Cryptocurrencies, Blockchain and ICOs: Designing a Functional Policy and Regulatory Approach to Distributed Ledger Technology and Digital Assets

Douglas Arner, Ross Buckley, Anton Didenko and Dirk Zetzsche

Draft: November 2018

Abstract

Distributed ledger technology, its highest profile form blockchain and their headline catching applications in the forms of cryptocurrencies and initial coin offerings have attracted extraordinary global attention. During 2017, the price of Bitcoin and other cryptocurrencies increased dramatically, before falling steeply in 2018, and regardless of their long-term performance, Bitcoin has now entered the history books as among the greatest financial bubbles of all time. Further, over the past two years, there has been an explosion in tokenization of assets and fundraising projects – utilizing digital tokens issued via and/or operated on blockchains, known as initial coin offerings (ICOs). At the same time, an increasing range of jurisdictions have become concerned about risks, particularly with non-sovereign cryptocurrencies and ICOs. This paper seeks to provide some light both on the trends as well as the concerns and potential opportunities for DLT, arguing that a proportionate functionally focused approach is necessary in order to balance potential benefits with new risks.

Key words: blockchain, cryptocurrencies, distributed ledger technology, initial coin offering (ICO), financial regulation

Contents

1. Introduction

Since the launch of Bitcoin in 2009, cryptocurrencies and the underlying blockchain technology have risen to global attention. Blockchain and other forms of distributed ledger technology (DLT) have attracted massive investment interest, with asset values, projects and investment likewise hitting records in 2017. During 2017, the price of Bitcoin and other cryptocurrencies increased dramatically, before falling steeply in 2018.

It is now clear that Bitcoin and a number of other cryptocurrencies – regardless of their eventual long-term performance – were the focus of one of the largest speculative bubbles in history. The Bitcoin Bubble of 2018 has now joined the South Sea Bubble of 1720, the Dot.com Bubble of 2000, the Tulip Mania of 1637 and many others.[1] However, such investment crazes are often not without foundation, as the joint stock company, global trade, the internet and others clearly demonstrate. At the same time though others have had weaker foundations, in the case of tulips and onions for instance.

In addition, especially over the past 24 months, there has been an explosion in tokenization of assets and the creation of new cryptocurrencies, digital assets and DLT initiatives, in the context of ICOs (initial coin offerings). ICOs typically use blockchain technology to offer tokens that confer various rights in return, most often, for cryptocurrency. They can be seen as a conjunction of crowdfunding and blockchain.

Hallmarks of a classic speculative bubble have likewise been present with ICOs but once again this does not necessarily mean that there may be substance beneath: at the height of the dot.com bubble, no one would have ever expected Amazon and Google to become as significant as they in fact have. As is often the case in hype cycles (of which financial bubbles are often one form), while the initial excitement is overdone, frequently the long-term impact is underestimated – this is the core idea of Amara's law:

> We tend to overestimate the effect of a technology in the short run and underestimate the effect in the long run.[2]

[1] For the classic treatment, see C. Kindleberger, Manias, Panics and Crashes (1978)
[2] Amara (1972).

This paper seeks to illuminate the global trends with respect to DLT and related concerns, risks and opportunities, focusing on policy options and approaches to balancing risks with supporting useful innovation in the region. The potential of DLT to be transformative, especially in the financial sector, is real. Many financial institutions are investing heavily in proof of concept demonstrations and the rollout of pilot applications of DLT, in addition to a range of high-profile consortia projects and an ever-increasing range of startups.

Part of the attraction of distributed ledger systems lies in transcending law and regulation, even to the extent of potentially providing an alternative trust solution to those traditionally provided by sovereign states and their political, monetary, financial and institutional structures. From a technological perspective, DLT is generally seen as offering unbreakable security, immutability and unparalleled transparency. This combination – proponents argue – provides a framework of trust based upon technology rather than human-based arrangements (such as states or banks) and so law and regulation are seen as unnecessary.[3] Yet while the law may be dull and the technology exciting, the impact of sovereigns and their institutions – in particular central banks, regulatory agencies and legal systems – cannot be simply wished away. Risk will remain, not least from the legal standpoint but also from the standpoint of the technology itself.[4] Policy-makers and regulators seeking to support appropriate approaches to twenty-first century financial infrastructure must focus on these potential consequences.

Following this introduction, section 2 provides a typology in order to underpin understanding of the often confusing terminology associated with DLT and explore related developments around the globe, focusing on the financial sector. The next two sections respectively consider in turn the two highest profile applications of DLT, namely cryptocurrencies (section 3) and ICOs (section 4). Section 5 highlights some of the major risks and considerations relating to DLT and its major applications. Section 6 presents a discussion of a comprehensive functional approach at both the domestic and regional level to balance the transformative potential of DLT with the speculative, technological and other risks involved.

[3] D Zetzsche, RP Buckley & DW Arner, "The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain", *University of Illinois Law Review* (2018)

[4] Zetzsche, Buckley & Arner (2018).

2. DLT, Blockchain and Cryptocurrencies

Over the past several years, interest in DLT and blockchain has exploded around the globe.[5] Regulators,[6] consultants,[7] technology firms[8] and academia[9] are promoting DLT and blockchain as new transformative technologies, not only in the financial sector but across all areas of economic and social institutional and market structures.

The hype cycle has also resulted in a disparate range of policy and regulatory responses across the region, with substantial differences between approaches to the specific contexts of cryptocurrencies and ICOs as compared to DLT and blockchain more generally.

As is often the case with new technologies and other innovations, there is frequently some level of confusion around terminology, resulting from the newness of many aspects but also from very different perspectives among those involved.

The best way to understand this field is to begin with the relevant underlying technology, not its applications such as cryptocurrencies or ICOs or the automation of back office clearing

---

[5] Focusing on legal and governance issues only: Lawrence J. Trautman, *Is Disruptive Blockchain Technology the Future of Financial Services?*, 69 THE CONSUMER FIN. L. Q. REP. 232 (2016); Carla L. Reyes, *Moving Beyond Bitcoin to an Endogenous Theory of Decentralized Ledger Technology Regulation: An Initial Proposal*, 61 VILL. L. REV. 191 (2016); Wessel Reijers, Fiachra O'Brolcháin & Paul Haynes, *Governance in Blockchain Technologies & Social Contract Theories*, 1 LEDGER 134 (2016); Trevor I. Kiviat, *Beyond Bitcoin: Issues in Regulation Blockchain Transactions*, 65 DUKE L. J. 569 (2015-16); Lewis Rinaudo Cohen & David Contreiras Tyler, *Blockchain's Three Capital Markets Innovations Explained*, INT'L FIN. L. REV. (2016), *available at* http://www.iflr.com/Article/3563116/Blockchains-three-capital-markets-innovations-explained.html.

[6] IOSCO, RESEARCH REPORT ON FINANCIAL TECHNOLOGIES (FINTECH) ch. 5 (February 2017), *available at* https://www.iosco.org/library/pubdocs/pdf/IOSCOPD554.pdf; ESMA, REPORT - THE DISTRIBUTED LEDGER TECHNOLOGY APPLIED TO SECURITIES MARKETS (Feb. 7, 2017); Press Release, ASIC, Op-ed: Blockchain, (Oct. 26, 2015) *available at* http://asic.gov.au/about-asic/media-centre/asic-responds/op-ed-blockchain/.

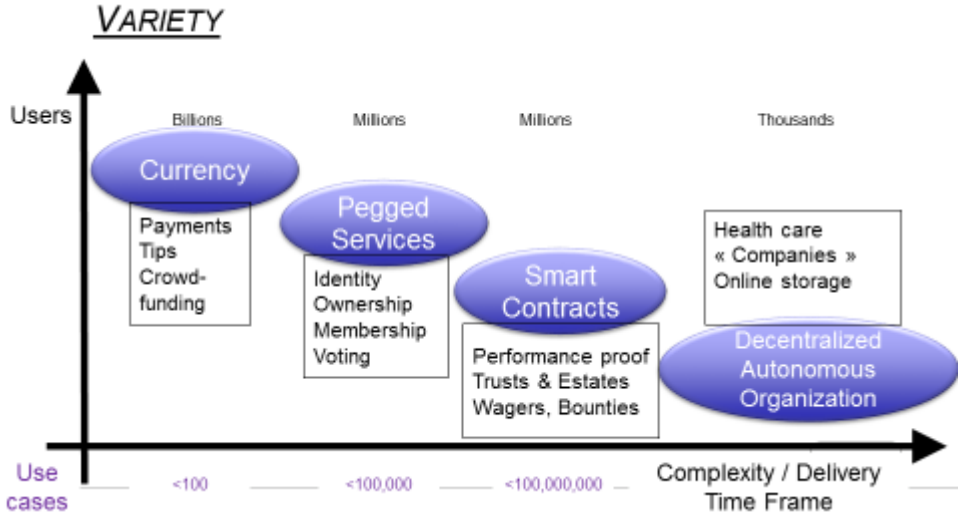
[7] It has been estimated that "distributed ledger technology could reduce banks' infrastructure costs attributable to cross-border payments, securities trading and regulatory compliance by between $15-20 billion per annum by 2022": see Santander InnoVentures, OLIVER WYMAN AND ANTHEMIS GROUP, THE FINTECH 2.0 PAPER: REBOOTING FINANCIAL SERVICES (June, 2015), *available at* http://santanderinnoventures.com/fintech2/; WORLD ECONOMIC FORUM (WITH DELOITTE), THE FUTURE OF FINANCIAL INFRASTRUCTURE - AN AMBITIOUS LOOK AT HOW BLOCKCHAIN CAN RESHAPE FINANCIAL SERVICES (2016), *available at* www3.weforum.org/docs/WEF_The_future_of_financial_infrastructure.pdf.

