COLUMBIA | SIPA
School of International and Public Affairs

ENTREPRENEURSHIP & POLICY WORKING PAPER SERIES

Regulation of the Financial Components of the Crypto-Economy

Leon Perlman

In 2016, the Nasdaq Educational Foundation awarded the Columbia University School of International and Public Affairs (SIPA) a multi-year grant to support initiatives at the intersection of digital entrepreneurship and public policy. Over the past three years, SIPA has undertaken new research, introduced new pedagogy, launched student venture competitions, and convened policy forums that have engaged scholars across Columbia University as well as entrepreneurs and leaders from both the public and private sectors. New research has covered three broad areas: Cities & Innovation; Digital Innovation & Entrepreneurial Solutions; and Emerging Global Digital Policy. Specific topics have included global education technology; cryptocurrencies and the new technologies of money; the urban innovation environment, with a focus on New York City; government measures to support the digital economy in Brazil, Shenzhen, China, and India; and entrepreneurship focused on addressing misinformation.

With special thanks to the
Nasdaq Educational Foundation for its support of
SIPA's Entrepreneurship and Policy Initiative.

Table of Contents

Abstract **1**

Acronyms and Abbreviations **3**

1 Introduction **5**

1.1 Overview 5

1.2 Paper Scheme and Methodologies 8

2 The Concepts of Blockchains and 'Distributed Ledgers' **8**

2.1 Key Concepts 8

2.2 Transformational Components and Effects of Distributed Ledgers 10

2.3 Evolution of Distributed Ledger Technologies 10

2.3.1 Overview 10

2.3.2 Consensus Mechanisms in Some Distributed Ledgers 11

2.3.3 Enhancing DLTs through 'Layer' Solutions 11

2.4 Typical Actors in a Distributed Ledger 12

2.5 Evolving Use Cases of Distributed Ledger Technologies 13

2.6 Active Components of DLTs 14

2.6.1 Overview 14

2.6.2 The Criticality of Tokens 14

2.6.3 Crypto-Currencies 15

2.6.4 Initial Coin Offerings (ICOs) 16

2.6.5 Utility Tokens 16

2.6.6 Security Tokens 17

2.7 Digital Fiat Currencies 17

2.8 Crypto-Wallets 17

2.9 Decentralized Apps (dApps) 17

2.10 Smart Contracts 17

3 The Crypto-Economy: Tokenized Crypto-Assets and Use in Decentralized Finance . . . 18

3.1 Overview . . . 18

3.2 Legacy and DeFi . . . 19

3.2.1 Legacy . . . 19

3.2.2 Decentralized Finance . . . 19

3.3 Decentralized Autonomous Organizations . . . 22

3.4 International Interbank Transfers . . . 22

3.5 Trade Finance . . . 23

3.6 Factoring . . . 23

3.7 Capital Markets . . . 23

3.8 Prediction Markets . . . 24

4 Trading in the Crypto-Economy . . . 25

4.1 Overview . . . 25

4.2 Centralized Exchanges . . . 26

4.3 Decentralized . . . 27

4.3.1 Exchanges . . . 27

4.3.2 Platforms . . . 27

5 Risks in the Crypto-Economy . . . 27

5.1 Overview . . . 27

A Trust Frameworks . . . 27

5.2 Custodial Issues and Key Management . . . 27

B Market Conduct and Integrity . . . 28

5.3 Addressing Money Laundering . . . 28

5.4 General Competition-Related . . . 28

5.5 Security Risks . . . 29

5.6 Trust in ‘Oracles’ . . . 30

5.7 No Standardized Rating Systems . . . 30

C Trading Risks . . . 30

5.8 Trading Platform Risks . . . 30

5.8.1 Overview . . . 30

5.8.2 Lack of Safety in Crypto-Asset Key Custody . . . 31

5.8.3 Technology Reliability, Standardization and Scaling . . . 31

5.8.4 Competition-Related . . . 31

5.8.5 Veracity of Trading Data . . . 31

5.8.6 Counterparty Risk . . . 32
D Technology Risks . . . 32
5.9 Speed and Scalability . . . 32
5.10 Lack of Technology Standardization . . . 33
6 Regulatory Approaches to the Sample Financial Components of the Crypto-economy . . . 33
6.1 Overview . . . 33
6.2 Regulatory Philosophies . . . 33
6.3 Types of Regulatory Foci . . . 34
6.4 Approaches . . . 35
6.4.1 No Action . . . 35
6.4.2 Regulatory Forbearance . . . 35
6.4.3 Restrictive . . . 35
6.4.4 Bring into Scope . . . 35
6.4.5 Bespoke . . . 36
6.4.6 Hybrid Approaches . . . 36
6.5 Stylized Application of the Approaches . . . 36
6.5.1 Exchanges . . . 36
6.5.2 Data Reporting and Record Keeping . . . 38
6.5.3 Custodial and Safekeeping Services . . . 39
6.5.4 Clearing and Settlement, and Settlement Finality . . . 39
6.5.5 Underlying Technology Use and Development . . . 40
6.5.6 Security of Transaction Systems and Data . . . 42
7 Regulation of the Crypto-Economy: Select Country Focus Summaries . . . 43
8 Conclusions . . . 46
Annex A. Consensus Protocols . . . 55
Annex B. Stablecoin Varieties . . . 56
Annex C. Regulatory Approaches in Various Regions . . . 57
Annex D. Model Crypto-asset Regulatory Framework . . . 71
Endnotes . . . 73

SIPA's Entrepreneurship & Policy Initiative Working Paper series

Regulation of the Financial Components of the Crypto-Economy

by Leon Perlman[I]

Abstract[II]

The emergence into the public discourse in 2009 of the novel peer-to-peer Bitcoin crypto-currency phenomenon caught many regulators unawares. We now know that Bitcoin and its underlying 'blockchain' technology represented a transformational vanguard of a new 'trustless' method of sharing data and processes and contracting in a decentralized, traceable and secure manner and, in many cases, without the need for intermediaries. The family of blockchains and its analogues are now known as distributed ledger technologies (DLTs).

Whatever their form or function, 'crypto'-derived and focused products and services based on DLT are here to stay. They are transformational not just of their utilitarian function in making data transfer and storage more efficient, but notably we argue also in their potential to democratize access to financial products and services, a change not seen the dawn of the commercial Internet in the 1990s. There are still many hurdles and risks to overcome though before they become mainstream, not least of which is regulatory certainty.

The 'crypto-economy', as we dub it, has many avenues for transformation by DLTs. This may be through DLT's novel utilitarian function of new data sharing and storage techniques that are secure, tamper-evident and distributed. Or the introduction of new financial products and trading techniques through the production and use of new 'crypto-assets' that feature at their core malleable crypto 'tokens' used as 'programmable money.' The financial sector in particular is seeing the release of these new asset classes that democratize access to financial products through tokenization, catalyzing and enabling fractional ownership of legacy and new crypto-inspired asset classes. Some of these crypto-assets have attached profit or governance rights, others providing some consumption value. They may also act as payment tool as a crypto-currency, enabling the buying and selling of goods and services. The crypto-economy may also support capital raising through a now controversial method called an Initial Coin Offering.

Overall, there is currently a bifurcation of interest in DLTs, between retail (individual consumers) and enterprises. The former are more engaged in trading of crypto-assets. Indeed there are few live mass consumer applications of DLT other than this direct trading. The focus by the latter is mostly on the utilitarian aspects of DLTs, as reliable, traceable and secure data processes and access. A number of DLTs are being developed by sector consortia of banks and other financial institutions, or shipping companies, or food supply networks. There is likely to be a convergence of the retail and enterprise focus areas over the next few years as the industry matures.

[I] Leon Perlman Ph.D.; Head: Digital Financial Services Observatory, Columbia Institute for Tele-information, Columbia University, New York.

[II] This paper was supported by a grant by Nasdaq, the world's first electronic stock exchange, to the Columbia School of Public Affairs (SIPA) for the study of entrepreneurialism. I thank Nasdaq and Dean Merit Janow. I am also extremely grateful to Michael Wechsler for contributing extensively to the country focus sections, and to Shija Mao for her valuable research assistance. And to Professor Eli Noam for his highly supportive role and comments on early drafts.

The technologies, products, services and even the participants and actors providing services are novel and will not only change business practices but also test the perimeters of current sets of regulations and the remits and capacity of regulators and authorities that may found remit over them. These effects may be magnified by the innate fluidity of crypto-assets, where the programmable 'tokens' underpinning them can rapidly morph from one type to another. And similarly, what is decentralized at one moment may become semi-centralized in another. This fluidity creates challenges in regulatory planning and oversight. Given their mandates of consumer protection, regulators have focused their initial regulatory responses on the retail components, particularly on crypto-currency trading and ICOs.

While the crypto-economy, as measured by capitalization compared to the real (legacy) economy, does not as yet raise any systemic concerns, the emergence of institutional investors will alter that calculus and accelerate we argue the need for regulatory planning or action. A general problem though is whether 'old' laws and regulations not specifically referencing DLT technologies, their development, use and application can be used for these new technology shifts and crypto-asset classes. Answering this is the primary goal and contribution of this paper.

In doing so we describe in some detail: the technical components of emerging distributed ledger technologies, their strengths and weaknesses; their potential business application and risks of crypto-assets used in a nascent crypto-economy; and the open legal, regulatory and policy dilemma this all presents to regulators, authorities and lawmakers, as well as to provide some suggested solutions. And similarly, for this crypto-economy to evolve from a current, relatively small pool of participants and traders, systems need to be hardened and operational and market integrity risk profiles decreased so as to attract institutional investors that can bring trillions of dollars for use in creating and trading tokenized assets.

This paper also contributes with a novel systemized taxonomy for classification of the various financial components of the crypto-economy, particularly crypto-assets and their token components. It describes their provenance, use and risks in a technical, business and legal sense. We show how the ecosystem has developed and how it can be used in the broader economy, where the weak points are, what the initial regulatory and policy responses have been, and what stylized legal and regulatory responses may be appropriate to bring certainty and order, close gaps, and remove arbitrage where and if needed. In later sections, we show how regulators in some countries have approached this.

The issues are complex, potentially disruptive and definitely transformative. In this being a challenge to regulators and policy makers, we argue that there is a familiar lens: the transformative impact of the introduction of the commercial Internet in the 1990s and the tension it ventilated between innovation and regulation.

We suggest for use by regulators boilerplate methodologies, challenges and strategies for approaching their task of understanding the components, actors, and risks in the crypto-economy, and suggest stylized solutions where they can be applied. We stylize the regulatory approaches as being: no action; forbearance; restrictive; bring into scope; bespoke; and a hybrid approach. We suggest that a hybrid of 'bringing into scope' and a new crypto-asset regulatory framework is a desirable approach given the nascent and fluid nature of DLT and crypto-assets. A novel model crypto-asset regulatory framework is again presented, modified following its use in an earlier study by the author.

We note too that a functional regulatory approach versus an institutional approach is preferred, given that many of the new models are organized into a decentralized, rather than in a readily identifiable (legacy) entity-based manner. Principles-based regulation, we argue, has a perimeter of utility and effectiveness and in many cases that approach may need to be adapted to the new actors and asset classes, governance structures, and to the overall impact of these technologies. Thereto, the effect of DLTs on legal and policy concepts of *inter alia* payment finality; on laws of evidence; contract law; laws of negotiable instruments; and on data protection is also discussed.

A balance of strict, normative regulation versus effective, but nurturing regulation may be needed. This we note to be the regulator's dilemma.

