislation.

One area of promising intersection is in verifiable credentials. Verifiable credentials are portable cryptographic certificates which attest to a fact, right or qualification relating to a person or a company. The certificate can be stored privately by the subject and presented to a verifier in a completely private peer to peer interaction.

To check the signatures on each certificate, a verifier needs a source of public keys. Public blockchains are being used as storage for of public keys. The keys are part of a distributed identity record (DiD) which gives basic information about the identity of the organisation that controls an associated private key. DiDs need to be easily available to verifiers so that they can check the signatures on the private assertions they receive from credentials holders. Public blockchains can be effective in this case.

As the BIS paper [3] has noted, the most promising design for general use is a CBDC built on a digital identity scheme, safeguarding data privacy while offering protection against illicit activity and potentially streamlining cross-border payments. We consider that the same is also necessary for a multi-asset tokenisation ledger.

The use cases for verifiable credentials are many. In particular, they can make client onboarding and KYC much more automated, as a client can use the same digital credential many times rather than having to continually present paper documentation.

[3] https://www.bis.org/publ/arpdf/ar2021e3.htm

10

A ROADMAP

A map is what helps you get from where you are to a destination. Crucially, unless you have Star Trek technology, you don't just materialise at the end of your journey. Having considered the current position, the state of our tokenisation technology and what is required on interoperability, the following is a possible route that gets us from our account based approach to a system of tokenised regulated liabilities.

Understand the landscape

Tokenisation is an emerging theme. Understanding why and where it is emerging is essential to creating a viable strategy. Consumers are becoming accustomed to instant settlement of everything. Instant messages, instant sharing and instant payments are part of the new culture. The internet provides the means for directly interacting with ownership ledgers. Looking at where and how this is evolving gives clues about how it will become mainstream.

Identify the liabilities that present the best opportunities

The essence of the internet of value is that it connects people to liabilities – making them the beneficiaries. Tokenisation makes these liabilities more generic in form and more instantly transferable between beneficiaries. Consider the benefits of this global accessibility. The mechanisms of distribution can dramatically impact the nature of what is being distributed – think of what YouTube has done to the suppliers and consumers of media.

Anticipate New Risks

Financial services regulations are often the result of market failures or bad practices. The purpose of regulation is to create an environment where trust is scalable. New systems can introduce new hazards and provide opportunities for bad actors. Key management where key loss results in asset loss is an example of a new risk.

Solve for Identity and Credentials

Crucial to ledgers of ownership is a reliable system of identity, permissions and credentials. Tokenisation uses public/private keys to assert changes but ownership requires a way of connecting those keys to a person or company. Such a system needs to be digital so it can be deployed alongside online global ledgers. Verifiable credentials systems have many of the characteristics which would meet these needs.

Consider how investors will interface with a tokenised ledger

Part of the benefit of tokenisation is the harmonisation around the concept of a wallet. A wallet is a software component that stores and deploys keys to digitally sign actions. Wallets are emerging in consumer contexts and they have very close parallels in some corporate settings – such as the way SWIFT members manage and deploys keys. It is likely that a wallet will become a more universal concept.

Benchmark solutions against regulatory environments

Don't assume that new technologies are somehow immune from current regulations. Anonymity on a blockchain is just as hazardous as anonymity in banking or money transfers. Look closely at data protection regulations and consider how your organisation might be exposed. Look out for solutions that publicise transaction details as part of their protocol – for example it is likely not acceptable to prove token ownership by passing the complete chain of transactions to the next owner.

Identify the elements of technology that create real utility

Isolate the parts of blockchain and DLT that add value to the tokenisation proposition. Consider the aims expressed in particular designs and how they may have impacted technology choices. For example, some elements of public blockchains are specifically designed to be 'censorship resistant'. Such features can add significant technical overhead with marginal consumer demand or benefit.

Consider realistic interoperability

Technical interoperability can be achieved in a number of ways. Each blockchain technology has taken a slightly different approach to core functions – such as the way that Besu and Fabric define private groups and interactions. Completely abstracting on top of these technologies will result in a lowest common denominator solution. On the other hand, there are many interoperability projects that try to 'boil the ocean' by setting unrealistically broad aims. Scope is important to interoperability.

Leverage neutral bodies and forums

The creation of open standards enhances competition as it allows new entrants to innovate in a 'plug and play' environment. Standards also reduce costs for participants in systems where there are many interconnections - allowing participants to focus on their core services. SWIFT has curated standards in financial services and those standards, such as ISO2022, could form the base of a co-operative approach to tokenisation.

Understand how to transform internal technology and operations

The trend towards more global ledgers of tokens will transform the kind of service that intermediaries offer. Think of how travel agents were replaced with Booking.com or Expedia. It's not that the intermediary disappeared, but they were replaced with a different kind of intermediary – one that understood how to technically connect hotels to customers world-wide. Whilst technology will be important, a deep understanding of the complex mechanics of financial services will be core.

Forming a common understanding between regulators, central banks and private sector on oversight, protection and stability

A token is a representation. The substance is what is regulated. It is important that regulators look out for regulatory arbitrage, such as stable coins vs e-money. Consumers need good guidance to allow them to evaluate the risks of various products while companies need a level playing field. Non-regulated equivalents could give rise to distorted market incentives. From the regulator's point of view, it is important that they work with the private sector particularly to avoid sudden and large balance sheet impacts.

Participate

Finally, the most important step to be taken is to participate. It can be tempting to observe what is happening from afar and to think that it is not significant. Tokenisation looks messy at the moment. The technology is unconventional and the use cases sometimes perplexing. The growth, however, is telling. There is something afoot and it is better to understand it than to ignore it.

11

ABOUT SETL

SETL is a London based technology provider with a proven track record in delivering distributed ledger technology (DLT) based solutions for financial markets, asset management and payments.

SETL's DLT technology powers regulated financial market infrastructures that are active and operational. These include the Central Securities Depository ID2S and the fund distribution platform IZNES. Most recently, SETL has successfully completed the world's first Central Bank Digital Currency (CBDC) live fund transaction in collaboration with Banque de France, using the SETL blockchain that powers the IZNES fund distribution platform.

SETL's core blockchain is proprietary and is designed to process 30,000 transactions per second across 100 million accounts. The SETL platform operates on its own blockchain but also across all major enterprise DLT's, allowing full interoperability and synchronisation at the token level. Smart contracts and flows can be driven from SETL's platform or from external DLT's giving completed flexibility on how functionality is implemented.

SETL is led by a team of financial services professionals with deep industry knowledge and expertise in disruptive innovation. SETL's proprietary market leading technology is designed specifically for regulated, high performance, low latency applications that comply with ENISA and NIST standards.

SETL's global capabilities include planning, design, support with regulatory approval processes, development and deployment; the solutions are delivered and hosted in a cloud, on prem or hybrid environments.

SETL's enterprise blockchain technology hosts Verafide, the Turnkey Opensource Solution for Verifiable Credentials. Verafide allows organisations, networks and individual users to simply and securely issue, hold, verify and share digital ID credentials.

SETL's board of directors is chaired by Sir David Walker, former chairman of Barclays and includes Christian Noyer, former Governor of the Banque de France and Professor Philip Bond, visiting researcher from the University of Oxford.

SETL

simple | unified | immediate

WWW.SETL.IO

July, 2021