[8] *See IBM Blockchain*, IBM, https://www.ibm.com/blockchain/ (last visited July 10, 2017).

[9] Quinn DuPont & Bill Maurer, *Ledgers and Law in the Blockchain*, KING'S REV. June 23rd (2015), *available at* http://kingsreview.co.uk/articles/ledgers-and-law-in-the-blockchain/; Eva Micheler & Luke von der Heyde, *Holding, Clearing and Settling Securities through Blockchain/Distributed Ledger Technology: Creating an Efficient System by Empowering Investors*, 11 J. INT'L BANKING & FIN. L. 652 (2016); Philipp Paech, *Securities, Intermediation and the Blockchain: An Inevitable Choice between Liquidity and Legal Certainty?*, 21 UNIF. L. REV. 612 (2016).

and settlement. By starting with the technology, we can then consider a range of applications, including the two of particular interest to financial regulators: cryptocurrencies and ICOs.

Figure 1: Blockchain Applications: End-User View[10]



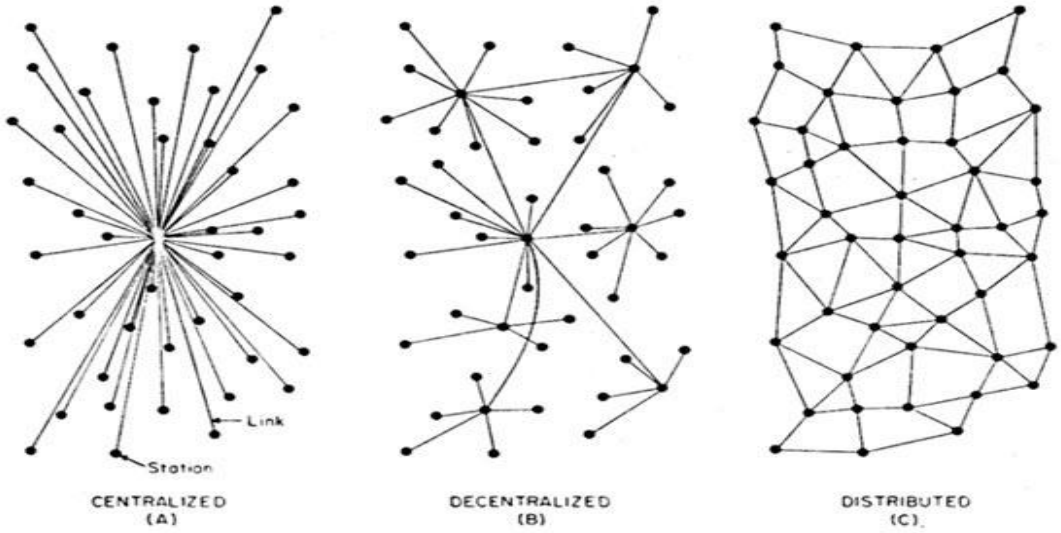
DLT is a digital ledger / recordkeeping technology underlying a whole range of innovations not only in finance but in an increasing range of other areas where the particular combination of security, permanence and transparency it offers has value. Blockchain is one particular adaptation of DLT, involving encryption of data stored on the ledger. The concept is imprecise and there is a great deal of disagreement among participants about exactly what is and what is not a "blockchain".

2.1 Centralized and Distributed Ledgers

Distributed ledgers are best understood in contrast to their counterpart, the centralized ledger, and are perhaps best understood diagrammatically, as demonstrated below in Figure 2.

Figure 2

[10] Taken from William Mougayar, *Understanding the Blockchain*, O'REILLY (Jan. 16, 2016), https://www.oreilly.com/ideas/understanding-the-blockchain (last visited June 30, 2017).



Source: Paul Baran, On Distributed Communication Networks, 1962

Centralized ledgers are the most common data storage device in finance today. Data are stored on the centralized ledger, and the trusted administrator maintains it, recording transfers of assets and the like upon receipt of appropriately verified notifications. Financial sector examples include the majority of securities clearing and settlement systems and central counterparties as well as large value payment systems including RTGS (real time gross settlement) systems in many jurisdictions around the globe. Others include traditional property registries (whether digital or not) and bank vaults. Centralized structures are typically characterized by security (because they are under the control of a single entity which can focus on this aspect) as well as speed of execution within the context of the system.

At the same time, risks exist in centralized structures. A ledger stored on a network server can be destroyed, or more likely, hacked or otherwise compromised, so that the original data are held for ransom or manipulated and replaced by new (inaccurate) data. Mathematical approaches can be used to determine how much effort is necessary to manipulate any given server. Every single server *can* be manipulated with sufficient computing power.

Centralized structures thus concentrate risk but use that concentration to focus security and management. Perhaps the best example of this comes in the context of central counterparties (CCPs), which have been a major focus of post-2008 global financial regulatory reforms. CCPs (for instance in the context of OTC derivatives or securities exchanges) provide a trusted central counterparty for transactions, removing counterparty risk and reducing

interconnections with potential systemic implications in the financial system. At the same time however CCPs centralize and concentrate risk and thus arguably create a new form of systemic risk, highlighted in the context of a range of processes from the Financial Stability Board, BIS Committee on Payment and Market Infrastructure (CPMI) and IOSCO (the International Organization of Securities Commissions) to develop regulatory approaches to systemically important financial market infrastructure such as CCPs and major payment systems, among others.

Distributed ledgers[11] address these problems by raising the barriers for manipulation of stored data. In distributed ledgers many data storage points (nodes) are all connected with each other and store all data simultaneously, and together constitute the common ledger. DLT requires consensus of those nodes. The technical details of how to achieve consensus vary – multiple concepts have been developed, such as proof-of-work,[12] proof-of-stake, proof-of-authority and many others.

To illustrate, assume there are N nodes (rather than one centralized ledger) and E describes the effort necessary to break into any single server. Given that all other conditions (security of each server etc.) are equal, we would expect the efforts necessary to manipulate all servers linked in the ledger to be N x E rather than 1 x E. The number of servers that will need to be manipulated to manipulate the outcome will depend on the number of servers necessary for consensus (C). If C>1 the distributed ledger is more secure than the centralized one. As already noted, this calculation is rather simplistic, since it assumes equal security of each server. In real-life applications, security of the central node on a centralized ledger is likely to be far superior to that of each of the distributed nodes. Our calculation also assumes that manipulation of existing nodes is necessary to manipulate the overall consensus, whereas in reality consensus can be steered by other factors (such as control of the majority of processing power in a proof-of-work system). Furthermore, the calculation will be noticeably more difficult in an open permissionless distributed database where new nodes can be easily

[11] For technical references in this part *see* Zetzsche, Buckley, Arner, *supra* note 1.

[12] In a proof-of-work system, multiple servers ('nodes') all try to solve one (generally complex and resource-intensive) mathematical problem. The first node to solve the problem is compensated for the 'work' it has performed, while all others use the solution provided by the first node to verify that the problem has been correctly solved; thereby the solution to the mathematical problem assumes the function of a unique, one-time-use code.

added to the ledger (in which case one could simply create a sufficient number of new nodes to achieve C).

As a result, DLT systems offer the potential for greater security but without the risks of concentration of centralized ledger systems. At the same time, they typically suffer by comparison in terms of speed of execution when compared to centralized systems.

2.2 Permissioned and Permissionless Systems

DLT can take various forms. In particular, DLT systems can be permissioned or permissionless. Permissioned systems are essentially private networks with a pre-defined governance structure where data authorization depends upon the agreement of multiple pre-defined servers. The leading example in the financial sector is Corda, under the governance of R3, a global consortium of financial institutions and related organizations.

In contrast, permissionless DLT systems such as Bitcoin operate on public domain software and allow anyone who downloads and runs the software to participate. In some cases even the code is further developed in the public domain. The participants in those distributed ledgers may not know who else is running a server functioning as a node at any given time. There is an additional security element in the unknown inherent in this structure: if the number of overall nodes is known a cyberattack may be planned with greater certainty given that the maximum number of nodes is certain.[13] Permissionless (or "public") systems include Ethereum and Hyperledger (which are both decentralized platforms on which a range of other applications can be built).

Permissionless systems arguably present the greatest opportunity to create alternative trust solutions, in that they are open to all and often designed to be self-perpetuating (as in the case of Bitcoin and Ethereum). However, they raise risks in terms of administration and control of data, with permissioned systems being today far more common, particularly in the financial sector context, as a result.

[13] IT experts refer to this strategy as "security through obscurity".

2.3 Blockchain

"Blockchain" refers to how data are stored on the ledger. Rather than being stored individually, data are stored in a block bundled with other data. A single block contains multiple data points, and all blocks are stored in a specific order (the "chain"). Each block includes a timestamp and a link to the previous block. Rather than manipulating one point alone, the bundling of multiple datasets in one block requires a cyber attack to manipulate the whole block of data as well as – due to the time stamp and link – the blocks linked to the attacked block (depending on the method used to connect the blocks into the chain). The level of resilience provided by the linking process may vary depending on blockchain's design. In a Bitcoin blockchain, such link is generated by hashing the data in the preceding block, which means that the attacker needs to manipulate not only the block containing the desired data, but also every single block after it – while outpacing the entire network of Bitcoin miners (due to the proof-of-work consensus algorithm).