Acronyms and Abbreviations

ABFT	Asynchronous Byzantine Fault Tolerance
ADE	The Revenue Agency
ADR	Alternative Dispute Resolution
AGID	Agency for Digital Italy
Altcoin	Alternative Coin
AML	Anti-Money Laundering
ASICs	Application-specific Integrated Circuits
BaaS	Blockchain-as-a-Service
BCB	Central Bank of Brazil
BdeM	Bank of Mexico
BdI	Bank of Italy
BIP	Bitcoin Improvement Proposal
BOT	Bank of Thailand
BTC	Bitcoin
BTH	Bitcoin Cash
C&S	Clearing and Settlement
CAC	Cyberspace Administration of China
CADE	Council for Economic Defense
CB	Central Bank
CBDC	Central bank digital currency
CBK	Central Bank of Kenya
CC	Crypto-currency
CDP	Collateralized Debt Position
CFT	Countering the Finance of Terrorism
CFTC	Commodity Futures Trading Commission
CMA	Capital Markets Authority
CNBV	National Banking and Securities Commission
CSA	Canadian Securities Administrators

CSRC	China Securities Regulatory Commission
CVM	Securities and Exchange Commission
DAB	Digital Asset Business
DAG	Directed Acylic Graph
DAO	Decentralized autonomous organization
dApps	Decentralized Applications
DC	Digital Currency
DCEP	Digital Currency for Electronic Payment'
DDOS	Distributed Denial of Service
DeFi	Decentralized Finance
DEX	Decentralized Exchange
DL	Distributed Ledger
DLT	Distributed Ledger Technology
EC	European Commission
ECB	European Central Bank
eIDAS	Electronic identification and trust services
EMI	Electronic Money Institutions
ERC20	Ethereum Request for Comment 20
ETC	Ether Classic
EU	European Union
EVM	Ethereum Virtual Machine
FATF	Financial Action Task Force
FCAC	Financial Consumer Agency of Canada
FIC	Financial Intelligence Centre
FINCEN	Financial Crimes Enforcement Network
Fintech	Financial Technology
FIU	Financial Intelligence Unit
FMA	Financial Market Authority

FSCA	Financial Sector Conduct Authority
FSR	Financial Services Regulator
ICE	Initial Exchange Offering
ICO	Initial Coin Offering
IFC	International Finance Corporation
IFPE	Electronic Payments Funds Institution
IFWG	Intergovernmental Fintech Working Group
IIROC	Investment Industry Regulatory Organization of Canada
IMF	International Monetary Fund
IoT	Internet of Things
IRS	Internal Revenue Service
ITF	Financial Technology Institution
KYC	Know Your Customer
LTC	Litecoin
MEF	Ministry of Economy and Finance
MNO	Mobile Network Operator
MOIT	Thailand's Ministry of Industry and Trade
NT	National Treasury
OSC	Ontario Securities Commission
PBC	People's Bank of China
POET	Proof of Elapsed Time
POS	Proof of Stake

POW	Proof of Work
PT	Payment Token
PrT	Protocol Token
RBI	Reserve Bank of India
RCL	Ripple Consensus Ledger
Regtech	Regulatory Technology
RFB	Department of Federal Revenue
SARB	South African Reserve Bank
SARS	South African Revenue Service
SBP	State Bank of Pakistan
SBV	State Bank of Vietnam
SC	Smart contract
SEC	Securities and Exchange Commission
SHCP	Ministry of Finance and Public Credit
SSC	State Securities Commission
ST	Security Token
STO	Security Token Offering
TGE	Token Generation Events
TPS	Transactions Per second
UT	Utility Token
VAT	Value Added Tax

1. Introduction

1.1 Overview

The emergence into the public discourse of the novel peer-to-peer Bitcoin crypto-currency phenomenon during the course of 2009 caught many regulators unaware. Many at the time were still struggling to incorporate fiat-backed electronic money (e-money) into their regulatory frameworks, as well as in many developing countries, understand the emergence of 'mobile money' systems being offered to the public by non-banks. They were also trying to figure out how to save the world economy.[1]

Bitcoin though, was the transformational vanguard of emerging 'cyber-punk' aficionados – now calling themselves 'Maximalists'—who coveted Bitcoin and its 'decentralized' design as the catalyst and the beginning of the end of 'centralized' central bank 'hegemony' over the issuance and control of money and indeed even the need for trusted 'legacy' institutions such as banks, stock-exchanges and other traditional intermediaries.[2]

'Trustless'—more the *need* not to trust someone—is coveted in this new paradigm. Anyone—'nodes' as they are known in the decentralized 'crypto world'—with basic communication facilities could participate in this new decentralized ecosystem.

When anonymous peer-to-peer crypto-currencies like Bitcoin began to gain traction and gain in value from 2011 onwards, moving from a penny novelty[3] with little real utility to one of increasing values, it was soon evident to many regulators that this was new ground. The most obvious, visceral reaction for some was to place restrictions on the possession, use or trading of Bitcoin.[4] The possible transformational use of its underlying 'blockchain' technology—and so its general use beyond Bitcoin—was not entirely evident as it is today and so did not feature then in their regulatory-response calculus. But even if there was interest by some governments and regulators following its evolution, this was quenched to a large extent by news reports of Bitcoin being embraced by bad actors who were apparently using the nascent largely anonymous, decentralized currency to buy industrial quantities of hard drugs and even to hire hitmen on the dark web.[5] The money laundering implications and the watchful eye of the global Financial Action Task Force (FATF)[6] loomed large over any decision-making by regulators. For many countries, public policy would not allow embracing of Bitcoin or any of technical components for 'mainstream' use.

As the technology underpinning Bitcoin has evolved and other and more sophisticated blockchains emerged, the term 'Distributed Ledger Technology' (DLT) emerged to describe the family of blockchains and similar technologies with the distributed, trustless decentralization theme as their lodestar. 'Distributed' here refers to the data on a distributed ledger (DL) being housed and processed remotely in a scattered fashion by the (mostly anonymous) nodes,[7] such that failure of one node does not impact anyone else on the DL unless the DLT design allows for that. Where a lack—for whatever reason—of nodes does impact, though, is determining whether a DL is decentralized. Less nodes means not necessarily decentralized, although that measure and quantification is still fuzzy. A fully decentralized system may attract a different regulatory response or regime than a semi-decentralized one, making regulatory certainty more fluid.

That noted, DLTs may provide an impetus for new sets of laws, regulations, policies, and internal rules. A general problem is whether 'old' laws not specifically referencing DLT technologies, their development, use and application can provide guidance for these new technology shifts and circumstances.

We've been here before, seemingly: the singularity of the introduction of the web browser operating over the native TCP/IP protocol around 1990[8] catalyzed the emergence of the commercial internet, altering soon conceptions of and methodologies for, *inter alia*, retail trade (through seamless e-commerce) and intellectual property (effortless distribution of context and entertainment assets). This protocol, though, was a form of 'dumb' piping that transported through packets the valuable data above and along it. The transformative nature of that time challenged legal norms by necessitating new rules and laws for contracting through the Internet and use of electronic data for evidentiary purposes. It became the 'internet of content,' going from the 'basic' Web 1.0 of the 1990s, to Web 2.0 with its vast array of media-rich applications and e-commerce.[9] In both generations, centralization was key, with Facebook, Amazon, Google and Apple dominating availability, purchasing and use of content and other assets.

The singularity of the DLT world here is that of the emergence of distributed ledgers and the protocols that empower them, and operating in a decentralized manner with (ostensibly) no single entity controlling a DLT.[10] That is, for any of its protocols, instead of being 'dumb' pipes that simply carry data and valuable applications above them, with DLTs the value can be and is embedded *inside* the protocol itself. One could now call this shift the equivalent of the 'internet of value,' or Web 3.0 as some term it.[11] In this latest transformation, centralization is replaced by protocols that facilitate and allow data—and thus innate, embedded value—to be distributed. In a nod to the decentralization motif of DLT, this could be without a central control point mediating what can be sent, used and seen.

Disassembly of the components of the DLT protocol demonstrates that there are two components at play: the technical parts that mediate the interactions with other users of the protocol (the nodes) and the business end called 'tokens' that—depending on the DLT protocol—are entirely programmable, even as a form of 'programmable money.'

That is, where the token has an asserted value that can be used to trade with others, it becomes a type of asset. Hence the emergence of the term 'crypto-asset' (CA) to describe a growing number of these programmable token types using new DLTs and protocols. So-called decentralized applications (dApps), such as automated execution systems called 'smart contracts' sitting atop the protocol stack in the DLT hierarchy, can use these crypto-assets as a means of payment for goods and services and also for facilitating the use of the smart contract to pay technical participants called 'miners or validators.' In some cases, the token and the application may be the same thing. For example, the genesis DLT, the Bitcoin[12] blockchain, also has as its crypto-asset its native 'coin,' Bitcoin.

As this token-based ecosystem has rapidly evolved, the term 'crypto-assets' gained traction to describe the class of crypto-based value archetypes. Thus, crypto currencies (CC) has become the genesis token, followed by initial coin offerings (ICO), utility tokens (UT), security tokens (ST), and the most recent incarnation—initial exchange offerings (IEO).

The CC class has functionally-specific components. We term them protocol tokens (PrTs),[13] payment tokens (PT); and stablecoins. PrT are native to the DLT that birthed them, used as a reward and incentive system for the 'miners'[14] who use their own computing power for technical maintenance of the DLT such as adding blocks to a blockchain and/or crypto-graphic validation of the provenance of blocks. In some DLT systems using the POS protocol, PrTs can be used for 'staking' a right to validate the blocks and being able to 'vote' on technical or any other changes to that DLT ecosystem. This governance of a DLT component is called 'staking.' They can be traded on secondary markets through an exchange or directly with a counterparty. Payment tokens (PT) can be used as a generalized means of exchange for paying for goods and services by whoever will accept them as such. Stablecoins have stabilization components which allow them to hold value by being less volatile in their valuation. Some stablecoins though could be seen as STs by some regulators.

In almost all these types, tokens specific to a DLT are issued and distributed. Their initial value can be determined by the issuer or the exchange. While some tokens have purely functional use[15] and thus invariably may not necessarily be assigned value and then even traded, others can be created, issued and then sold directly as one of the CA classes to interested parties by the creator/issuer themselves. Or they can be created and issued through a special crypto-oriented or focused exchange on behalf of the creator as an IEO. These exchanges can also trade these tokens on in a secondary market. Tokens can also be given away (usually free) by the creator through what is now known as an 'airdrop'[16] process,[17] often applied as an incentive purpose much like redeemable store rewards. Token distributions (issuance) have been known as 'token distribution events.'

These tokens as CAs, when traded, can become very valuable when measured in fiat currency. Their value often fluctuates widely though, pointing to reflexivity of the trustless, decentralized ecosystem which mostly has no solid anchor[18] outside of participants' assessments—making them inherently unstable.[19] This volatility and often stratospheric values mean that it becomes good practice to securely store them in some way, either offline by the owner or custodian, or online by a custodian and/or exchange. All these methods have risks. Exchanges that trade them thus also need to be secure and keep their trading systems accurate, fair and transparent, practices that are not always adhered to and which have led to hack of some exchanges and massive loss of customer value.

While these nascent CAs develop from the underpinning of Web 3.0, they are forming part of what can be called the 'crypto-economy.' This can involve tokenization of 'legacy' assets such as securities, streamlining of legacy processes, but transformationally, introduce new actors[20] who invent and provide access to new asset classes and financial processes as a type of 'democratization' of access to finance and instruments. This latter transformation has become known as Decentralized Finance (DeFi). Simply put, the ideal of DeFi's proponents is that DLTs provide the technical and business process means to 'tokenize' any asset, market or service which can be accessed and bought, even fractionally, by anyone with access to the tokens. Music royalties, stocks, and indeed anything of (legal) value is tokenizable. This ideal of fractionalization is the native business and technical feature of the emerging crypto-economy, with fractionalization using DLT-based tokens seen then as the catalyst for a transformative democratization of access to finance. For some, DLTs and DeFi are a solution looking for problem to solve.

Not surprisingly, alongside this rush to tokenize, bad actors and equally bad business practices have quickly crept in. Often some of the activities are legally dubious[21] or outright illegal. ICOs have been particularly prone to bad actors and practices, while crypto-asset exchanges have been hacked and substantial value stolen. Some have been alleged to have falsified trading volumes to inflate their popularity and/or (potentially) to inflate prices of the assets traded. Legal, regulatory and policy uncertainty surrounding the ecosystem overshadows its evolution, with a potentially chilling effect on innovation. There are also additional risks to the crypto-economy, same native to the nascent ecosystem, and others analogues or the same as 'legacy' systems. Cyber-security risks are omni-present.

But, as noted earlier, regulators were slow to respond to the Bitcoin phenomenon as it gained traction in many markets, and, in time, conflated the crypto-currency with the underlying 'blockchain' technology.[22] A more nuanced understanding of the differences has emboldened regulators to even test DLT for their own internal use[23] and to investigate creating their own central bank digital currencies (CBDC), also known as digital fiat currencies (DFCs).[24]

But screaming headlines about fraud in ICOs, general uncertainty about the nature and legality of ICOs and other CA classes has led to a clampdown by many regulators who have calibrated their responses according to whether and how the nascent CAs fit into existing legal, policy and regulatory frameworks. The approach is particularly focused on classification of financial instruments, tax implications, and within financial market infrastructure (FMI)[25] regulations. There have also been assessments of whether there are systemic implications of CCs to an economy, but none have yet been found.[26]

Yet other regulators embraced forbearance, while others—especially smaller jurisdictions eager to attract fintech innovators and capital—have developed bespoke CA frameworks. Standard Setting Bodies such as FATF and pan-continental bodies such as the European Commission (EC) are still in the early stages of developing crypto-economy wide policies. Besides the policy issues—that is, how far (if at all) DLTs and their applications such as crypto-assets—can be implemented in specific sectors, there are also open legal and regulatory issues to consider.

While the crypto-economy as measured in capitalization does not as yet have any systemic effect on any national economies, the emergence of institutional investors may alter that calculus. Regulators need to be prepared for this.[27]

This paper provides a novel systemized taxonomy for classification of the various (financial) components of the crypto-economy, particularly crypto-assets and their token components and describing, in semi-technical detail, their provenance, use and risks at a technical, business and legal sense. We show below how the ecosystem has developed and how it can be used in the broader economy, where the weak points are, what the initial regulatory and policy responses have been, and what potential legal and regulatory responses could be appropriate to bring certainty and order where and if needed. A novel model 'crypto-asset regulatory framework' is also presented.[28] In later sections, we show how regulators have approached some selected risks and the emergence of the technologies and new asset classes themselves.

We argue that, for regulators and policy makers, there is a familiar lens: the impact of Web 1.0[29] in the 1990s and the tension it ventilated between innovation and regulation. Finding a balance is the regulator's dilemma.[30] And similarly, for this nascent crypto-economy to evolve from a current relatively small pool of participants and traders, systems need to be hardened and risk profiles decreased to attract institutional investors that can bring trillions of dollars for use on creating and trading tokenized assets such as STs.

The combination that this new technology and thoughtful regulatory responses we argue will aid in a transformative democratization of use and access to finance and in developing new financial instruments and asset classes, but in a calibrated manner that does not have negative systemic implications.

1.2 Paper Scheme and Methodologies

The paper is organized in the following way:

- Section 1 introduces the paper and its goals.
- Sections 2-5 outline key contextual and technical information that informs any potential regulatory approaches.
- Section 6 outlines potential regulatory areas of interest and regulatory approaches.
- Section 7 contains highlights of recent regulatory approaches to DLTs and the crypto economy in sample jurisdictions, with further details provided in Annex C. Only normative regulations/rules as well as official statements and policies were included. No analogous self/co-regulations and rules were included.
- Section 8 contains the paper's conclusions, as well as suggesting boilerplate methodologies and strategies for regulators to approach the task of understanding the components, actors, and risks and where and if regulations can and should be applied.

This paper embraces and uses the technical term Distributed Ledger Technology (DLT) to describe all distributed ledgers, no matter what underlying DLT technology or protocol is used.[31] Where needed, the term blockchain is used interchangeably with DLT as the primary exemplar of DLT.

Overall, unless otherwise stated, any reference to 'Bitcoin' is to what is now known as Bitcoin Core and its underlying technology and traded under the ticker symbol BTC. The BTC price used in this paper is of June 4, 2019.

The taxonomy, ontologies and terms used in this paper for categorizing components of the DLT ecosystem and the 'crypto-economy,' as we dub it, is our own. Where the taxonomy, ontologies and terms differ from, are similar or identical to other taxonomies or terms of art, this is so stated and explained.

Given space constraints and readability, the regulatory components discussed in this paper do not represent a *numerus clausus* of all regulatory issues related to DLTs and the crypto-economy. That we leave to further studies.

Research for this paper was conducted through desktop research and direct interactions by the author with regulators and ecosystem developers and participants and other experts. The author thanks them for their invaluable and forthright insights.

The technologies cited, as well as any laws, policies, and regulations quoted are as of May 31, 2019.

All citation hyperlinks where provided in the footnotes were checked for online availability during the period May 10, 2019 to June 6, 2019. To improve readability of the footnotes, hyperlink shorteners have been used in some cases.

2 The Concepts of Blockchains and 'Distributed Ledgers'

2.1 Key Concepts[32]

Distributed ledger Technology (DLT) is a new type of secure database or ledger that is replicated across multiple sites, countries, or institutions with no centralized controller. In essence, this is a new way of keeping track of who owns a financial, physical, or electronic asset and in newer iterations, automating these interactions. As shown in Exhibit 1, the core motif of DLT is that of 'decentralization,' where there is no single controller of the DLT.[33]

The concept of DLTs emerged after the launch in 2008 of the Bitcoin,[34] now known as the first 'decentralized' crypto-currency. The design called for the crypto-currency[35] information to be stored on blocks which would be added sequentially in a chain. The chain would be the sole record of the use of Bitcoin. To avoid any double-spending of the currency, additions of blocks to the chain would be authenticated by those (now known as nodes) who have access to the blocks. Additions would be confirmed through a consensus mechanism and actual additions, once confirmed through consensus, would be undertaken through what are now known as 'miners,' who would solve a cryptographic puzzle devised by Nakamoto and be rewarded for doing so by the nodes. Usually that reward is in the native Bitcoin currency, which could be traded for other values, currencies or services.

Bitcoin's decentralized transaction authentication rests on blockchain approaches: It records in a digital *ledger* every transaction made in that currency in identical copies of a ledger which are replicated—*distributed*—amongst the currency's users—*nodes*—on a chain of data blocks.[36] As the system gained traction, the term 'blockchain' was used to describe Nakamoto's chain and blocks. The Bitcoin blockchain is the archetype and other 'blockchains' with more functionality other than use as a crypto-currency have been developed. Ethereum, launched in 2014, is the most popular and flexible blockchain, allowing the development of other types of use cases, including so-called crypto-assets.

Blockchain, though, has its technical limitations, particularly in the speed of being able to add blocks. Nakamoto, for example, purposely added a ten minute wait time for Bitcoin blockchain blocks to be chained together sequentially, ostensibly to allow the nodes scattered around the world enough time to reach consensus about addition of any particular block. Other versions of Bitcoin try to speed this up but, in modifying the protocols, face security issues. Attempts to have maximum/optimal levels of scale, governance and security in a blockchain has been termed the 'blockchain trilemma.'[37] Newer technologies have emerged that embrace the decentralized, no-control, distributed motif of blockchain 'ledgers.' They don't, however, necessarily use blocks, and if they do, these are not necessarily added sequentially in a chain.

There are similar technologies to blockchain. But since all these definitions and concepts relating to these technologies ultimately refer to databases which are *distributed*, the term DLT is commonly used as a term of art by those in the technology development community as the generic descriptor for any distributed, encrypted database and application that is shared by an industry or private consortium, or which is open to the public.[38]

This paper embraces and uses the technical term DLT to describe all distributed ledgers, no matter what underlying sharing technology or protocol is used.[39] Where needed, the term blockchain is used interchangeably with DLT as the exemplar of DLT.

Centralized connection of counterparties using a server

Decentralized connection of counterparties using DLT nodes

Exhibit 1: Differences between legacy centralized and blockchain-powered distributed methods of storing and accessing data. Blockchain technology, as an example of a DLT, has as its most disruptive innovation the elimination of the need for third party intermediaries in favor of *distribution* of the data across participant nodes. This means that every participant—a *node*—in a blockchain can keep—*share*—a copy of the blockchain. The blockchain updates the nodes automatically every time a new 'transaction' occurs. Accuracy of the information is maintained through synchronization of the nodes, so that the information on each node precisely matches each other node.

2.2 Transformational Components and Effects of Distributed Ledgers

DLTs generally integrate a number of innovations which include: Database (ledger) entries that cannot be reversed or otherwise modified, the ability to grant granular permissions, automated data synchronization, rigorous privacy and security capabilities, process automation, and transparency, such that any attempts at changes to entries will notify others. Its main disruptive attribute is that it is decentralized and therefore not dependent on a central controller or storer of the data.

While there are still significant challenges in the development and implementation of DLTs, many incorporate some or all of the following design features:

- ‘Distributed’
- ‘Decentralized’
- Consensus mechanisms
- Cryptographic techniques to reach consensus on data entry and accuracy
- Scalability
- Transparency of data entry
- Authentication of the entry of data
- Disintermediation of trust
- Replication of data to avoid single point of failure
- Evidence of tampering[40]
- Borderless
- Quick to update
- Permanent uptime
- Access control & authentication through cryptographic keys
- Smart, self-executing contracts.[41]

A blockchain is distributed at a minimum, and decentralized to degree that those using it allow, so does not reside in a central place. It is said then to be distributed across nodes. The data on the blockchain may or may be shared in the sense that while it may be on the blockchain, it may only be visible to (and/or editable for) those with an appropriate cryptographic key. Layers of permissions for different types of users may be necessary. There are hybrid iterations though, with some privacy components called zero-knowledge proofs being built atop even the public, permissionless DLTs.

Anyone can, with the right tools, create a blockchain and decide who can see the data in the blockchain, or add data to it. Banks, governments, and private entities are rapidly developing and implementing blockchain-based solutions worldwide.

These innovations also prompt a number of challenges related to their implementation, including the nascent (and often not yet properly stress-tested) nature of the technologies used; uncertain legal and regulatory status; privacy and confidentiality issues; cultural changes in requiring users to have ‘trust’ in often anonymous counterparties; scalability of the DLTs for mainstream use comparable to and exceeding existing non-DLTs performing similar functional tasks;[42] and the ability to link[43] different DLTs together, where required.[44]

2.3 Evolution of Distributed Ledger Technologies

2.3.1 Overview

Two major types of DLTs have evolved over the past few years. The blockchain is the oldest, being derived from Nokamoto white paper. The second DLT type gaining traction though is Directed Acylic Graph (DAG).[45] As the technology evolved and more uses have been found for DLTs, scalability and speed issues have necessitated ‘redesigns’ of blockchain, including the emergence of smart contracts, lightning networks, and DAGs.[46]

The Forbes Global 2000 list of 2018 of the world’s largest public companies indicates that not only are all ten of the largest public companies in the world exploring DLTs but at least 50 of the biggest names on the list have already done so.[47]

The emergence of Ethereum technology enabling many new features and ostensibly speeding up transactions led to it being called ‘Blockchain 2.0’[48] in so far as it builds upon the ‘Blockchain 1.0’ idea of exchanging value—primarily currency—in a peer-to-peer and decentralized manner such as Bitcoin.[49] Now with ‘Blockchain 2.0,’ what is (additionally) being transferred are programmable smart contracts which developers can program transactions and make them execute only under specific circumstances.

An important application of the use of blockchain technology is the Bitcoin crypto-currency. All blockchains operate by taking a number of records and putting them in a block and then chaining that block to the next block, using a cryptographic signature. The method used to validate the accuracy of a distributed ledger is known as 'consensus.'[50] **See Section 2.3.2** for the types of consensus mechanisms.

The *manner* in which consensus for proposed changes to the ledger is reached defines the type of blockchain.[51] If the process is open to everyone—such as with Bitcoin[52]—then the ledger is said to be 'permissionless' and the DLT has no owner. If participants in that process are preselected, the ledger is said to be 'permissioned.'[53] These may also be public[54] or private. IOTA's Tangle is designed to mediate use of Internet of Things (IoT) devices.

2.3.2 Consensus Mechanisms in Some Distributed Ledgers

To add data to a blockchain, so-called consensus mechanisms have evolved that require a miner (validator) to prove that they have undertaken the task of being able to add the blockchain to the chain. Bitcoin and Ethereum (for now) uses proof of work (POW), while proof of stake (POS) has evolved to solve, *inter alia*, the power consumption issues in POW as well as scaling[55] issues.

DLT Type	Consensus Mechanism	DLT Examples
Public	Proof of Work	Bitcoin, Ethereum, Zcash, Monero, SiaCoin
Public	Proof of Stake	Tendermint, Ethereum (W/P)
Public	Delegated Proof of Stake (dPoS)	Lisk
Private	Proof of Elapsed Time (PoET)	Hyperledger Sawtooth
Private	Practical Byzantine Fault Tolerance (PBFT)	Hyperledger Fabric (FT), Hyperledger Indy (RBFT), Hyperledger Iroha (Sumeragi)
Federated	Stellar Consensus Protocol	Stellar Network
Federated	Ripple Consensus Algorithm	Ripple Payment System and Crypto-currency

Exhibit 2: Consensus protocols in use in various DLT types.[56]

2.3.3 Enhancing DLTs through 'Layer' Solutions

The emergence of a number of DLTs, each with their strengths and weaknesses and targeting a particular vertical—finance (fast), or ID (privacy)—has led to a number of what are known as 'off-chain' additions designed to enhance the native DLT without needing a complete overall. The distinction then between the original and the enhancements is said to be Layer 1 and Layer 2, with the former said to on-chain and the latter off-chain. Exhibit 3 demonstrates this hierarchy.