Blockchain is effectively a combination of DLT and cryptography (which provides the method of securing the data blocks). Blockchain may also involve smart contracts. A blockchain may be used as a technology to generate, store and distribute a cryptocurrency or could involve one or more cryptocurrencies in some fashion but this is by no means necessary: Bitcoin is a blockchain based cryptocurrency. Ethereum is a blockchain based system which includes a cryptocurrency (Ether) as well as an open permissionless blockchain platform which can be used as the basis upon which to design a range of applications (smart contracts). Corda is certainly a DLT system although purists differ on whether it is a blockchain. It does not involve a native cryptocurrency although it will support the use of a range of digital currencies. Hyperledger is generally agreed to be a blockchain but does not involve its own cryptocurrency. Throughout this paper, we will thus generally refer to DLT to cover the full range of blockchain applications.

2.4 Technology-based Trust Solutions

The basic argument in favour of DLT and blockchain is that they provide trust solutions, involving enhanced security, transparency and permanence, and that these characteristics make them suitable for a wide range of potential applications. These include, among other things, asset finance, back office clearing and settlement, trade processing and settlement,

insurance claims tracking, cross-border remittances, internet of things, smart contracts and digital identity instruments. Among the best-known applications of blockchain to date are cryptocurrencies such as Bitcoin, and ICOs, and these are of particular interest to financial market regulators, as are many of the other uses being developed in the context of various forms of financial infrastructure, from trade finance to securities settlement and beyond.

At the heart of many arguments in favour of blockchain is this idea of an independent non-sovereign technology-based trust solution: the idea is that blockchain can provide an alternative underlying platform for many core functions in modern economies and societies, from money (e.g. cryptocurrencies) to identity (e.g. a permanent public storage system independent of state control) to ownership (e.g. ownership and transaction registries for land, companies, intellectual property etc). These arguments usually depend in their extreme form on public permissionless blockchain solutions – as these are argued to best realise the ideal of technological independence.

Proponents of such views argue that blockchain offers an alternative to existing mechanisms for the institutional underpinnings of economies and societies. From the standpoint of the long-term impact, DLT certainly does have the potential to redesign many systems and to offer an alternative – superior in some cases – platform for the design of institutional frameworks and markets. However, it is generally becoming clear that this is not universally true – because the key attributes of DLT and blockchain (security, transparency, permanence) are certainly not absolute and are not necessarily as strong as suggested and because these attributes are not appropriate for every context – a topic which we return to in more detail in Sections 5 and 6.

2.5 Smart Contracts

In some cases, DLT systems are designed as alternatives to existing institutional structures, for instance Bitcoin is designed as an alternative to traditional state-based currencies. Other DLT systems however are designed as platforms, on which a range of applications can be built, with Ethereum, Corda and Hyperledger all examples. Key to such platforms are “smart contracts” – self-executing structures designed to increase efficiency.

Across many systems and platforms, whether DLT or otherwise, software code design and structure define the freedom of users: the code will determine what users can and cannot do, and what they must and must not do when using the system. This will be particularly so in the machine-based interactions often referred to as smart contracts.[14]

Smart contracts are neither smart, nor contracts, but rather self-executing software protocols that reflect the terms of an agreement between two parties. The conditions of the agreement are directly written into lines of code. Although not exclusively linked to distributed ledgers and blockchain, the code and the agreements contained therein could be spread across a blockchain network as well as embedded in other DLT systems and platforms.

These smart contracts permit transactions to be carried out among disparate parties without the need for an external enforcement mechanism (such as a supervisory authority or central clearing facility). As long as the code does not provide for a reverse procedure,[15] they render transactions traceable, transparent, and irreversible from a technological standpoint, if not necessarily form a legal standpoint.

The key impact of smart contracts is to disintermediate, not only in an institutional sense, but also in a personal sense. Human intervention could delay administrative processes if the latter exclusively depend on "if – then" binary conditions. In contrast, a computer that detects an "if – then" condition is met can automatically execute the protocol. For instance, if settlement exclusively depends on payment or margin coverage, a computer if adequately programmed

[14] *See* on smart contracts, the pioneering work by Nick Szabo, *The Idea of Smart Contracts*, *in* NICK SZABO'S PAPERS AND CONCISE TUTORIALS (1997); and Nick Szabo, *A Formal Language for Analyzing Contracts*, *in* NICK SZABO'S PAPERS AND CONCISE TUTORIALS (2002), *available at* http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/contractlanguage.html; Anthony J. Casey & Anthony Niblett, *Self-Driving Contracts* (Unpublished working paper, March 1, 2017), *available at* https://ssrn.com/abstract=2927459; Joshua Fairfield, *Smart Contracts, Bitcoin Bots, and Consumer Protection*, 71 WASH. & LEE L. REV. ONLINE 35, 36 (2014); Merit Kõlvart, Margus Poola & Addi Rull, *Smart Contracts*, 133, *in* THE FUTURE OF LAW AND ETECHNOLOGIES (Tanel Kerikmäe & Addi Rull, eds., 2016); Koulu, *Blockchains and Online Dispute Resolutions: Smart Contracts as an Alternative to Enforcement*, 13 SCRIPTED 40, 43-69 (2016); Karen E. C. Levy, *Book-Smart, Not Street-Smart: Blockchain-Based Smart Contracts and The Social Workings of Law*, 3 ENGAGING SCI., TECH. & SOC'Y 1 (2017); Cheng Lim, et. al., *Smart Contracts: Bridging the Gap Between Expectation and Reality* (Oxford Legal Stud. Res. Paper, July 11, 2016), *available at* https://www.law.ox.ac.uk/business-law-blog/blog/2016/07/smart-contracts-bridging-gap-between-expectation-and-reality; Riika Kevin D. Werbach & Nicolas Cornell, *Contracts Ex Machina*, 67 DUKE L. J. * (2017), *available at* https://ssrn.com/abstract=2936294; Aaron Wright & Primavera De Filippi, *Decentralized Blockchain Technology and the Rise of Lex Cryptographia* 10-12 (Unpublished manuscript, March 12, 2015), *available at* https://ssrn.com/abstract=2580664.

[15] Adding such a procedure would remove most benefits of a smart contract to both parties.

could check more quickly and with greater accuracy whether the conditions are met than human beings. There are multiple uses in the collective investment scheme context, for instance, as well as across a range of networked market structures such as syndicated loans, trade finance, securities settlement, corporate actions, etc.

2.6 DLT Use Cases and Investment Trends

DLT and blockchain have clearly moved beyond just cryptocurrencies, and their application – in a range of forms – is now being explored and increasingly across the entire financial system. Capital raising, trading, clearing and settlement, global payments, deposits and lending, property and casualty claims processing (InsurTech), digital identity management and authentication, and RegTech solutions (such as automated compliance, administration and risk management, and anti-money laundering and client suitability checks) have all been identified as significant potential DLT use cases.

The key benefit of DLT lies in its ability to address the storage trust issue. DLT ensures the validity of datasets by spreading data over many nodes which have to agree, via the previously determined consensus mechanism, to confirm that data are correct. DLT can ensure better than other technologies that data are not manipulated while stored. DLT can also ensure that the party making a transfer has title on the ledger to the asset being transferred, and is not able to transfer it twice to separate buyers. This is leading to a wide range of innovative applications, with Everledger for the diamond market being a leading example.

The core attributes of blockchain – security, transparency, (relative) permanence – underlie its potential impact and are core to its highest profile use cases (discussed in the following two sections) but also raise some of its core risks and limitations – the subject of Section 5 below.

3. Cryptocurrencies

As noted above, the cryptocurrency Bitcoin was the first application of blockchain and remains the highest profile one. However, in many ways, it is now somewhat unusual in the broader DLT landscape.

From a typological standpoint, Bitcoin combines DLT and cryptography in the context of a blockchain. It is a permissionless system, open to anyone who downloads the open source software, with the transaction record publicly available. It is a decentralized system, in that there is no single or group of controllers but rather all participants are involved in the development and use of the system. It is designed to provide a non-sovereign permissionless decentralized trust solution in the form of an alternative currency, with security provided through the blockchain structure. Bitcoin uses the proof-of-work concept to achieve consensus among the nodes, with transaction confirmation through independent users who solve cryptographic problems in order to generate new blocks evidencing transactions and are in turn paid in newly created Bitcoin (as well as applicable commissions) ("mining").

Since the launch of Bitcoin, there has been an explosion of other cryptocurrencies,[16] some of which, such as Ether on the Ethereum network, combine blockchain with cryptocurrency and smart contracts (e.g. systems allowing the building of a range of applications which operate on the underlying blockchain and which may use the systems' cryptocurrency for transactions, recordkeeping etc.).

There are typological divisions between (1) alternative currencies which are alternatives to sovereign issued currencies; (2) digital currencies which are digitized forms of sovereign or alternative currencies; (3) cryptocurrencies which may be sovereign or non-sovereign and are generally based on blockchain and rely upon cryptography; and (4) ICOs which may or may not involve cryptocurrencies, alternative currencies or digital currencies / e-money but which typically do involve the offering of rights on a blockchain. Blockchain is simply the underlying technology which is used to facilitate cryptocurrencies and ICOs (along with many other applications) and which typically will not be involved in many alternative and digital currencies.

[16] See https://coinmarketcap.com/all/views/all/

Cryptocurrencies thus fall both into the DLT / blockchain typology (with Bitcoin as the genesis and also highest profile use case) and also into the currency typology.[17] In both, the key distinction is between sovereign and non-sovereign applications.

3.1 Non-sovereign: Alternative currencies and cryptocurrencies

Cryptocurrencies are a subset of a larger category – alternative currencies. The latter operate outside the regulated space and create what may be called "alternative payment systems" that co-exist with the payment systems recognized by national/supranational laws.[18] Alternative currencies come in a variety of forms. They can be physical (like seashells still used by some Pacific nations), or digital (like Bitcoin), or both (like the Bristol Pound, which has a paper and a digital version circulating at the same time).[19] They can enjoy varying levels of convertibility into fiat currency and can be either centralized (i.e. with a single centre of issuance and administration), or decentralized (i.e. without such a centre).[20] Overall, the number of alternative currency options is significant, limited only by human ingenuity.