On-chain then refers to blocks on the native Layer 1. Any data (even in blocks)—say on Layer 2 or from/to oracles—is said to be 'off-chain.'

New solutions are being developed to solve the Achilles heel of most Layer 1 DLTs: speed of transaction processing, and scalability to allow more transactions to be processed. The issue for some of the most popular blockchain versions of DLTs—Bitcoin core and Ethereum—is that it takes longer than commercially desirable when compared to current centralized solutions for blocks[57] to be added to a chain to advance the blockchain.[58] These block addition times are mediated (and ultimately, delayed) by waiting for consensus to reach this required finality. Each protocol[59] has its own rules for block addition.[60] Whatever the protocol, the principle is the same: no finality means there is a potential for reversal of the putative addition.

Layer 2 solutions attempt to solve this issue by undertaking the processing of transactions between parties relatively faster than on Layer 1. When a transaction needs to be settled, the record thereof, and the actual settlement is done on the Layer 1. In effect then, Layer 2 for transaction processing, and batches of transactions (if more than one) between parties are cleared and netted at Layer 2, with the settlement on Layer 1.

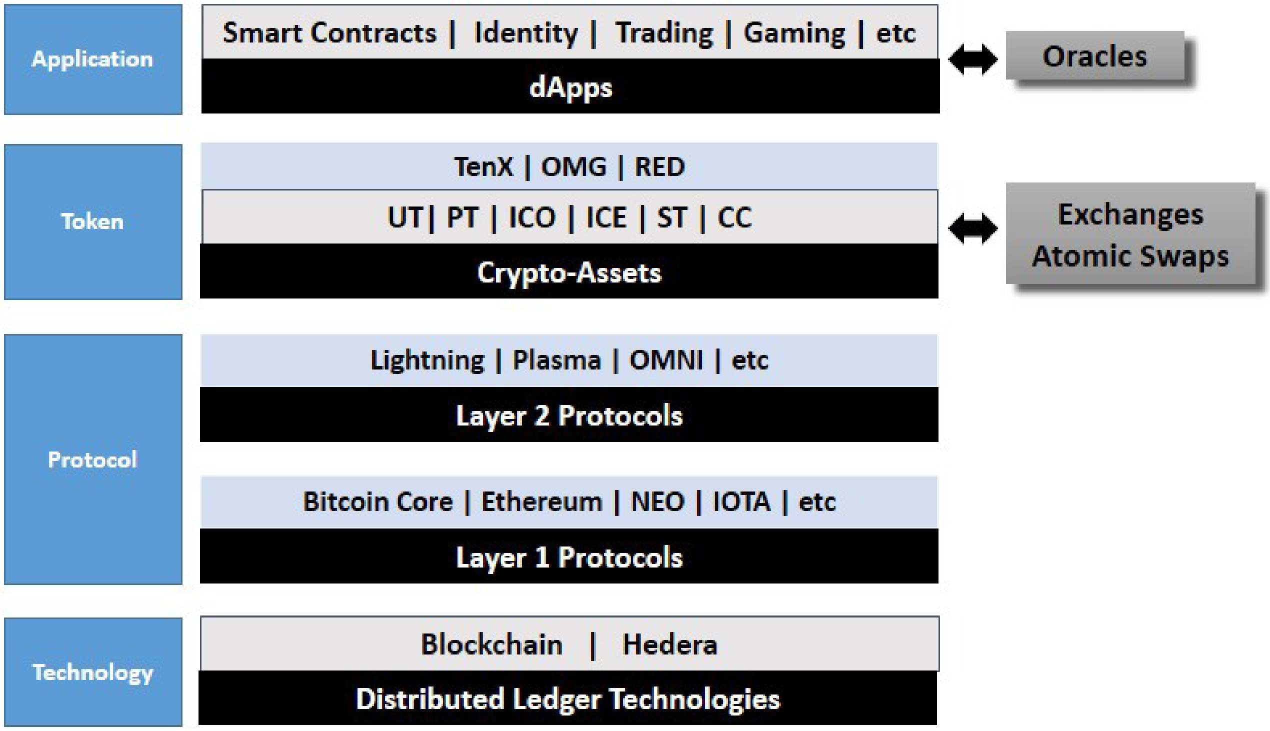

Application
Smart Contracts | Identity | Trading | Gaming | etc
dApps
Oracles
Token
TenX | OMG | RED
UT| PT | ICO | ICE | ST | CC
Crypto-Assets
Exchanges
Atomic Swaps
Protocol
Lightning | Plasma | OMNI | etc
Layer 2 Protocols
Bitcoin Core | Ethereum | NEO | IOTA | etc
Layer 1 Protocols
Technology
Blockchain | Hedera
Distributed Ledger Technologies

Exhibit 3: DLT Hierarchies and Taxonomy

Key: UT = Utility Tokens; ST = Security Tokens; CC = Crypto-currencies; ICO = Initial Coin Offerings; IEO = Initial Exchange Offering; DLT = Distributed Ledger Technologies; dApps = Distributed Applications

Layer 2 is however considered 'off-chain' and thus, while faster than the 'on-chain' Layer 1 for transaction processing, is natively less secure and reliable.

Using the Bitcoin blockchain, the Lightning Network and RootStock are being launched.[61] The Lightning technology is a so-called 'state channel'[62] This 'Layer 2' technology as it is known is dependent upon the underlying technology of the blockchain, using real Bitcoin/blockchain transactions and using its native smart-contract scripting language to create a secure network of participants which are able to transact at high volume and high speed. It adds another layer to Bitcoin's blockchain and enables users to create payment channels between any two parties on that extra layer. These channels can exist for as long as required, and because they're set up between two people, transactions will be almost instant and the fees will be extremely low or even non-existent.[63]

Scaling solutions for Ethereum include Sharding,[64] Plasma, and Casper, all known as 'Layer 2' protocols. (See **Exhibit 3**) It's been noted that attempts such as the Lightning Network or Sharding—as well as DAGs—suggest that scaling can be improved if using the design principle that not all participants—or network nodes—need to know all the information at all times to keep a DL network in sync.[65]

Ethereum's 'Constantinople' upgrade is designed to use POS.[66] There is also delegated POS (dPoS) and a host of other consensus mechanisms, some of which are described below. **Exhibit 2** shows the various consensus protocols in use in DLTs.

2.4 Typical Actors in a Distributed Ledger

Actors in DLT/blockchain ecosystems include:

- Authenticators who are miners/validators/forgers and provide operational and validation services;
- Developers who program and maintain the core DLT protocol; and
- Users who own, invest and otherwise use tokens and engage in activities on the system.[67]

Different levels of governance exist for each of these domains.[68] At the transactional level, miners and validators operate the system in exchange for incentives and govern which blocks are accepted into the blockchain according to the rules set forth in the system and its consensus mechanism. At the protocol or development level, programmers (who may be voluntary and not employees or contractors of a centralized organization) contribute and evaluate code.[69]

Type	Typical Role in Distributed Ledgers
Inventors	First publisher of new DL technology[70]
Developers	May improve on the initial DL technology
Miners/Validators	Paid to add new data to blocks
Users	Use data stored on a DL
Oracles	Provide input/output data for use in Smart Contracts
Centralized Exchanges	Exchange tokens, facilitate ICOs
Nodes	Hold copies of a DL
Auditors	May test smart contracts for coding errors and/or legal validity
DLT Network Operators	Defines, creates, manages and monitors the blockchain network. Each business in the network has a blockchain operator[71]

Exhibit 4: Typical participants in a blockchain-based Distributed Ledger.[72]

2.5 Evolving Use Cases of Distributed Ledger Technologies

In the financial industry and in business networks generally, data and information usually flow through centralized, trust-based, third-party systems such as financial institutions, clearing houses, and other mediators of existing institutional arrangements. These transfers can be inefficient, slow, costly, and vulnerable to manipulation, fraud and misuse.[73]

Samples of DLT use cases include:

- **Financial:** Clearing and settlement (C&S); Clearing houses;[74] Correspondent banking; Credit provision; Derisking;[75] Digital Fiat Currencies; Factoring; Insurance contracts; Interoperability between banking and payment platforms; Remittances; Results-Based Disbursements; Share registries; Shareholder voting;[76] Small medium enterprise (SME) finance; Trade finance and factoring; Taxes[77]
- **Financial Integrity:** Electronic know your customer (e-KYC);[78] Identity (ID) systems
- **Legal:** Notarization of data;[79] Property registration
- **Utilitarian:** Agricultural Value Chains; Food Supply Management; Medical Tracing; Project Aid Monitoring; Supply Change management; Internet of Things (IoT)
- **Intellectual Property:** Digital rights management

Bilateral and multilateral agreements are needed,[80] which are typically recorded by the parties to the agreements in different systems (ledgers).[81] A number of blockchains and DLTs have emerged in recent years that aim to address these issues. Each may have its own different use cases, offering benefits such as larger data capacities, transparency of and access to the data on the blockchain, or different consensus methods.

2.6 Active Components of DLTs

2.6.1 Overview

Described below is how the DLT ecosystem is attempting to evolve and expand beyond its genesis product—'crypto-currencies'. Key to this is the emergence of the 'token' as the launchpad and incentive for all manner of innovations in the decentralized ecosystem. Without incentives, for example, to add blocks to a chain, there would be no chains. Thus, a number of programmable token types have emerged, programmed for example to provide value, governance or utilitarian features, or a combination thereof. Where the token has an asserted value that can be used to trade with others, it becomes a type of asset. Hence the emergence of the term 'crypto-asset' to describe a growing number of these tokens types using new DLTs and protocols. So-called decentralized applications (dApps) such as 'smart contracts' sitting atop the protocol stack in the DLT hierarchy can use these crypto-assets as, for example, a means of payment for goods and services, to raise capital, and for facilitating the use of the smart contract to pay technical participants called 'miners or validators.'[82]

2.6.2 The Criticality of Tokens

While the underlying DNA of blockchain-type DLTs are blocks or the equivalent, coded within that DNA are cryptographic representations called tokens.[83] These tokens are characteristic of the newest types of DLTs such as Ethereum, and are 'programmable' to the point that they (the DNA) is able to be expressed in any manner of ways the DLT protocol allows. Tokens can thus be programmed to be the crypto-graphic representations of, for example, rights, value, assets, and processes.

With more sophisticated—that is, increasingly programmable with additional features—blockchain types emerging in 2015, additional types emerged now under the umbrella terms 'crypto-assets.' These varied in the rights they grant their owners; in their actual and potential uses as a means of payment, or for investment, consumptive, crowd-sourcing functionality, or hybrids thereof. Thereto, new terms of art entered the lexicon as Initial Coin Offerings (ICOs) in 2016-2017, Utility Tokens (UT) in 2017; and Security Token Offerings (STOs) and the Security Tokens (STs) they create from 2017; and Initial Exchange Offerings (IEOs) from 2018.

These include:

- Utility. These tokens facilitate smart contract and gives access to certain features of a platform.
- Asset. They represent a product or an asset.
- Equality. These tokens give control and ownership over something.
- Security. Represent shares of a company, similar to stocks.
- Reward. Received for contributions on the blockchain.

As a right, they can represent the ability to 'vote' on a change to a DLT protocol or give the holder the ability and right to act as a miner in POW or POS paradigms.

In many cases these tokens are tradable and consumptive and so the appellation crypto-assets has been given to reflect their value-based role in the crypto-economy other than just a plain vanilla functionality of storing data in a crypto-graphically secure and tamper-evident manner. That is, while ecosystems—such as for asset tracking—may use DLTs for single utilitarian use, at a more expansive level, the programmability of the tokens expands tokens at both the protocol and application layer themselves such that they may, in and of themselves, contain value.[84] In that sense, they may amount to 'programmable money' and be the tradable, asset component of what often termed Decentralized Finance (DeFi).

Both the interlinked terms—crypto-assets and DeFi are relatively new and their meaning fluid and temporal given the evolving nature of potential constituent components. At a high level, they can be said to be digital representations of value generated, derived, issued and distributed through DLTs.