The term "cryptocurrencies" can be potentially confusing, since cryptographic protection is utilized in a variety of alternative currencies, from Bitcoin to digital commodity currencies (like the Bristol Pound) or even "gold" in computer games.[21] Clearly, real-life use cases, as well as regulatory and policy implications of these currency types vary dramatically. For this reason, in this paper "cryptocurrencies" will be interpreted narrowly, by reference to those alternative currencies that are (i) digital, (ii) cryptographically protected, (iii) based on DLT and (iv) convertible by design into fiat currency (and vice versa).

The launch of Bitcoin[22] in 2009 gave rise to subsequent development of a whole range of cryptocurrencies, the number of which has skyrocketed: in 2015 their overall number reached

[17] For a comprehensive currency taxonomy see A. Didenko and R. Buckley, 'The Evolution of Currency: Cash to Cryptos to Sovereign Digital Currencies'. forthcoming 42 Fordham International Law Journal; UNSW Law Research Paper No. 18-69, available at SSRN: https://ssrn.com/abstract=3256066.

[18] ibid 33.

[19] Ibid 35.

[20] ibid 36-39.

[21] See ibid 40-41.

[22] Bitcoin was the first cryptocurrency and the first decentralised convertible virtual currency – see FATF, Virtual Currencies: Key Definitions and Potential AML/CFT Risks (2014), available at http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-

500,[23] and at the time of writing this paper, it had more than tripled, reaching over 2000.[24] These are however dominated by a small number of "major" cryptocurrencies, including Bitcoin and Ether.

Cryptocurrencies are often presented as decentralized alternatives to the existing currency types in the financial system: this is the fundamental premise of Bitcoin. As such, Bitcoin was presented as a disruptive alternative to existing sovereign currency arrangements, a technology based alternative which operated independently of any government. This had a strong appeal to many people in the aftermath of the 2008 Global Financial Crisis and the timing of Bitcoin's launch was thus very fortuitous and in fact came during a period characterized by FinTech – "financial technology" – seeking to develop better alternatives to traditional financial institutions, markets and approaches.

At the same time however governments and central banks found such a challenge less than appealing and often reacted negatively, particularly around concerns of value and transparency as well as usefulness. Thus a wide range of jurisdictions have developed regulatory approaches to cryptocurrencies, ranging from facilitative frameworks (e.g. in Japan) to outright bans (e.g. China).

Much discussion centres around whether cryptocurrencies are in fact money or currency, functionally and/or legally. From a functional standpoint, money plays three major roles: as a unit of account, as a store of value, and as a means of exchange. Functionally, cryptocurrencies do in some cases fulfill these functions but the volatility in value erodes all three functions, meaning that cryptocurrencies certainly over the past year have been more speculative than monetary in nature.

From a legal standpoint, whether something is money or currency is determined by the laws of an individual jurisdiction, with many jurisdictions providing a monopoly to the national currency in these roles (e.g. China). In such jurisdictions, absent a change in law, cryptocurrencies will not be legal forms of money. Other jurisdictions however have been

---

aml-cft-risks.pdf, 5-6. For additional detail see ECB, Virtual Currency Schemes (2012) 22; https://bitcoin.org/bitcoin.pdf.

[23] ECB, Virtual Currency Schemes – A Further Analysis (2015) 4.

[24] See https://coinmarketcap.com/all/views/all/.

more facilitative (e.g. Japan, Singapore, Switzerland) in allowing alternatives to the national currency, including in some cases specifically cryptocurrencies.

Overall, this question of whether or not to allow the use of cryptocurrencies for payment and settlement appears to largely be a domestic policy question. To date, Bitcoin has been most popular in economies with very volatile currencies, often issued by governments with financial challenges. It seems thus that the question whether Bitcoin or other cryptocurrencies can challenge sovereign alternatives has been answered: good money will drive out bad – regardless of the source, per Gresham's Law.

In jurisdictions which have determined not to regulate cryptocurrencies as money, other potential approaches apply, beyond prohibition (which is often of limited effectiveness outside of effective national internet surveillance) or development of a specific legal framework (as has been done in Japan). The most common issue in such jurisdictions is whether cryptocurrencies can be recognized as a part of the formal payment system, which in most jurisdictions draw regulatory scrutiny, typically from the central bank under international standards from the Committee on Payment and Market Infrastructure of the Bank for International Settlements. The question of whether a given cryptocurrency will be recognized as a of the formal payment system will largely depend on how it is meant to be used in a given jurisdiction: Bitcoin and Ether often fall outside such remits while Ripple and XRP often fall within such remits.

Other jurisdictions may classify cryptocurrencies as commodities (e.g US) or simply apply consumer protection laws.

Overall, the key for any jurisdiction is to consider the potential range of risks and develop a balanced and proportional approach to the risks which arise.

From the standpoint of monetary policy, the most important focus is thus not cryptocurrencies but rather appropriate management of the domestic economy and currency, as has long been the case. Appropriate macroeconomic policy should reinforce trust in the domestic currency, thus removing the need for, and reducing the appeal of, non-sovereign alternatives. At the same time, monitoring of markets would be potentially valuable in understanding asset values and financial flows in and out of individual economies.

From the standpoint of financial stability, although the value and volatility of cryptocurrencies is high, so far there appears to be little linkage to the credit system, the formal payment system or the traditional financial system, thus minimizing potential sources of systemic risk. So far, the Financial Stability Board (FSB) has concluded that 'crypto-assets do not pose a material risk to global financial stability'.[25] Monitoring however is in order.

From the standpoint of market integrity and consumer protection, issues arise, which we return to again in sections 5 and 6.

3.2 Alternative Currencies: Legal Status and Regulatory Implications

Only certain types of alternative currencies have triggered a regulatory response. Unlike their freely convertible counterparts, alternative currencies operating within closed virtual systems remain unregulated. Semi-convertible alternative currencies are becoming increasingly popular in mobile and computer games and also do not seem to attract regulatory attention insofar as their use is limited to virtual communities.[26]

The situation with regulatory treatment of freely convertible alternative currencies (a category to which many cryptocurrencies belong) is more complicated. Clear links to the real economy and entry points to the formal payment system are a cause for concern, which is reflected in various regulatory measures adopted throughout the globe. The most popular reaction so far has been in the form of warnings in respect of cryptocurrencies and prohibitions on their use as part of the formal payment system.[27] In contrast, some states have gone further, attempting to subject cryptocurrencies to comprehensive domestic regulation.[28]

---

25 Financial Stability Board, 'Crypto-Asset Markets: Potential Channels for Future Financial Stability Implications', available at http://www.fsb.org/wp-content/uploads/P101018.pdf 1. A crypto-asset is defined as 'a type of private asset that depends primarily on cryptography and distributed ledger or similar technology as part of their perceived or inherent value'. See Annex 2 in ibid 17.

26 See A. Didenko and R. Buckley, 'The Evolution of Currency: Cash to Cryptos to Sovereign Digital Currencies'. forthcoming 42 Fordham International Law Journal; UNSW Law Research Paper No. 18-69, available at SSRN: https://ssrn.com/abstract=3256066 41-42.

27 ibid 42.

28 ibid.

As a result, cryptocurrencies are often subject to regulatory scrutiny in the form of warnings, prohibitions or express legislation. Effectiveness of these measures hinges on clear and unambiguous definitions of their subject matter – yet regulators generally reuse the existing terminology and, by doing so, fail to achieve the clarity required. Cryptocurrencies issued by central banks might further complicate the existing taxonomy.

3.3 Sovereign Digital Currencies and Cryptocurrencies

It would be extremely naïve to expect governments and national regulators to act as idle observers of the proliferation of cryptocurrencies, which have the potential to challenge the existing value exchange process based on fiat currency (even though at the time of writing such a possibility remains largely theoretical). Since direct regulation of cryptocurrencies built on top of a permissionless blockchain can be impractical, if not impossible (at least in the absence of a coordinated *international* response), a number of countries are now rethinking their approach to cryptocurrencies. Instead of attempting to regulate something as elusive as Bitcoin (which has no issuer and centre of operation and, consequently, no situs and no "home country"), we now observe what can be seen as the early stages of a paradigm shift towards offering end-users new or re-designed government-issued or government-backed currencies that – if designed accordingly – could be more convenient, resilient and ultimately more useful than (formally unrecognized and unregulated) cryptocurrencies, and may even come with significant added benefits for regulators (such as automated taxation or better information about the flow of value within the economy).

We envisage three alternative approaches: (i) central bank accounts with general access, (ii) central bank accounts with intermediated access and (iii) new digital forms of official (fiat) currency.[29]

3.4 Central Bank P2P/Intermediated Payment Systems

[29] For a more detailed discussion of available approaches see A. Didenko and R. Buckley, 'The Evolution of Currency: Cash to Cryptos to Sovereign Digital Currencies'. forthcoming 42 Fordham International Law Journal; UNSW Law Research Paper No. 18-69, available at SSRN: https://ssrn.com/abstract=3256066 47-50.