They may form the basis of institutional exchange tradable funds such as derivatives and futures. For the most part, unlike the value of fiat currencies which is anchored by monetary policy and their status as legal tender, the value of some crypto-assets rests solely on the expectation that others will also value and use them. Since valuation is largely based on beliefs that are not well anchored, price volatility has been high.[85]

However, many of these are 'retail' assets, in so far as individuals—or individuals operating in pools or consortia—are the primary buyers and traders in these crypto-assets. Institutional investors—weary of the volatility and often legally unclear nature of these assets—are only recently but still haltingly beginning to embrace the crypto-assets as tradable assets or investments opportunities. Stepping back from their temporal functionality, aspirationally, they may be seen as digital bearer instruments that are designed to settle peer-to-peer, on a gross basis, in near-real-time and in with the token containing the actual crypto-asset such that when crypto-assets trade, the buyer and seller simultaneously exchange value for value in gross settlement.[86] Besides usurping the role of many 'legacy' intermediaries—such regulated centralized exchanges, brokers, asset custodians, for example—in trading, the effective vesting of real (ownership) rights to a token 'containing' a tradable crypto-asset has implications in the wider economy, providing an element of super-negotiability the crypto-asset that allows that asset to be used for unencumbered collateral in the credit and capital markets.[87] This, theoretically at least, opens up now pools of liquidity and capital divorced from traditional actors such as investment banks.

These crypto-assets have engendered regulatory reaction around the world, with a number of regulators issuing specific crypto-asset regulatory frameworks or rules that capture or reflect on some of all of these components. That said, there is not yet any standardized terms, so that any crypto-asset taxonomy[88] in any one jurisdiction may depend on the jurisdictional framework relating to legacy products as well as recency bias—that is, use in regulations or rules of terms with the most headlines at any one time.[89]

Ultimately, for these tokens to have ubiquity, they must be transferable between counter-parties, either directly or through some type of exchange. Depending on the level of development, liquidity, decentralization or sophistication of the technologies or platforms underpinning the token's provenance, other parties may be involved in this transfer. Regulatory considerations motivated by safe and soundness may even mandate the need for these intermediaries to be involved in transfer of tokens, mirroring to some extent 'legacy' systems.

For example, with the increasingly programmable nature of some DLTs, the term 'token' has largely replaced the 'genesis' term as used in the original Bitcoin—that is the use of the simple term 'coin.' The latter is more broadly known as a crypto-currency. But the term coin in its most narrow utilitarian function of being the means to offer incentives to miners/validators and other technical facilitators in a DLT to generate a token, has stuck. That is, the interplay between a crypto-currency—a 'coin'—and an associated token is demonstrated through the production of the token, which invariably requires a crypto-currency. That is, 'coins' are the native digital assets of their blockchain, in the way that Bit(coin) is the rationale for the DLT it encompasses.[90]

Some taxonomies[91] then draw a distinction between 'native' and 'non-native' tokens. Native tokens are intangible, non-physical assets that derive their value from the DLT platform. Bitcoin is native to the Bitcoin blockchain. Non-native tokens are those which represent tangible and/or financial assets that exist elsewhere.

To that extent, in their native genesis state, coins can exist independently, but tokens can't.[92] So there's a chicken and egg: to build tokens, you need 'coins.' That is, if you want to use a token on the Ethereum DLT, you will have to spend some Ethers, the native digital 'coin' asset of the Ethereum blockchain, to validate the creation.[93] And to trade—or just simply send—the token to someone else, you have to pay what are known in the Ethereum world as 'gas' fees,[94] essentially transaction fees[95] to the miners.[96] Genesis-level 'coins' require significant processing power to mine, while tokens are relatively easy to create on say the Ethereum DLT by following the provided template on the platform.[97]

2.6.3 Crypto-Currencies

Crypto-currencies in our thinking are digital representations of value generated through cryptographic techniques by non-state entities or persons, and which may or may not be used as a means of payment or value transfer; which may or may not be issued; and which may or may not confer claims against an issuer. They are a class containing the following types: protocol tokens; payment tokens and stablecoins.

Protocol Tokens

Most blockchains use digital tokens to compensate parties for participation in some activity that contributes to the maintenance of the DLT and its network. These have been referred to as 'protocol tokens' (PrT) because they anchor complex incentive mechanisms in the protocol governing the network's maintenance.[98] A more expansive view is that these protocol tokens serve as the genesis of the blockchain—for example Bitcoin—as well as having multi-function roles.[99] Ethereum's design incorporates what is known as an Ethereum Virtual machine (EVM), a processing engine that is said to be 'Turing Complete.'[100] To prevent EVM overuse (and abuse) as well as to provide additional functionality of the PrT is to execute—where available—more sophisticated applications, users must pay its 'gas'[101] fee.[102]

Payment Tokens

Payment Tokens (PT)—as we classify them here, but popularly conflated as being a crypto-currency in of itself—can be seen as having money-like properties of having a unit of account (for example a 'Bitcoin'); act as a means of exchange; and act to store value for the holder. The latter two qualities are eminently contestable: legal precedent would confer the means of exchange attribute as to being widely accepted for use in commerce or settlement of a debt (a claim) whereas it is trite that nascent crypto-currencies are of almost novelty use and not widely accepted. Indeed, given their speculative nature they can be seen as asset classes and in some jurisdictions, are indeed seen as such. Similarly, the volatile trading values of crypto-currencies do not make them a practical measure of store of value as measured in purchasing power. Potentially, as described below, so-called stablecoins—stability meaning less or no-volatility and more consistent in terms of purchasing and trading power—may be the nirvana to more widespread use of crypto-currencies as a class.

Stablecoins

Stablecoins are a new innovation designed to act as an antidote to the volatility characteristic of the range of crypto-currencies being traded today. Simply, they describe any crypto-currency designed not to have price volatility relative to a fiat currency. The majority of the crypto-currencies available today—even the largest such as Bitcoin and Ether[103]—exhibit significant price volatility. Most crypto-currencies as they are currently formulated cannot, natively, guarantee that absolute value. Hence, the introduction of stablecoins. In some cases, stablecoins could be classified as STs, and thus attract a different, and stricter regulatory regime.

It is trite that a crypto-currency with price stability—one that can be used in a variety of decentralized applications as a unit of account -is sorely needed to enable the growth and maturity of the crypto-economy and to bring it from a fringe novelty to mainstream acceptance.[104] Smart contracts in particular could benefit from stablecoins to ensure stability of payment as to provide a modicum of 'store of value.'[105] Four major classes of stablecoins[106] have emerged: fiat-backed; commodity-backed; crypto-currency-backed and seigniorage-style, all shown in Annex A.

2.6.4 Initial Coin Offerings

Initial Coin Offerings[107] (ICOs) are the basis for project financing by the issuance of tokens against payment predominantly in the form of crypto-currencies. ICOs are often directed at a broader public, requiring each investor to accept identical, non-negotiable terms. The project may not yet have an identifiable or available product that is 'functional.'[108] Their tokens are issued and traded on exchanges, which charge millions of dollars for the right to 'list' a token on their exchange. While many innovative fintech startups raised hundreds of millions of dollars via ICOs during the 'boom' years of ICOs in 2017 and early 2018, the entire ICO ecosystem was sullied by scammers. This damaged trust in ICOs, and with many skirting obvious regulations, led to new regulatory frameworks being developed in some countries,[109] and enforcement actions in many others.[110]

2.6.5 Utility Tokens

Utility Tokens (UT) are also known as app coins or user tokens and provide users with future access to a product or service[111] but do not offer the holder any rights of ownership. Similarly, unlike equity securities of a company, they do not grant any control rights, or claims to dividends. Thus, investors buy tokens for their utility value or for speculative reasons such as a higher resale price.[112] Unless they are caught under the definition of a security, spot trading and transactions in UTs do not generally constitute regulated activities. To avoid the appearance of being associated with

ICOs (and thus by proximity, to regulated IPOs), UT creators will term their offerings of tokens to as 'token generation events' (TGEs) or token distribution events (TDEs).[113] In some jurisdictions, UTs may be classed as securities, but may qualify in some cases for an exemption to any registration requirements.[114]

2.6.6 Security Tokens

Security Tokens (ST) are tokens offered to investors which are ostensibly backed by identifiable or available product or some physical assets that underpins the token's value.[115] In essence they are seen bridging and transforming real-world assets into crypto-assets domain by bringing them 'on-chain through tokenization.[116] Thus if a crypto token derives its value from an external, tradable asset, it is classified as a ST and, at least in the US, may be subject to securities regulations.[117] Examples of STs include currencies and commodities (for value storage and transfer); debt instruments (for automated lending); and securitized debt instruments (for trading); physical property as real assets (for raising capital).[118] Payment for STs may be predominantly, but not exclusively via crypto-currencies.

The introduction of a legal construct for the token law may require that the legal consequences, such as ownership, possession and transfer, must also be defined by law.[119] In most cases, the STO will be provided and/ or traded in operating primary/secondary markets through licensed market intermediaries and market operators dealing or managing investments in STs. Shares can be directly represented as a token through a physical certificate, creating an interface between securities law and any crypto asset laws.

2.7 Central Bank Digital Currencies

Central Bank Digital Currencies (CBDC)—also known as digital fiat currencies (DFC)—is a digital representation of value generated through cryptographic techniques and issued by state entities—usually a central bank—which may be used as a means of payment or value transfer and which may confer claims against the issuer. This can be distinguished from reserves or settlement balances held by commercial banks at central banks. With value issued in fiat at source but tokenized, CBDCs may be considered the ultimate stablecoin.

2.8 Crypto-Wallets

Many tokens or crypto-currencies are stored in a wallet, a medium to store the seeds/passphrases/keys associated with crypto-asset accounts. These secrets are required to generate the private keys used to sign transactions and spend money.[120] The public keys and address can be made public but may compromise anonymity and linkability.[121] There can be hot or cold wallets, with the former like saving accounts which must be connected to the internet. There is however a higher risk of theft than cold wallets which are like saving accounts and can be kept offline. There are also online wallets, which are kept by a third-party exchange.[122] Hot wallets are manifestly imperfect, though, as exchanges are vulnerable and have been hacked often. If the exchange is down, no tokens can be accessed.[123] There's also 'deep cold storage,' referring to keeping a reserve of a crypto-asset offline, using a method that makes retrieving coins from storage significantly more difficult than placing or sending them there.[124]

2.9 Decentralized Apps (dApps)

The business end of DLTs revolves the application layer. Bitcoin was the first application in the decentralized economy, and they have grown to any number of types, ranging from trading exchanges to prediction markets. The universe of applications running on a DLT are known as 'decentralized apps' or 'dApps.' Examples of dApps include those for Gaming; Prediction Markets; Experimental Universal Income; Exchanges, and Smart Contracts.

2.10 Smart Contracts

Most dApps in use are based on Ethereum,[125] specifically using the Ethereum ERC-20 'programmable' token to create what are known as 'smart contracts.' They have built-in intelligence, setting (business logic) rules about a transaction as part of what is called a 'smart contract.[126] These are of 'if-this-then-that'-type instructions recorded in blockchain code and which can be automatically executed. The instructions embedded within blocks—such as 'if' this 'then' do that 'else' do this—allow transactions or other actions to be carried out only if certain conditions are met. They are tied to the blockchain-driven transaction itself and must be executed independently by (user) every node on a chain.

For example, in the Ethereum blockchain, its EtherScript programming language allows the use of natural language 'notes' in an EtherScript that helps improve human readability in smart contracts. These notes are analogous but, importantly not identical to, to the wording in a separate (physical) legal contract.[127] In all then, a legal contract is ostensibly being replaced by computer code, and for the maximalists, the need for lawyers to be involved in the chain of execution of the smart contract is (mistakenly, we submit)[128] thought to be redundant.[129]

In a practical use case example, where a contract between parties to purchase a property asset is written into a blockchain and a preset triggering event such as a lowering of interest rates to a certain level is reached, the contract will execute itself according to the coded terms and without any human intervention. The trigger could be through a so-called oracle providing rate data input.[130] This could, in turn, trigger payment between parties and the purchase and registration of a property in the new owner's name. In some cases such as atomic swaps of tokens of different type,[131] the smart contract may also make the need for separate escrow redundant as the token locked into a SC-mediated vault could be the escrow itself.