The idea to provide alternative and safer options for storing value in the form of official currency is not new but these options have generally not been technologically feasible. However, over the past 30 years technology has now advanced to the point where this is no longer necessarily the case. As a result, there are increasing numbers of proposals, pilots and launches of systems allowing broader access to central bank accounts for the general public and non-financial institutions. Such access can be provided to end-users *directly*[30] or *via intermediaries* (such as private operators guaranteed by central banks).[31]

Such discussions raise a major policy question: even if the technology is now available to replace our traditional interbank large value payment systems with alternatives (particularly based on provision of individual accounts via a centralized system), should we do so? At present, despite having reviewed the potential, the major central banks which have so far faced this question (including the Bank of England and the Bank of Canada) have decided that they do not yet want to take this leap into the unknown. From a policy standpoint, the arguments in terms of efficiency and macroeconomic and macroprudential monitoring capability for the central bank are compelling, as are the possibilities of removing the traditional public good of providing payments from the banking system. However, the existing system, which largely evolved in the 19th century and which has been digitized and improved from the early 1970s particularly in the context of large value RTGS systems, is familiar. In addition, as a result of the long period of attention, it is also arguably robust: payment systems in major markets functioned without issue throughout the 2008 crisis. At the same time, there is real concern about the impact on the banking system – which still plays an important role in financial intermediation and savings in addition to payment.

3.5 Sovereign (Central Bank) Cryptocurrencies

The declared intent and ongoing work of some states to develop digital currencies linked to central banks has attracted a lot of attention to the prospects of an "official" cryptocurrency.[32]

---

30 ibid 48-49.

31 ibid 47-48.

32 See Ruth Wandhoefer, The Future of Digital Retail Payments in Europe: A Role for Central Bank Issued Crypto Cash? (2017), available at http://www.ecb.europa.eu/pub/conferences/shared/pdf/20171130_ECB_BdI_conference/payments_conference_2017_academic_paper_wandhoefer.pdf; Morten Bech and Rodney Garratt, Central Bank Cryptocurrencies, BIS Quarterly Review (2017) 55; John Barrdear and Michael Kumhof, The Macroeconomics of Central Bank Issued Digital Currencies (2016), Bank of England Staff Working

So far, Venezuela has been the first country to do so[33] but an increasing range of countries are studying or considering such projects, across both developed and developing countries. A summary is highlighted in the following table.

Summary Table of Central Bank Cryptocurrencies: Existing and Announced Projects

Country	Project	Description	Source
Canada	CAD coin	Testing new payment system	Bloomberg
China		Goal: Issuing digital currency	SouthChina Morning Post
East Caribbean	East.Caribbean dollar	Issued by the East. Caribbean Central Bank; cooperation of 8 national central banks	Forbes
Estonia	Est Coin	Testing for its own digital currency	EUobserver
India		Issue of Bitcoin-Like cryptocurrency backed by Central Bank	Coinspeaker
Israel		Clause for a legal framework for use of an official state cryptocurrency	calcalistech
Japan	J-Coin	Create a digital currency "J-Coin" before 2020.	calcalistech
Kazakhstan		Create own sovereign cryptocurrency and bring the financial system onto the Blockchain.	The Daily Economist
Kyrgyzstan		Create national gold backed cryptocurrency	The Daily Economist
Marshall Islands	SOV	New Sovereign Cryptocurrency	Nasdaq
Netherlands	DNB Coin	Internal blockchain prototype	Coinmis
Papua New Guinea		The Central Bank adopts Blockchain	Bitcoin magazine
Russia	Cryptoruble	CryptoRuble will be launched in Mid-2019.	Cointelegraph
Senegal	eCFA	Supported by Senegalese Central Bank, supposed to be African cross-border cryptocurrency	Bloomberg
Singapore	Ubin	Central bank and industry explore the use of DLT for clearing and settlement of payments and securities.	Monetary Authority Singapore
Sweden	E-krona	Central bank testing the feasibility of issuing a digital currency	Calcalistech
Tunisia	eDInar	Government-sponsored implemented by Tunisienne Poste	e-dinar.poste.tn
United Kingdom		Bank of England is assessing the implications of digital future for sterling.	Bank of England
Uruguay		Central Bank presented rollout of its	news.bitcoin.com

Paper No 605, available at https://www.bankofengland.co.uk/-/media/boe/files/working-paper/2016/the-macroeconomics-of-central-bank-issued-digital-currencies.pdf?la=en&hash=341B602838707E5D6FC26884588C912A721B1DC1; JP Koning, Fedcoin: A Central Bank-issued Cryptocurrency (2016), available at https://www.r3.com/wp-content/uploads/2017/06/fedcoin_central-bank_R3.pdf; Walter Engert and Ben Fung, Central Bank Digital Currency: Motivations and Implications, Bank of Canada Staff Discussion Paper 2017-16, available at https://www.bankofcanada.ca/wp-content/uploads/2017/11/sdp2017-16.pdf; George Danezis and Sarah Meiklejohn, Centrally Banked Cryptocurrencies (2016), available at https://eprint.iacr.org/2015/502.pdf.

[33] See A. Didenko and R. Buckley, 'The Evolution of Currency: Cash to Cryptos to Sovereign Digital Currencies'. forthcoming 42 Fordham International Law Journal; UNSW Law Research Paper No. 18-69, available at SSRN: https://ssrn.com/abstract=3256066 49-50.

		pioneering digitization of the Uruguayan peso	
USA	Fedcoin	Proposal for digital central-bank money in public use	Andolfatto Blog
Venezuela	Petro	Launching an oil-backed cryptocurrency by the government.	Washington Post

The concept of an "official" cryptocurrency issued by a central bank is an attempt to marry the benefits of certain alternative currencies and central bank money. Its status as central bank money ensures its universal acceptance within the formal (regulated) payment system. Nonetheless, in contrast to various proposals envisaging intermediated access to central bank money via authorized private or public parties, this method allows complete elimination of middlemen. The key disadvantage of existing forms of digital central bank money is thus eliminated: the latter finally becomes accessible for the majority of end-users.[34]

DLT offers various advantages to the circulation of central bank money, such as the ability to have at all times a secure record of each transaction and elimination of various intermediaries and the corresponding risks.[35] In terms of issuance control, the system is likely to be centralized. Existing concepts of central bank issued cryptocurrencies suggest different approaches.

3.6 Sovereign digital currencies: Benefits, opportunities and risks

As noted in the preceding section, a number of governments have already begun preparations for launching sovereign digital currencies, thus contemplating what can be called an "official" response to Bitcoin and many of its spin-offs. However, it should be stressed that so far most of the known projects remain in a testing phase. Still, the sheer number of countries working in this space[36] suggests that governments are either (i) seriously concerned

[34] On the role of distributed ledger technology in eliminating intermediaries see eg Mojmir Hampl, Central banks, digital currencies and monetary policy in times of elastic money, available at https://www.bis.org/review/r170720b.htm, 2.

[35] This is particularly relevant for jurisdictions with large numbers of commercial banks, many of which are risky deposit-holders. For example, Russia has over 800 registered banks, however just over 500 have the right to carry out banking operations as a result of various restrictions imposed by the central bank.

[36] See Table 4 above.

that cryptocurrencies possess the ability to upset the fundamentals of existing payment systems based on the duality of central bank and commercial bank money, or (ii) see sufficient benefits that stem from the new sovereign digital currencies (or both). Apparently, there exists yet another reason that is much more pragmatic: sovereign digital currencies can be used as a vehicle for raising money by the state – a feature of the Petro, the newest national digital currency issued during Venezuela's ICO in 2018.[37] While a comprehensive analysis of the entire range of benefits and risks associated with sovereign digital currencies, as well as the underlying regulatory implications, is outside the scope of this paper, we will only outline some of the more prominent aspects.

Benefits and opportunities

First, sovereign digital currencies may reduce the risks associated with the circulation of fiat money in digital form, which is routinely held through commercial bank accounts. Direct access to central bank money generally remains a privilege for a very limited number of entities, such as the largest banks, foreign central banks or governments. Sovereign digital currencies may change this status quo by offering much broader access to central bank money. We expect that, within the new sovereign digital currency schemes, central banks are likely to act as the ultimate trusted intermediary that is immune to insolvency, replacing commercial banks. A truly disintermediated sovereign digital currency is conceivable in theory, but seems unlikely in practice, since this would require regulators to relinquish control over transaction confirmation and recordkeeping for operations in the new digital currency – a giant leap of faith that requires absolute trust in the technology that is still in its infancy.

Second, integration of blockchain into the sovereign digital currency offers enhanced record-keeping functionality. Bitcoin's implementation of the blockchain technology demonstrates the ultimate level of transaction tracing whereby every single unit of currency can be tracked back to its source. A similar level of tracing functionality could be integrated into a sovereign digital currency to enhance the quality of data on the national economy compiled by central banks. Ironically, this seemingly enticing benefit for regulators may be seen as unnecessarily

[37] See Petro *Financial Proposal*, (White Paper), 14, available at http://elpetro.gob.ve/index-en.html#home

intrusive and privacy-defying by end-users and could, conversely, promote the use of 'real' cash instead of its new 'digital' counterpart.

Third, sovereign digital currencies can be used as a vehicle for critical national expenditure (public procurement, military expenses, payments of salaries and government subsidies) to bypass commercial banks completely. This could substantially reduce the systemic risks associated with commercial banks, lower the impact of collapse of any given financial institution and, consequently, diminish incentives to bail out failed banks.

Fourth, central banks can seize the opportunity to modernize their ageing wholesale payment systems, many of which are already at the end of their technological life cycle.[38] Furthermore, governments can use sovereign digital currency platforms as the foundation for further development of their payment systems – one that is capable of supporting smart contracts and other advanced functionality.

Fifth, sovereign digital currencies have the potential to dramatically alter the financial inclusion landscape, provided that the necessary infrastructure is in place. Further advantages for regulators may include enhanced control over benefits distribution and easier collection of data on spending patterns of the most vulnerable demographic groups.

Challenges

Regulatory challenges relating to sovereign digital currencies are also many and can be grouped into three broad categories.

The first one covers all kinds of technical issues involved in setting up a sovereign digital currency, particularly in the absence of accepted international standards on DLT and blockchain.[39] As a result, regulators are faced with a multitude of possible design choices, but at the same time may possess inadequate resources, insufficient knowledge or limited access to computer engineering, cybersecurity and other kinds of expertise that may be required. The technical questions regulators need to answer prior to setting up a sovereign digital currency

[38] See eg Morten Bech and Rodney Garratt, "Central Bank Cryptocurrencies", BIS Quarterly Review (2017) 66, available at https://www.bis.org/publ/qtrpdf/r_qt1709f.pdf.

[39] See section 6.1 below.

are many. Should the system utilise DLT and, if so, what consensus algorithm should be implemented?[40] Will the database constitute a blockchain and, if so, how will the blocks be linked together? What cybersecurity protections should be put in place? Can each unit of sovereign digital currency be traced back to its source at any point of time and, if so, how would such system scale over time, as the number of transactions increases? Can transactions on a sovereign digital currency blockchain be reverted and how can mistakes/erroneous payments be rectified? What algorithm or which regulator/authority/group of entities controls the process of issuance of sovereign digital currency? What information about users of sovereign digital currency and their transactions is public and what kinds of data are only available to the regulator? How do end users access their sovereign digital currency balances: via biometric/multifactor identification or otherwise?

The second set of challenges concerns the impact of a sovereign digital currency on the payment system, financial markets and economy as a whole. Regulators should consider performing a comprehensive ex ante analysis of the corresponding financial system, while identifying entities that may end up being in direct competition with the state once it implements an "official" cryptocurrency: such entities may include commercial banks, electronic money issuers, international payment card platforms and other payment services providers, as well as issuers of non-sovereign cryptocurrencies. Excessive competition from the state may require some of these businesses to rethink their business model, relocate to another jurisdiction or seize operations altogether. Uncontrolled implementation of sovereign digital currencies may lead to commercial bank runs and upset the duality of central bank and commercial bank money, which forms the basis of most payment systems today. At the same time, regulators might consider collaboration, as opposed to direct competition, with other participants of the payment system. On the one hand, sovereign digital currencies could utilise existing infrastructure of commercial banks upon agreement with the latter. On the other hand, regulators may implement a range of measures to create a level playing field with private parties – or even artificially make sovereign digital currencies less attractive (at least initially, to allow the market to adjust). These measures could include establishing upper limits of, or negative interest rates on, sovereign digital currency balances, as well as lifting deposit insurance limits (at least up to the maximum permitted sovereign digital currency balance, if the latter is restricted). While the partnership with private entities reduces most

[40] Although the starting question should arguably be different: does the use of DLT and blockchain provide sufficient benefits compared to a centralised database in the first place?

likely the time to develop and implement new currency systems, the impact of involving private entities and the entities' incentive structure as well as their activity on financial markets must be carefully considered if those entities get hold of proprietary information. Regulators also need to take into account any implications for money supply and consider whether the new currency will be issued via an ICO (or other form of initial distribution) or in exchange for other forms of sovereign money (eg cash or central bank account balances for eligible entities) or commercial bank money (or both) and design corresponding conversion mechanisms.

The third category of challenges is legal and reflects the need to introduce the concept of sovereign digital currency into the national regulatory system. This may, in turn, alter the existing approach to the regulation of non-sovereign cryptocurrencies in jurisdictions that already have dedicated rules, or lead to a change of regulatory stance in relation to non-sovereign cryptocurrencies in countries that have opted for a "wait and see" approach instead.

Such structures could offer a range of important benefits, including in many cases replacing non-sovereign cryptocurrencies in the context of a range of DLT applications. A trusted central bank cryptocurrency would likely be attractive in other DLT applications. In particular, there are significant discussions regarding "stable coins". Stable coins are cryptocurrencies which are backed by fiat currencies – rather than issuing its own sovereign cryptocurrency, a central bank might allow, support or facilitate the creation of a stable coin, backed by deposits of fiat currency with the central bank which then could provide the role of sovereign currency trust in the context of specific systems, for instance in the context of applications developed on Corda which would value the reduction or elimination of risks through linkage of digital asset values to a tokenized fiat currency rather than to an alternative non-sovereign cryptocurrency.

4. Initial Coin Offerings and Tokenization

ICOs apply DLT (usually blockchain) to fundraising, particularly early stage fundraising utilizing the crowdfunding[41] model. ICOs are one form of tokenization: representing currencies and other assets with a digital token evidencing (or at least purporting to

[41] A form of raising finance by soliciting contributions from a large number of funders, commonly via the Internet or using mobile phones.

evidence)[42] some sort of right or interest. ICOs – like crowdfunding – take a number of forms, depending on what sort of token is being offered. Following the crowdfunding typology, these range from donation to rewards to investment ICOs, as well as pure cryptocurrency ICOs.

4.1 ICO Typology

Donation ICOs are tokens offered in exchange for donations in support of some activity or product, mirroring donation-based crowdfunding, for instance in the context of GoFundMe.com.

Rewards ICOs are based on tokenization of some sort of advance purchase, or other type of entitlement to the outcomes of the project funded by the ICO, mirroring reward-based crowdfunding, for instance in the context of KickStarter.com. These are frequently labelled as "usage" or "utility" tokens but this label is often misleading – frequently it is used to try to avoid characterization as a financial product and the related legal and regulatory requirements. The key to a rewards ICO is that it entitles the holder of the token in the future to use something, typically the software to be developed with the proceeds of the ICO, or to be a member of some community with certain rights. One can think of it as paying in advance for a software license or community membership.

Investment ICOs involve issuance of tokens for a wide range of different investment opportunities generating financial return, typically involving potential profits through the appreciation of the value of the token over time. This is in contrast to rewards ICOs, where the return on funding is provided in kind. Investment ICOs raise the same sorts of issue as any other form of financial product and generally raise the same sorts of potential risks and concerns, albeit with the addition of issues raised by the application of DLT. Investment ICOs in the US will typically be characterized by the SEC as constituting securities, and be subject to the securities laws. This is also increasingly the case in other jurisdictions around the world, as highlighted by the wide range of related statements collected from individual securities regulators around the world by IOSCO.[43]

[42] The legal effects of tokenization, the nature of connection between a token and the underlying asset or right, as well as enforceability of tokens is ultimately a matter of applicable law.

[43] See: http://www.iosco.org/publications/?subsection=ico-statements

In addition to this traditional crowdfunding typology, there are also specifically "cryptocurrency ICOs". In their pure form, these are means to raise funds to develop, or ensure the wide distribution of created, new cryptocurrencies. However, these are often also combined with some aspect of blockchain platform technology, tokenization and/or smart contracts, as with Ethereum. As such, they are often in reality investment ICOs, with pure cryptocurrency ICOs being uncommon. For pure cryptocurrency ICOs, the typical treatment is under currency, payment or commodity rules in most jurisdictions, typically resulting in a lower regulatory burden than that which would be applied to investment ICOs. Cryptocurrency ICOs that confer upon the holder of the token the right to an amount of cryptocurrency could also be classified as derivatives, as the value of the ICO derives from the value of the underlying cryptocurrency, if the derivatives definition in that jurisdiction includes references to cryptocurrencies, or fiat currency if the cryptocurrency relates to that.

In addition to these categories, ICOs can also be asset-backed: digital tokens backed by specific assets. In a rewards structure, the token might take the form of a digital coupon which could be presented for an underlying asset (e.g. a pizza). In an investment structure, the token could represent an investment asset (such as a security or other ownership interest). In a cryptocurrency ICO, the token could represent another cryptocurrency. Such tokens highlight an important element of the broader potential of blockchain: the use of digital tokens to provide liquidity, transparency and permanence for real assets which were previously largely illiquid (such as real estate in the context of a blockchain based property registry) or where ownership and/or providence concerns are high (e.g. diamonds or agricultural products).

From this typology of ICOs, an ICO can be seen as an application of blockchain or DLT, in the context of fundraising. ICOs may or may not involve cryptocurrency but will typically involve the conferral of rights that are issued and managed on a blockchain.

4.2 ICOs around the globe – some figures

ICOs have raised very substantial amounts of funds, particularly in 2017 and 2018.

In Asia, unlike the rest of the world, ICOs targeting financial industry projects are the second largest rather than the largest category, with commerce and advertising taking the largest share. However, a range of other categories including trading and investment, payments, and exchange and wallets are often related to financial sector projects. Nonetheless, the range of projects for which fundraising is occurring is significant, and this highlights some of the greatest potential benefits in the combination of blockchain and crowdfunding though these must be carefully balanced against the risks, the subject of the next section.

ICOs thus are a form of raising finance built around the concept of "tokenization" of various assets that uses DLT.[44] Distributed ledgers are used to store and allocate tokens among ICO participants. The technology offers greater transparency of entitlements offered by the ICO originator that are shared across the entire ledger. Coupled with blockchain, it also allows better tracking of such entitlements, since each transfer of such entitlements will be recorded in a sequential order.[45] DLT-based cryptocurrencies are often used as the consideration to be provided in exchange for ICO tokens, but this use of cryptocurrencies is circumstantial: consideration can generally take the form of "any type of valuable asset".[46]

4.3 Regulation of ICOs

Regulators around the globe have adopted a range of responses to ICOs.

Outright ban

Chinese and South Korean regulators have pursued this approach. However, it is generally not seen as fruitful in most markets.

Regulatory warnings

[44] For a detailed explanation of ICO mechanics see D Zetzsche, RP Buckley, DW Arner, & Foehr "The ICO Gold Rush: It's a Scam, It's a Bubble, It's a Super Challenge for Regulators", https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3072298 [add pinpoint].