3 The Crypto-Economy: Tokenized Crypto-Assets and Use in Decentralized Finance

3.1 Overview[132]

While a broad range of use cases are being developed for DLTs as a utilitarian function of a secure, traceable database, the most valuable use cases for tokens are forms whereby tokens are programmed according to their protocol, to be used within a suit of emerging token classes such as payment tokens, utility tokens, security tokens, and ICOs. These programmed tokens can be used as crypto-assets in a decentralized manner in financial transactions. Instruments for derivatives, securitization of assets, lending, escrow, and insurance can now be expressed as tokens.[133]

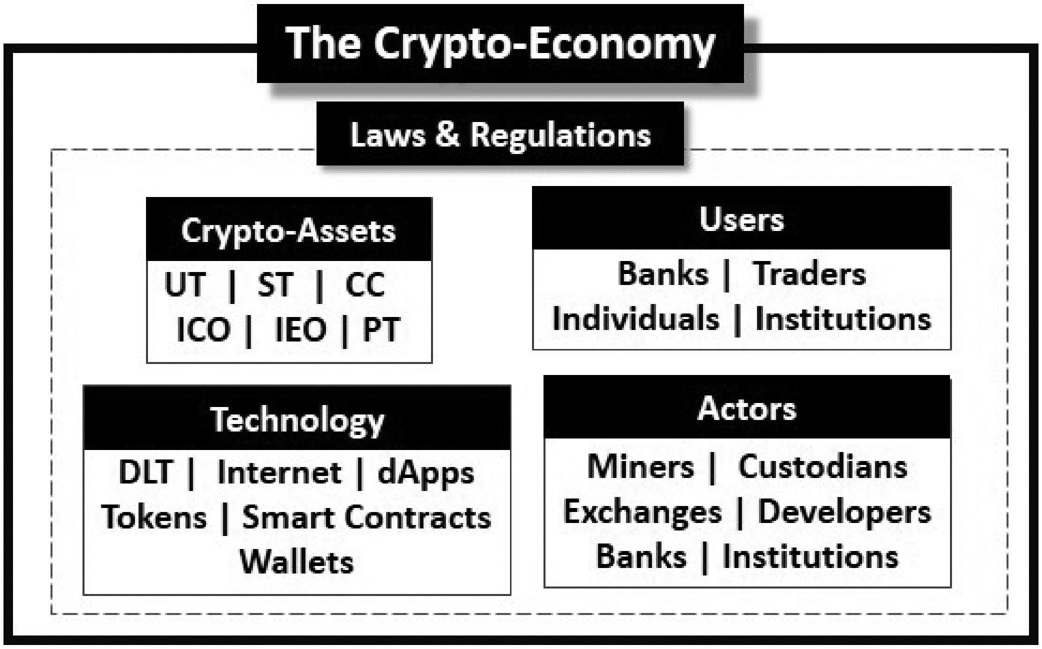


Exhibit 5: The stylized 'crypto-economy,' using crypto-assets and 'wrapped' in applicable laws and regulations. Actors here are those involved in any process which generates, values, issues, stores, or trades a crypto-asset.

Key: UT = Utility Tokens; ST = Security Tokens; CC = Crypto-currencies; ICO = Initial Coin Offering; IEO = Initial Exchange Offering; DLT = Distributed Ledger Technologies; dApps = Distributed Applications

Hence the emergence of the term DeFi to describe this 'transformed' financial ecosystem. DeFi simply describes the potential of new asset verticals made possible by tokenization and decentralization. The crypto-asset components of the crypto-economy—outlined in **Exhibit 5**—are essentially digital bearer instruments (tokens) capable of being settled peer-to-peer on a gross basis. The sections that follow outline the role and type of each of the constitution crypto-asset classes is described below, as are the methodologies for in trading them alongside, any identifiable risks.

3.2 Legacy and DeFi

To track the evolution of these crypto-assets, and to highlight their potential transformative effects, its worth describing differences between legacy and crypto assets and systems. The distinction may be fuzzy however, given the nascent evolution towards DLT-based systems and products. The critical distinction though would be the way the assets are issued and settled.[134]

Feature	Legacy Assets	Crypto-Assets in DeFi
Account Type	Omnibus (assets polled in fungible bulk)	Individual
Asset Type	Debt-based	Equity-based
Composition	Natively 'analog'	Natively digital
Custody	Mostly intermediaries	Mostly self-custody
Issuance	Multi-actor process for issuance of securities	Self- or Exchange issuance
Ownership	Indirect (registered owner ≠ true owner)	Direct (registered owner ≠ true owner)
Reconciliation	Multiple Asynchronous Ledgers (need reconciliation)	Single "Golden Copy" Ledger (no reconciliation needed)
Settlement	• Via Intermediaries • Netted • Delayed, thereby creating counterparty risk	• Peer-to-Peer • Gross • Value exchanged simultaneously

Exhibit 6: Salient differences Between Legacy Assets and Crypto Assets in the 'Decentralized Finance' Paradigm.[135]

3.2.1 Legacy

A legacy institution such as a bank may not have any use or exposure to DLT, or it may have hybrid legacy and DLT products and services. For example, it may use a DLT-based platform to process legacy assets in its back-office reconciliation system. Or it may also have its own DLT-based payment token 'crypto-currency,' for example the JP Morgan Coin discussed below.[136] Or, as Long describes it, it may 'wrap' DLT around an existing (legacy) product—that is, '*crypto wrapped around legacy*'—such as a security or some other asset, effectively just using DLT for reconciliation and security purposes.[137] The latter may be a stablecoin or security token. There may also be a hybrid '*legacy wrapped around crypto*,' asset, for example Bitcoin-linked ETFs or futures which are issued, traded and settled in the legacy system.[138] The crypto asset (here, Bitcoin) collateralizes the traditional financial instrument, with the underlying crypto-asset operating on a DLT.

3.2.2 Decentralized Finance

Decentralized Finance (DeFi) is a term that emerged during the course of 2017 used to describe financial systems and product applications designed where, ideally, crypto-entrepreneurs can recreate traditional financial instruments in a decentralized architecture, outside of companies' and governments' control and without intermediaries.[139] The notion is that, for example, legacy market makers, capital markets, broker dealers, exchanges, asset custodians, and even fiat currency would be replaced by an entirely new set of actors, or

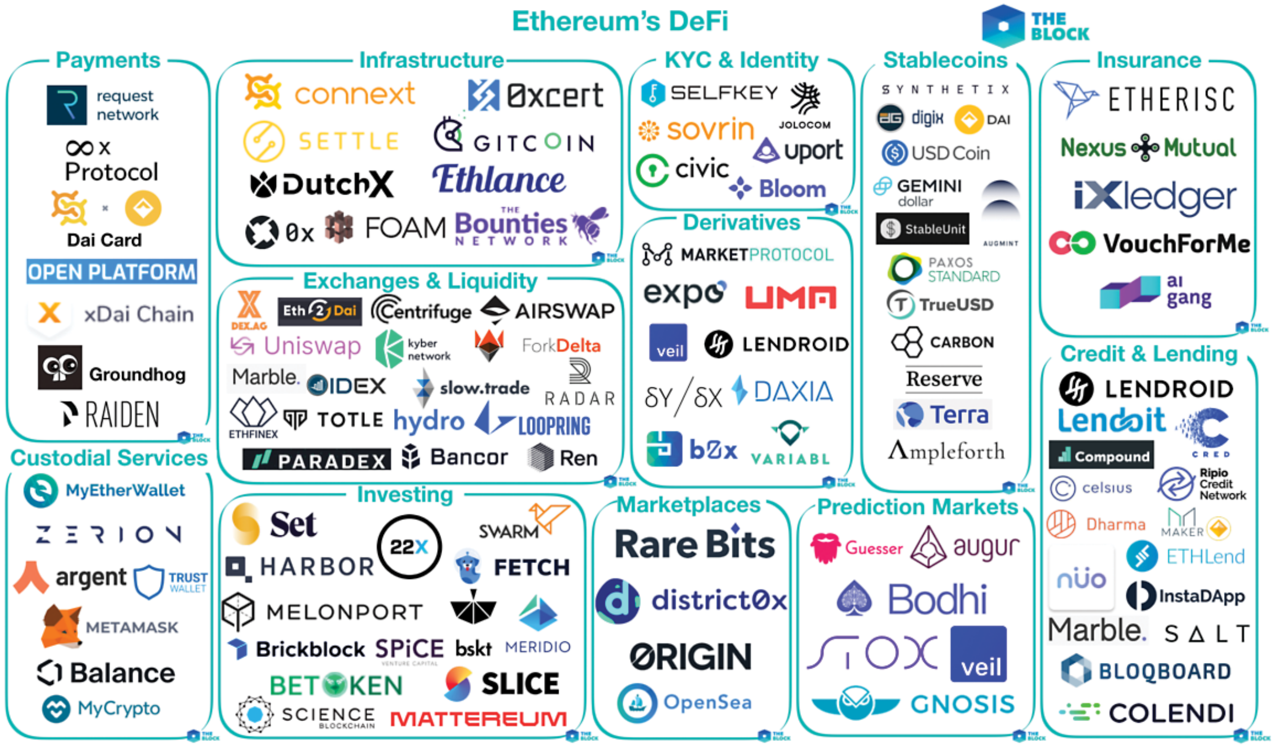


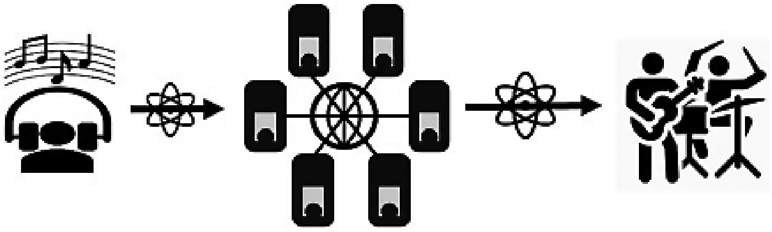
Exhibit 7: Published components of DeFi based on the Ethereum DLT.[140] The core technologies that make up the globally accessible DeFi platforms are stablecoins,[141] decentralized crypto exchanges,[142] or DEXs (and/or exchanges that do not hold—have custody of—users' private keys), multi-currency wallets, and various payment gateways that include lending and insurance platforms, key infrastructural development, marketplaces, and investment engines.

at the very least, legacy components and actors would need to adapt to blockchain through internal disruption, to transform themselves into a decentralized version of their centralized business models and processes.

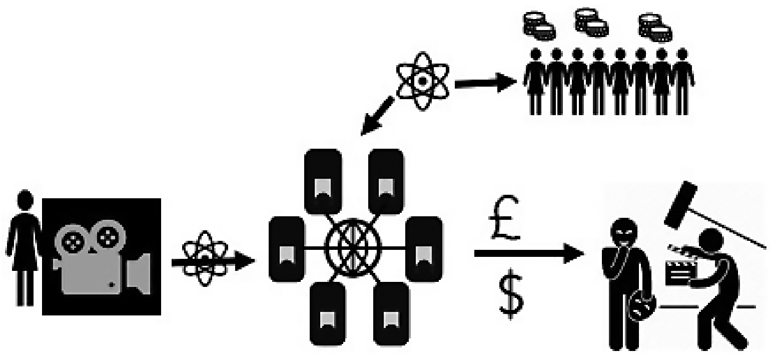
A crypto-asset used in a DeFi environment may have vastly different characteristics or the entity itself may be decentralized. A Distributed Autonomous Organization (DAO) discussed below, for example, would be 'natively' all-DLT with governance, organization and activities all decentralized. The grand ideas in DeFi versus legacy include that intermediaries are made redundant or the need reduced; transparency and security of asset transfer and financial transactions are improved; that users get direct custody and thus ownership rights and direct negotiability to their assets without the need for custody by intermediaries; that smart contracts automate many of these processes in a trustless manner; and that asset transfers can be done on a gross—versus net—basis; and directly between counterparties at low or no cost; with all transactions on a tamper-evident DLT, where there is privacy by design; and where the transaction provenance is indisputable.

Of course, while there are a number of emerging use cases, a larger economy-wide rollout—that is, as a 'crypto-economy'—is for the near future, largely aspirational. To be sure, appetites for such fundamental transformation of systems and processes are still to be contemplated; the technologies built out to scale, speed, security, ubiquity, and reliability. Similarly, capacity and skill sets need to be developed, alongside any new rules, or adaptations of old rules, that could potentially govern these new methodologies and asset classes.

Starting modestly, some asset classes can be fractionalized in this DeFi paradigm to essentially democratize the ability of anyone with the technology and technological and financial wherewithal to get access to hereto unavailable asset classes, be that fractional own-



In the dApp media use case diagram top, the end user sends a request to stream a song which travels through the public network, along with a micropayment (fraction of a cent) of crypto-currency. The nodes on the network come to consensus that both the song request and micropayment are valid. The network sends a receipt of the request to the media application's gateway and passes the micropayment on to the artist directly. The application streams the requested song for the end user and the musician is paid immediately without the need for *financial* intermediaries such as music rights organizations and/or agents to be involved.[143]



Often royalty payments are paid every 6 months. Actors can factor expected future royalty earnings from movies they appeared in by tokenizing on a DLT the total expected future royalty value and then selling fractional components to potentially thousands of small investors at a discount through a smart contract. The investors can then trade that token. This token may approximate to a security token in some jurisdictions, but this usually depends on how it is marketed.

Exhibit 8: Use of smart contract dApps using tokenized financial assets, here music (top) and movie (bottom) royalties.

ership in music royalties due (**see Exhibit 8**) or buying shares. Abra, for example, is offering (non-US users) the ability to invest in stocks, ETFs, and commodities in over 150 countries using Bitcoin to make fractional investments in stocks and ETFs with zero trading fees.

As we see it, there are four components evolving: the underlying infrastructure layer (such as decentralized platforms for trading, payments processing and value transfers); a service component (such as custodians of private keys); the crypto-asset components (such as STs and UTs); and the application layer. In some cases, the service component may be provided the same providers of the infrastructure component. Exhibit 7 shows the ecosystem from a macro level.

Indeed, DeFi appears to be evolving into one of the more active[144] complements of blockchain developments. While Bitcoin and Ethereum are the original DeFi applications—both are controlled by large networks of computers, not central authorities—there is considerable evidence of this change, albeit slowly and with an eye to compliance with existing regulations. Legacy behemoths such as JP Morgan and Goldman Sachs are notable proponents of DeFi, with a number of banks and financial institutions in financial verticals consortia testing decentralized systems to improve, *inter alia*, processing times for payments, trade finance, and interbank transfers. For these legacy financial institutions, embracing DeFi is as much as testing the new technologies for streamlining and enhancing their current processes as it is about being part of a potentially transformative movement that recognizes their leadership role and includes them.

3.3 Decentralized Autonomous Organizations

Decentralized Autonomous Organizations (DAOs) were designed to be informal virtual assembles of parties whose interactions are created, mediated and extinguished purely by and entirely within the algorithm of its code.[145] Although long postulated, DAOs were brought to life through the mainstream use of DLTs and the emergence of companion smart contracts. Bitcoin's network is widely considered to be the first truly autonomous corporation, meeting one of the key requirements to be a DAO.[146]

DAOs are at a very early stage of development and operation, and are experimental in nature, providing a high risk investment which some believe is worth the reward.[147] DAOs work without any requirement for a centralized party to make decisions[148] and a DAO can control crypto-assets which can represent almost anything, including real-world assets, fiat money, valuable objects like cars, houses or precious metals—even solar power plants in developing countries. Those assets are usually placed under control of multi-signature wallets[149] which DAO members have control over.[150]

The most well-known attempt at a DAO was the world's first decentralized hedge fund launched in 2015 known as 'The DAO.'[151] It failed quickly though after its code was hacked.[152] The initial plan was for The DAO participants to receive The DAO's tokens after payment, then vote for which projects to fund.[153] The 'Solar DAO' creates a Community to fund solar plants across the globe. Decentralized platform for energy storage. It also allows for people to become 'prosumers' by selling their own electricity to others within the Solar DAO network. Profits are distributed among token holders.[154] There is a governing 'council' where members have three-year maximum terms so as to limit the impact of centralized power and authority.[155] In most DAO cases, interactions between the DAO members are guided by SCs, for example funding something once a certain number of votes are cast or when a threshold rate or date is met. The need for consensus is another crucial aspect of DAOs, requiring that the majority of stakeholders agree on a decision before moving or withdrawing funds. Even bugs cannot be taken care of until the majority of stakeholders agree to do so.[156] Anyone with internet access could hold DAO tokens or buy them and The DAO creators could set whatever rules they voted on.[157]

But transformatively and radically, there is no recognizable or actual legal structure behind many DAOs. Its structure could be seen as analogous to a partnership—whose members, theoretically, could stay anonymous[158]—and where the partners jointly represent DAOs and are liable for its actions and obligations. Depending on the type of DAO, it may or may not have assets from which to indemnify third parties. Where there is a liability caused by the actions of the DAO, a court—which somehow finds jurisdiction over a DAO—could see the DOA entity as fiction and hold individual members liable, or even the person or entity who created the code or SC to run the DOA.

3.4 International Interbank Transfers

Payment reach through pre-funded account liquidity is a critical prerequisite for cross-border payments. Liquidity in this context is the ability to easily convert between the originating and destination currencies.

Historically, financial institutions accessed liquidity through pre-funding accounts in the destination country. There are several costs to pre-funding: the opportunity cost of having scarce capital sit idle in accounts, compliance costs, and account maintenance costs. This is manageable for high-volume currency pairs, like the USD and the Euro, as the financial institution has enough volume to offset these costs. However, this model is not viable for low-volume currency pairs. Sourcing liquidity for payments between less frequently traded currencies can be expensive and cumbersome, requiring several intermediaries and complex processes. These pain points result in long settlement times and high fees for consumers.

Using approved crypto-assets can resolve these limitations with a new model for liquidity that connects currencies, especially illiquid pairs, more efficiently. Removing the requirement to pre-fund accounts overseas eliminates one of the largest cost factors in cross-border payments while expanding reach to new regions. Financial institutions can bring that capital back home and use it to directly support lending and investing in local communities.

Crypto-assets can act as a bridge between fiat currencies that allows financial institutions to access liquidity on demand, without having to pre-fund accounts in the destination country. Ripple's XRP asset using its XRapid system has been in place for interbank transfers and are finalized over the local payment systems, which added just over two minutes to payments, speeding up from settlement times of 2-3 days on legacy systems. Portions of the payment that rely on XRP last 2-3 seconds, minimizing exposure to price volatility.

While Ripple improves currency pairings for remittances and interbank transfers, JP Morgan has developed its 'Interbank Information Network' (IIN)[159] based on its development of Quorum,[160] a permissioned-variant of the Ethereum blockchain. Historically, correspondent banks have communicated one-way, bank-to-bank primarily through SWIFT. The IIN using Quorum[161] is said to remove the need for these individual settlement processes amongst multiple banks, using a common standard that has instant traceability over Quorum to reduce the time correspondent banks currently spend responding to compliance and other data-related inquiries that delay payments. The bank has attracted over 220 correspondent banks to the platform.

3.5 Trade Finance

A particular pain point in international trade finance is complicated reconciliation processes that results in days required to settle even simple transactions. Consortia have been formed to use blockchain to simplify letter of credit transactions to deliver speedy settlement times and resolution of discrepancies, as well as improve sanctions screening where needed.

For example, R3 is an enterprise blockchain technology company that leads an ecosystem of more than 300 firms working together to build distributed applications on top of its primary blockchain product called Corda for usage across industries such as financial services, insurance, healthcare, trade finance, and digital crypto assets. Around 50 other banks and companies have participated in tests of a Corda-derived decentralized trade finance application called Voltron to make simulated letter of credit transactions. While the existing process is paper-based and has removing time-consuming reconciliation processes, R3 claims Voltron[162] processes transactions in 'under 24 hours' compared to the 5-10 days it traditionally takes using one source of shared data.

3.6 Factoring

Factoring using DLTs represents a novel way to extract future earnings for current use. As described in **Exhibit 8**, a person who is owed future earning based on royalties, for example, for a song or acting in a movie can factor expected future earnings by tokenizing the total expected value on a DLT and then selling fractional components to potentially thousands of small investors at a discount through a smart contract. The investors can then trade that token. This token may approximate the nature of a security token.

3.7 Capital Markets

We have described above the most popular capital raising mechanism using DLTs: Initial Coin Offerings (ICOs, and their ICE derivatives) as the basis for project financing by the issuance of tokens against payment predominantly in the form of crypto-currencies. There are also Security Tokens that are offered to investors and which are ostensibly backed by identifiable or available product or some physical assets that underpin the token's value. **Exhibit 9** shows the largest ICO raises.

ICO	Raised Amount	Market Share
Ethereum	21,194	88%
Waves	156	2%
Stellar	296	1%
Separate blockchain	88	1%
NEO	210	1%
Scrypt	26	1%
Bitcoin	309	1%
NEM	69	0%
EOS	18	0%
Bitshares	22	0%
Other	2,625	5%
TOTAL	USD 25,013 million	

Exhibit 9: The largest ICO raises, in USD Millions. These are ICOs that ended as of May 31 2019.[163]

But despite the screaming headlines and enforcement actions, ICOs have had limited success: notably only between 25%-33% of crypto-assets issued through ICOs during the course of 2017-2018 are currently being traded. This may also be because issuers may impose a lockup period before the crypto-asset may be traded.[164] And of 5489 published ICOs, 3400 did not raise funds.[165]

3.8 Prediction Markets

Prediction markets allow users to buy and sell shares in the outcome of specific events. After the event occurs, users holding shares of accurate event outcomes are rewarded while users holding the inaccurate ones invariably lose their money.[166] In a legacy system, betting on the value of goods in the future is similar if not identical to a type of (legacy) derivative known as a binary option.[167] These are relatively new instruments in financial markets and often packaged with derivative type products.[168] In the US, they are regulated by the CTFC.

Decentralized versions of these prediction markets appeared in late 2017 with Augur.[169] Oracles provide data input for market assessment of the predicted event. Prediction events include betting on sports or elections; predicting the movement of stocks, commodities and bonds or other type of asset without owning the underlying asset. The potential for creating illegal or unethical prediction markets has however been shown.[170]

Exhibit 10 shows the differences between new and legacy versions in prediction markets. In essence, the decentralized versions use crypto-currencies and smart contracts as the payment and 'processing engines,' and compared to legacy services that restrict access and manage market creation, they allow anyone to register, create a market and participate in the process, so significantly broadening the (indirect) availability of 'exotic' financial instruments to anyone.[171] This means, for example, that a nurse in Uganda can use her basic mobile phone to fractionally 'bet' USD 5 on the movement of Tesla or Amazon stock without having to own the stock. Another significant difference is that there is also no custody of funds by intermediaries: users control their own private keys, versus the need to deposit funds with legacy systems. Augur has hit some headwinds though, with reports of 'wash' manipulation that skewed the bets on the price of ETH. There is also significant regulatory uncertainty on the entire model and the US Commodity Futures Trading Commission (CFTC) has noted[172] the resemblance of the Augur contracts to binary options, which fall under its jurisdiction.[173] It has already sanctioned a similar entity.[174]

Centralized Market:	Decentralized Market
Money escrowed	Hold your own money
Shares escrowed	Hold your own shares
Popular markets	Choose any market
Match orders	Open order matching
Exchange lock-in	Use any exchange
Adjudicate outcome	Trust agility
Easily disrupted	Fault tolerant
Potentially transparent	Transparent by design
High fees	Low fees
Semi-prone to manipulation	Prone to manipulation
Verified data stream	Use of unverified oracles
Legal/Ethical Predictions	Illegal/Unethical Predictions Possible

Exhibit 10: Comparison between Centralized and decentralized prediction markets.[175]

4 Trading in the Crypto-Economy

4.1 Overview

Trading of crypto-assets is the lifeblood of the nascent crypto-economy. For example, an ICO token after issuance by a person or entity becomes non-redeemable but can be traded on secondary markets. Or the token can be issued directly by an exchange itself—as an Initial Exchange Offering (ICE)—for primary trading. Platforms for trading crypto-assets will, aspirationally, attempt to bring a measure of transparency to trading, and try to match the reliability and speed trades of non-crypto-assets. It has, however, been a tough hill to climb, with infrastructure, technology and regulatory impediments. In short, based on technical, regulatory or risk reasons, many of the actors who undertake or facilitate trading of non-crypto-assets were have not been available (or allowed) to do so for crypto-assets.[176]

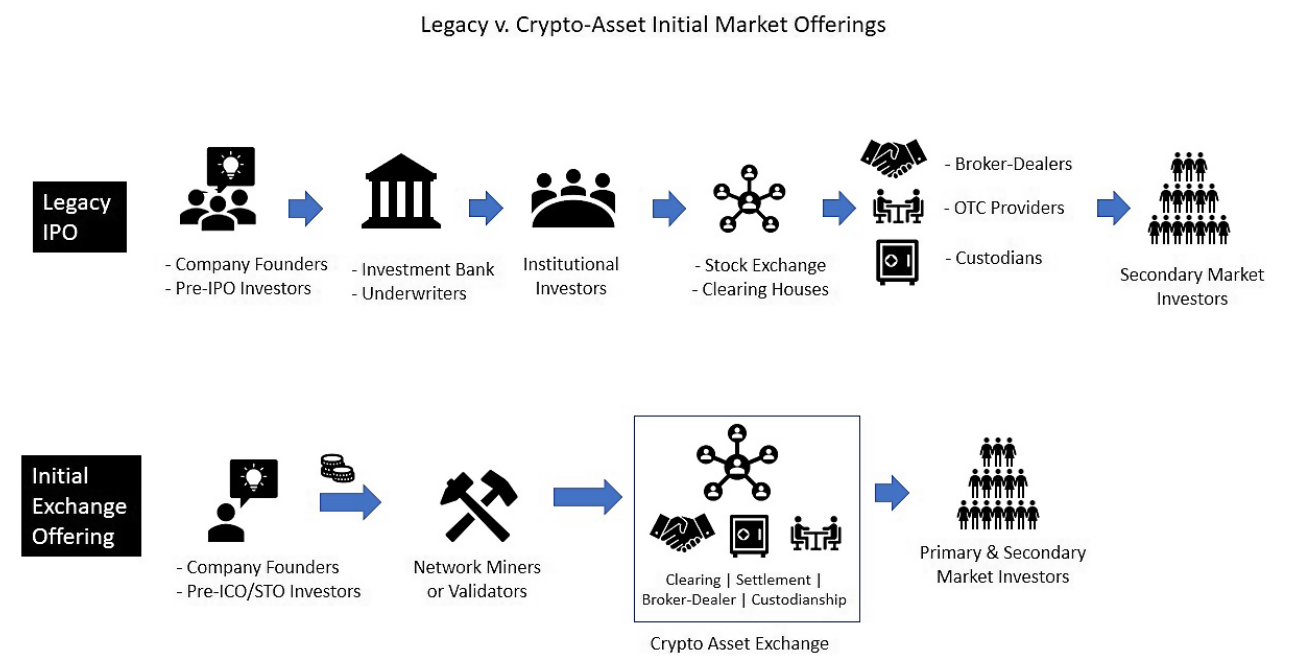


Exhibit 11: Stylized comparison between legacy IPOs for raising capital (top), and use of Initial Exchange Offerings (IEO) for raising capital using DLTs.