[45] ibid.

[46] Ibid.

Other regulators have not been so decisive and have adopted a more cautious approach, issuing warnings to various stakeholders stressing the risks of investment in ICOs. These are now common to the extent that IOSCO maintains a comprehensive listing on its website.

Application of existing securities and investment product laws

An increasing number of jurisdictions around the world are taking the approach of clarifying that relevant financial regulatory frameworks apply to ICOs which are in effect investment products. As several of the authors have argued elsewhere, the crowdfunding typology provides an appropriate approach, differentiated on the basis of the purpose of the ICO, which we return to in the final section.

Is DLT the Problem?

Interestingly, the regulatory measures adopted thus far do not appear to be a direct response to the use of DLT in ICOs. If nothing else, greater access to data and transaction recording can simplify regulatory monitoring and oversight of financial markets. Regulatory concerns seem to be much more prosaic: inadequate disclosure, immaturity of the business or the entrepreneurs, respectively, risks of fraud and other forms of deceptive business practices are the key issues so far. This is hardly surprising, given the existing "cavalier disregard" of the need to provide adequate disclosure, coupled to the lack of appreciation of legal risks that is seen in many ICOs.[47] Opportunistic expectations that ICOs can somehow exist outside any legal system are, of course, naïve.[48] Nevertheless, existing regulatory measures in the area of finance are not based on or triggered by the defining features of DLT. DLT is merely the technology underlying the operation of the ICO. It is what the ICO promises, how it discloses the risks it poses, and how it is promoted to the market, that will determine how it falls for regulation under the laws of each country.

5. DLT: Risks and Concerns

[47] D Zetzsche, RP Buckley, DW Arner, & Foehr "The ICO Gold Rush: It's a Scam, It's a Bubble, It's a Super Challenge for Regulators", https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3072298 [add pinpoint]

[48] Ibid.

With so much interest and so many potential uses around the globe, many argue that DLT will transform the entire financial system, from money to infrastructure to fundraising. A high level of industry penetration requires careful analysis of underlying risks. The authors have already provided a detailed account of such risks elsewhere.[49] For this reason, this article outlines only the major issues.

The starting point of the discussion that follows is the conclusion that "risk does not vanish if financial services are provided via distributed ledgers**"**.[50] Simply put, DLT may enhance efficiency (e.g. by making it more difficult to tamper with the stored data), but the underlying risks do not disappear entirely: DLT does not necessarily make data tamper-proof. At the same time, this is only one side of the coin. Specific features of DLT may multiply some of the existing risks and even give rise to new risks of a different nature.

This section identifies the key limitations relevant for all applications of DLT and outlines the corresponding implications. Three major types of risk are relevant for DLT: ledger transparency risks, cyber risks and operational risks.

5.1 Transparency Risks

The key idea behind DLT – that the same data are distributed among all data nodes – promotes transparency as well as security. The data that end up being distributed across the entire ledger can be repackaged or encrypted, but remain accessible by every node operator.[51] This makes DLT systems potentially ideal for dealing with issues concerning money laundering (thus contra to the often perceived problem of total secrecy: rather DLT – if designed – provides complete transparency of identity and transactions, including over time in that the history is immutable).

---

[49] See D Zetzsche, RP Buckley & DW Arner, "The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain", forthcoming *University of Illinois Law Review.*

[50] D Zetzsche, RP Buckley & DW Arner, "The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain", forthcoming *University of Illinois Law Review* [add pinpoint].

[51] For instance, in Bitcoin, all the data is on the blockchain except the identity of the owners. To know that, one requires the private key. The private key is stored on the owner's wallet rather than the ledger. "However, anyone can see who owns each block, via its public header information, and can follow the links through the entire chain right back to the first block." *Cf.* Jude Umeh, *Blockchain Double Bubble or Double Trouble?,* 58:1 ITNOW 58 (2016).

At the same time, this creates obvious complications for the use of DLT whenever shared data or parts of shared data are intended to remain confidential. Even where data on a DLT do not reveal the identity of a person (e.g. a Bitcoin wallet owner) because a private key is required for that function, there is a risk that the information from the user's profile could be used to reconstitute such identity. Repersonalization of pseudonymous data on distributed ledgers has already become a business, with companies offering data tracking services.[52]

Increased transparency puts a higher emphasis not only on the protection of data on a distributed ledger, but also on its structure and content. Distribution of personal data is generally restricted under data protection laws. Penalties for violations may be severe.

This also raises particular problems in the cross-border context, in that data protection legislation in most regions (unlike in the EU, with the new General Data Protection Regulation – GDPR)[53] varies from jurisdiction to jurisdiction, often with conflicting requirements. This raises the potential need for regional cooperation in addressing data issues – and also for a range of possible technological solutions, including through DLT systems.

5.2 Cyber risks

DLT does not result in an immediate reduction of cyber risks, and in some cases even enhances them.

First, a set of inaccurate data distributed across a distributed network will remain inaccurate, and its visibility within the entire network may increase the likelihood that others may act upon such data. The use of DLT certainly does not rectify inaccurate data.

Second, DLT offers increased safety of data compared to a centralized ledger only when the cybersecurity of the central node of the centralized ledger is lower than the resilience of such

[52] For example, Elliptic offers Bitcoin forensic services that draw on "extensive number of both public and privately accessible sources of information in order to identify real-world identities on the bitcoin [*sic*] blockchain". https://www.elliptic.co/what-we-do?hsCtaTracking=66b61351-d3ad-4fc5-9518-a31527e547d1%7Cce44b826-4995-4d71-a9e5-0f9901e96d62

[53] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119/1, 4.5.2016.

number of nodes that is sufficient to establish a consensus of the entire distributed ledger. In practice, this assumption is often inaccurate. On the one hand, centralized ledgers often boast robust security mechanisms that significantly outclass individual end-user nodes on a distributed ledger. On the other hand, not all nodes of a distributed ledger are equal, often as a result of the adopted consensus algorithm. For example, in a proof-of-work model, generation of new data on the ledger is often limited to a handful of nodes with the highest processing power. Ledgers that require a majority of nodes to vote for a consensus may be more easily manipulated if attacks are targeting nodes with the weakest level of cybersecurity.[54] This concentration can be abused by potential attackers.

While DLT is proliferating across the globe, there are to date no systems of certification of blockchains. While the attractiveness of DLT is based on its central attributes of security, transparency and permanence, the reality is that blockchains are not created equal.

5.3 Operational Risks

Operational risks are another area where DLT's strengths may turn into weaknesses. Any errors in the code implemented on the ledger are replicated across the entire network. Outdated or otherwise insecure code can be abused by attackers in wide-scale attacks, as was the case with Mt. Gox and the DAO.[55] At the same time, the consensus mechanism that is used to reconcile data across all nodes may itself be inadequately coded and, consequently, exploited.

The distributed nature of a ledger does not reduce the end-users' reliance on experts who understand how the system operates. As a result, mistakes made by such experts are likely to be repeated by others. When mistakes happen or the expectations associated with the increased efficiency of DLT are not met, questions as to who is responsible and their legal responsibilities will arise.

---

[54] See further D Zetzsche, RP Buckley & DW Arner, "The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain", forthcoming *University of Illinois Law Review* [add pinpoint].

[55] See further D Zetzsche, RP Buckley & DW Arner, "The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain", forthcoming *University of Illinois Law Review* [add pinpoint]. Provide separate cites to sources re Mt Gox and the DAO.

It is important to note in this context that simply because the Bitcoin blockchain has proven famously robust, not all blockchains will be. While wallets and exchanges for Bitcoins have often been hacked the underlying Bitcoin blockchain has proven highly resilient and robust. However, not all blockchains are created equal. A blockchain can now be built using on-line resources by a moderately talented technologist in a few hours. It will not, in all likelihood however, be very robust.

There is thus a clear need for some sort of certification system in order to differentiate blockchain quality, for instance in the context of the International Standards Organization (ISO) and its certification processes.

5.4 Blockchain-Specific Risks

Blockchain's key feature distinguishing it from other variations of DLT is the sequential order of data that is split into portions ("blocks"). This structure is append-only and allows information to be added, but not removed. Changes to a single block in the chain require alteration of the whole sequence of blocks that come after it. Depending on the type of consensus implemented by the blockchain, this feature may make reversal of records on a blockchain extremely difficult, thus creating a semblance of immutability.

The immutability feature of DLT is at odds with the "right to be forgotten" granted in some jurisdictions.[56] It may also preclude effective implementation of certain remedies, in cases where actions recorded on a blockchain need to be reversed. For example, if an asset registry is transferred to a blockchain and a fraudulent transfer of title occurs as a result of a hacking attack, the title could be subsequently transferred back to the rightful owner, but the block recording the fraudster's transaction would remain on the chain. At the same time, consensus algorithms could be adjusted to provide for transaction reversal in required circumstances.

6 Looking Forward: A Functional Policy and Regulatory Approach to DLT

[56] See further D Zetzsche, RP Buckley & DW Arner, "The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain", forthcoming *University of Illinois Law Review* [add pinpoint].

Not surprisingly given the intention of non-sovereign cryptocurrencies to replace the state along with the massive investor interest in blockchain, cryptocurrencies and ICOs, policy-makers and regulators around the world have taken an increasing interest.

Regulatory measures addressing technological innovation take time to develop. Governments often stay in "listening mode" while observing the development trends and assessing the risks underlying new technologies. While regulators are waiting, businesses come up with new business models and products implementing the new technologies in practice. If successful, this implementation may delay or eliminate the need for new regulation. However, if new – especially systemic – risks emerge, a regulatory response may arrive swiftly. Urgent measures generally target specific business models or products, rather than technologies as such.

6.1 International regulatory context

The main challenge of DLT regulation lies in its multifaceted nature. Different variations of distributed ledgers can be applied across the entire financial system. As a result, the regulatory response to DLT has been limited so far. Some legislatures are attempting to provide a firm legal basis for distributed ledgers by implementing the corresponding definitions by virtue of statute.[57] Others focus specifically on blockchain.[58] The majority, however, appear silent on the matter of bespoke DLT regulation.

This does not mean, however, that DLT systems operate in a legal vacuum.[59] Both regulators and lawyers end up applying already existing legal constructs and principles, including but not limited to company, contract, torts and property law. It remains to be seen whether this is

[57] Russian draft Federal Law N 419059-7 "On Digital Financial Assets" defines a "distributed ledger of digital transactions" as a "systematic database of digital transactions that are stored and simultaneously created and updated on all nodes of all ledger participants on the basis of pre-defined algorithms ensuring its sameness among all users of the ledger". In 2017, Delaware's *Act to Amend Title 8 of the Delaware Code Relating to the General Corporation Law* (*available at* https://legis.delaware.gov/BillDetail/25730) established the legal basis for the maintenance of stock ledgers using "distributed electronic networks or databases".

[58] Arizona and Delaware have each adopted a blockchain law. See An Act Amending Section 44-7003, Arizona Revised Statutes; Amending Title 44, Chapter 26, Arizona Revised Statutes, By Adding Article 5; Relating To Electronic Transactions § 2 AZ HB2417 (2017) Cite both here

[59] For a comprehensive analysis of applicability of law to DLT generally see D Zetzsche, RP Buckley & DW Arner, "The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain", forthcoming *University of Illinois Law Review* [add pinpoint].

a temporary solution. It is likely that jurisdictions will approach the matter in different ways in the absence of international rules.[60]

Early attempts to regulate DLT have been fraught with problems of terminology, especially in jurisdictions aiming to establish special rules for blockchain. The latter concept has proven particularly difficult to define with sufficient accuracy, culminating in new rules that are not only overly simplistic, but also confusing and even misleading. For example, the new blockchain law in Arizona claims that data stored on a blockchain is "*immutable* and auditable and provides an uncensored truth", thus creating a qualitative test that is extremely hard if not outright impossible to fulfil for any DLT application, since absolute immutability is only achievable in theory and remains unrealistic in practice, at least at the current level of technology.[61]

The apparent confusion of some lawmakers and hesitation of others can be explained, at least in part, by the lack of accepted international terminology and the absence of agreed standards to define DLT and blockchain:

> Whoever is right, one thing is quite clear: the terminology around the whole phenomenon is still heavily in flux. Caught in the middle of it all, it can be difficult to form a clear picture on blockchain technology and the phenomenon that surrounds it."[62]

One of the latest attempts to fix the terminology barrier is the creation of a dedicated ISO Technical Committee ISO/TC 307[63] focusing on the development of a whole range of international standards, including ISO/CD 22739 "Blockchain and distributed ledger technologies – Terminology".[64]

---

[60] See generally A Didenko, "Regulating FinTech: Lessons from Africa", San Diego International Law Journal, (2018) Issue 19-2, 311.

[61] This matter has already attracted academic attention: a recent study challenges the simplistic approach to understanding the blockchain technology, questioning the widespread (and allegedly wishful) association of blockchain with the 'immutability' characteristic. See Angela Walch, "The Path of the Blockchain Lexicon (and the Law)", 36 REV. BANKING & FIN. L. 718 (2017).

[62] Juri Mattila, "The Blockchain Phenomenon: The Disruptive Potential of Distributed Consensus Architectures" 3 (Berkeley Roundtable of the Int'l Econ., Working Paper 2016-1), http://www.brie.berkeley.edu/wp-content/uploads/2015/02/Juri-Mattila-.pdf.

[63] See International Organization for Standardization, "ISO/TC 307: Blockchain and distributed ledger technologies", available at https://www.iso.org/committee/6266604.html.

[64] See International Organization for Standardization, "Standards Catalogue; ISO/TC 307: Blockchain and distributed ledger technologies", available at https://www.iso.org/committee/6266604/x/catalogue/p/0/u/1/w/0/d/0.

6.2 A Functional Proportional Approach Balancing Risks and Opportunities

At the most general level, the specific core attributes of DLT of security, transparency and permanence makes it highly attractive in the context of applications which benefit from these characteristics. However, it is very clear that not every application benefits from these characteristics. Therefore, the potential of DLT in any particular context varies with the needs and requirements of the individual use-case. Thus, use cases need to be considered very carefully against the core strengths of the technology. Blockchain is thus not the solution to all problems but depending on the specific context may be an appropriate – and in some cases even transformative – platform technology.

Over the medium to long term, it is likely that DLT will find its way into an increasing range of contexts and in some cases will fundamentally improve the particular system involved. Examples are likely in certain areas of financial infrastructure that benefit from security, transparency and permanence, in particular anything relating to registration or ownership of property and property rights as well as the execution of standard transactions (such as clearing and settlement system). Other examples are likely in the context of areas where a chain of custody or provenance are significant, as in the case of trade goods, artworks, jewelry, diamonds etc. In areas where speed, anonymity and fungibility are central (such as securities trading as opposed to settlement), DLT solutions are less likely to be fundamentally suitable or beneficial.

Over time, perhaps the greatest impact may simply be that the hype around DLT encourages a wide range of people to consider the design of underlying systems and infrastructure and how new technologies such as blockchain might be the basis for the redesign of these systems or the design of better systems. It is this incentive to consider aspects of underlying infrastructure (such as property registries) that may well offer the greatest long-term impact of DLT: the mere fact that it incentivizes such a process, regardless of whether or not it is eventually the chosen solution (as so far it has not be in the context of high volume payments systems).

Nonetheless, as this paper has made clear throughout, even if DLT is suitable, there are wide variations in the design and governance of systems, with permissionless public systems at one

extreme and permissioned closed systems at the other. In the context of the former, network effects mean that – as in the context of most platform technologies – there will be a trend towards consolidation and a small number of major systems will eventually dominate. In the context of the latter – already by far the most numerous and greatest focus of investment – this will not necessarily be the case, although many of these will tend to use the major platforms as opposed to creating new systems.

In any of these systems, just because it is a DLT system does not necessarily mean that it actually has the key attributes (besides that its functions are somehow distributed among several nodes): not all blockchains are created equally and there is a real need for a system of certification, ideally through the ISO or similar processes.

Whether individual jurisdictions will need specific legislation to support DLT will vary. However, jurisdictions seeking to highlight their openness to innovation as well as those with judicial systems which are less than robust may find such an approach useful. Note that the often over-stated distinction between civil and Anglo-Saxon legal families does not play a role here, since all advanced legal systems have legal instruments to deal with cooperation – which is the core of DLTs. In all cases, jurisdictions will need to consider the robustness of consumer protection legislation and enforcement arrangements in order to deal with public interactions with DLT systems. In addition, data protection rules may impact the use of DLT, given that data are spread over and stored by many nodes simultaneously.

A field where legislation could provide additional certainty, however, is in the field of conflicts of law where multiple nodes from multiple jurisdictions interact. While exclusivity stipulations in national law regarding the law applicable to torts rarely find acceptance in other jurisdictions, national legislation could clarify which law applies to DLT solutions that are legally characterised as multi party contracts and partnerships, or more precisely what type of connecting factor determines the applicable law.

Beyond the general framework of certification and standardization combined with the general legal framework and systems of consumer protection and data protection which should apply across all the various functional applications, there will also be a need to consider how specific applications fall into functional categories which draw additional regulatory attention, such as money, payment, fundraising, credit provision, insurance etc. In each case, DLT

systems should be treated according to the same general objectives and principles applicable (such as financial stability, prudential regulation, financial integrity and conduct, data protection, and competition considerations). A part of such a treatment is whether the technology itself furthers market concentration (which in turn prompts antitrust concerns).

Finally, exchanges and similar arrangements should be subject to specific attention, with differential treatment depending on the type of digital asset involved, with digital financial products exchanges a particular focus of attention.

In summary, we recommend the implementation of a functional approach:

1. In general, policymakers and regulators should treat DLT and blockchain as a platform technology which can be used across a wide variety of functional areas, from identity to property registration to financial infrastructure, payment and fundraising. Regulatory treatment should vary depending on the context.

2. At the most general level, there should be a system of categorization and certification (generally on an industry basis e.g. through the ISO) combined with the general legal system (because as demonstrated elsewhere, the reality is that the legal system will apply everywhere where there are users of the system rather than nowhere) and in particular consumer protection, data protection, choice of law/courts and competition frameworks.

3. In the absence of a DLT-focused legal regime, regulators should focus on specific applications of this technology associated with biggest risks. The recent examples of measures targeting ICOs are an illustration of this approach, where differential treatment is merited for those which are in fact financial products as opposed to those which are not (as in donation, rewards and pure cryptocurrency ICOs).

4. In addition to this functional approach, there is a clear need to focus on the public interactions with such systems and the role of intermediaries, as this is where the greatest potential risks have already arisen and are likely to arise in future (with digital asset exchanges being the most urgent focus of attention, not only from the pragmatic standpoint but also from the standpoint of addressing the largest range of market integrity, consumer protection and potential financial stability risks).

5. At the same time, policy makers and regulators should take the opportunity to better understand individual use cases and systems, balancing the opportunities presented to build better financial infrastructure with massive long term benefits while at the same time managing the many risks which arise along the way.