Thus, the nascent industry had to 'create' is own trading platforms in the absence of being able to use other existing platforms trading non-crypto-assets or atomic swaps where no platforms *per se* were required to trade. Similarly, the notion of broker-dealers who match buyers and sellers, hold funds or value (say in the form of equities) as custodians on behalf of their clients or who seek out liquidity to trade, was not easily replicated for use in the crypto world.

A number of trading platforms, exchanges or facilities emerged, some of which can be achieved peer-to-peer (counterparty to counterparty) in a fully decentralized manner called 'atomic swaps.' These effectively dispose with the need for any intermediary such as an exchange, or legacy intermediaries such as clearing houses, custodians and broker-dealers. Ironically but emblematic of the nascent nature of the crypto-economy, trading in 'decentralized' crypto-assets is largely off-chain and done in a centralized entity, but with some on-chain elements.

4.2 Centralized Exchanges

Crypto-exchanges were developed to not only trade crypto-assets but also to hold value (the equivalent of a custodian in the non-crypto-world; clear and net positions (the equivalent of exchanges in the non-crypto-world) and settle the trades. Various models have been employed with varying degrees of success.

While crypto-assets as components of a DeFi ecosystem are themselves largely decentralized, the method of buying and selling crypto-currencies is still largely centralized, requiring at least one third party intermediary such as an exchange. They will act as custodians of the crypto-asset seller's value in what is called a 'hot wallet' by holding[177] the private keys of the asset to, ostensibly, improve liquidity by being able to trade quickly instead of being impacted by delays from the 'owner' providing the keys. A typical centralized exchange, acting as an intermediary between buyers and sellers, acts as a central clearing house, as a prime broker if providing tools for leverage and margin trading.[178] Some exchanges may facilitate fiat-crypto swaps only and others crypto-crypto only. Trading is fragmented, however, with not all exchanges listing all coins. In one model, a hybrid model is employed where (for OTC providers) trading and net settlement is done off-chain and then net out positions at the end of trading session—when the net position is done. The rationale of each of these variations is to keep everything 'on-chain' since the mantra to the decentralized crypto-economy is that it moves at the speed of crypto-currencies, not fiat.

In all, there are around 250[179] of these platforms operating globally, although a handful concentrate most of the flows with the largest located in Asia or in the United States.[180] Coinbase and Binance dominate this area. The latter only does crypto-to-crypto pairings to avoid full KYC requirements when dealing with fiat and similarly it allows customers to deposit or withdraw only up to 2 Bitcoins per day without a full identity check.[181]

Media reports of these custodial crypto exchanges being hacked and value stolen from users' hot wallets are an almost weekly occurrence. For now, the AML/CFT requirements fasten mostly on the former although this is likely to change. Trading a token on these platforms has often come at a high cost, with some reportedly charging up to USD 1 million per ICO.[182] The daily trading volumes of the largest exchanges are in the range of USD 15-20 billion per exchange, down from a peak of around USD 70 billion in January of 2018.[183] However, reports indicate that data may be inflated through 'wash trading' and unsophisticated reporting tools.[184] One report indicated that some 95% of all reported Bitcoin trading volume is either fake volume or wash-trading.[185]

In response to bans of ICOs in many jurisdictions,[186] companies looked to exchanges as a workaround, now termed an Initial Exchange Offering (ICE). Effectively, an 'ICO' is conducted and administered by and on the platform of a crypto-currency exchange. Token issuers pay a listing fee along with a percentage of the tokens sold during the IEO. Exchanges that facilitate such token sales for a fee in the US are likely to meet the legal definition of securities dealers if the issuer or any of the buyers are based in the US and, as such, they need to follow the registration and licensing requirements for broker-dealers, alternative trading systems (ATS) or national securities exchanges.[187]

Besides hacking incidents, a number of risks fasten on centralized exchanges, attracting regulatory scrutiny and, for the moment, repelling institutional investors. These risks are described below.

4.3 Decentralized

4.3.1 Exchanges

There are non-custodial (decentralized) exchanges (DEXs) such as such as Flyp.me and Localbitcoins.com which simply act as a meeting place for those buying and selling crypto-assets and do not store—that is, do not have custody of—any buyer/seller value or keys/credentials and value. A newer DEX version is Binance DEX,[188] launched in early 2019 as a non-custodial exchange using a delegated POS (dPOS) system on the Binance chain with a decentralized network of nodes.[189] Users hold their own private keys and manage their own wallets.[190]

4.3.2 Platforms

Also known as atomic swaps, trading of crypto-assets (with no fiat component) is done between counterparties on a peer-to-peer basis without the need for intermediaries or central authority. Rather, smart contracts govern the transactions such that the exchange of the two crypto-assets resulting from a trade will initially be locked through the use of Hash Timelock Contracts (HTLC), a time-bound smart contract between parties that involves the generation of a cryptographic hash function which can be verified between them and can only be retrieved by the relevant counterparty using a cryptographic hash function[191] and requires both parties to acknowledge receipt of funds within a specified timeframe using a cryptographic hash function.

If one of the involved parties fails to confirm the transaction within the timeframe, the entire transaction is voided and funds are not exchanged. The latter action helps remove counterparty risk. The time-lock function ensures the refund of the two crypto-assets to the original counterparty in the case that one of the counterparties did not retrieve the crypto-asset within a predefined time period. The first atomic swap was reportedly conducted in September 2017 between Decred and Litecoin crypto-currencies[192] but, for the most part, are in nascent stages of development.

5 Risks in the Crypto-Economy

5.1 Overview

A number of risks exist in the emerging crypto-economy, reflective of the new actors, technologies and products. Often many of these new actors are startups who do not necessarily have the resources—or inclination even—for assessing and acting on any security or compliance-related issues. The risks outlined here are not an economic analysis, which is covered in a separate paper.[193]

A Trust Frameworks

5.2 Custodial Issues and Key Management

Crypto-assets are bearer assets, meaning that if a private key is lost, the assets are lost. In that sense, custody of crypto-assets is very different from, for example, the custody of shares.[194] Reports of the theft of crypto-asset tokens are a regular occurrence, reaching over USD 1.3 billion up until May 2019.[195] The issue is that the method of storing the keys used to secure the token are insecure, or user risk management and operational security is poor. For example, investors may choose to hold their crypto-assets themselves in using hardware or software wallets so that they are in sole control of their private keys. If the hardware wallet is lost or hacked somehow, the crypto-asset as a digital bearer instrument and its value is lost. Similarly, if someone loses/forgets their password, the value may also be lost.

Cloud solutions from custodial wallet providers offer holding of private keys as an agent, conferring them with some control over these crypto-assets. In many cases, keys are sent via unsecured email. If they are selling custody, they are selling trust. Custody used to be just keys, but the breath of custody now also involves—for POS protocols—staking and governance. This is difficult for traditional custodians, as they may lose customer value[196] in sending[197] to the wrong address.[198]

A risk issue, however, is whether the custodial they have the necessary measures in place to segregate assets and safeguard them from hacks. Regulations in most of the world are silent on this type of custodial element, as private key custody is largely not yet codified as imputing possession and custody. Custodial solutions for tokenized assets are being launched by existing licensed financial service companies where the regulations allow this. In an example of the utility of an enabling bespoke crypto-asset regulatory framework, the Swiss stock exchange SIX to develop a trading platform for tokenized assets with a fully integrated trading, settlement, and custody infrastructure.[199] The Swiss investment bank Vontobel launched the Digital Asset Vault to provide trading and custodial solutions to banks and asset managers.[200]

B Market Conduct and Integrity

5.3 Addressing Money Laundering

Despite equivocation and potential arbitrage in application of legacy-type rules to the emerging crypto asset ecosystem, risk of money laundering appear to be addressed by regulators and standard setting bodies. For example, following the adoption of the fifth Anti Money Laundering Directive (AMLD5)[201] in the EU, AML rules will extend to providers engaged in exchange services between crypto currencies and fiat currencies and custodian wallet providers. Similarly, new rules for FATF require exchanges and other custodial entities that take custody of their customers' crypto-currency to obtain identifying information about both parties before allowing a transaction over their platforms. This will function much like the FATF's 'travel rule' for correspondent banks and may impose additional compliance obligations on custodial exchanges.[202] This may precipitate industry consolidation if smaller participants cannot do necessary compliance. Some believe that the new rules are over-reach and may drive the crypto-industry underground awaiting the mainstreaming of atomic swap technologies which ostensibly do not require any exchange intermediaries.

5.4 General Competition-Related

While the DLT ecosystem is still nascent, considerations of risks to fair competition still arise. This may manifest as inability for others to participate in the DL or allowing interoperability with other DLs; inability to access encryption key or access to technologies based on enforcement of patents in a relatively new market. These barriers may arise by technology design or because of market development. Market conduct regulators would have to consider whether there is a dominance of a DLT within a particular market activity. However, with the rapid evolution of DLs, competition law and regulators may struggle to define these markets, a determination that may also be complicated by cross-jurisdictional issues.

Similarly, the creation and invocation of so-called 'banlists' where groups of people decide which nodes to prohibit from accessing a particular blockchain is a percolating issue in public DLs, with no resolution as yet visible. So-called 'watchtowers' operating over the 'Layer 2' Lightning network can also identify ostensibly malicious actors who may then be blocked.[203] The question also arises in relation to governance of DLs, as to who and how changes to the consensus protocols/software are agreed to in the face of security bugs, and changes to commercial environments, and regulatory changes.[204] Does the (consensus) validation method adopted allow for manipulation by a majority of authenticators or an undisclosed consortium?[205]

Consortium, permissioned DLTs may be prone to inherent competition-related concerns. Simply, they amount to a closed group, with in most cases high qualification barriers.[206] In developing these platforms, there will invariably need be collaborative efforts necessary to implement the chosen DLT to the particular use case within a vertical. Internal governance may ameliorate or exacerbate these concerns, especially if there are governing bodies made of up of members who have the power to include or exclude members.[207] Cross-border jurisdictional issues may complicate enforcement by market integrity regulators, if they can found jurisdiction over DLTs.

And as noted above, crypto exchanges have been shown to act in concert to remove some tokens from trading.[208] Lack of practical on-chain interoperability between DLT also raises competition concerns, with balkanization of DLTs and with exclusion from technologies and data possible across vertical asset classes. Similarly, mining pools undertaking POW could monopolize some DLTs or change the underlying protocols.

The main advantage of this approach is that the investor remains the sole owner of its private keys at all times, which reduces the risk of a hack, as there is no central point of failure. Yet, not all investors may have the necessary expertise and equipment to safe keep their private key properly. Also, this model may be ill-suited to certain types of investors, e.g., institutional investors, where several individuals and not just one need to have control of crypto-assets.

5.5 Security Risks

DLTs are theoretically secured via cryptographic fingerprints that indicate whether data have been tamped with, and through the use of a range of 'consensus protocols' by which the nodes in the network agree on a shared history. Only if there is agreement—consensus—by a specific number of nodes will new data be added to a DLT system.

But while there are ground-breaking new technologies such as smart contracts associated with DLTs, they have in many cases ported security issues from the centralized world, as well as created new sets of vulnerabilities particular to the components of DLT-based ecosystems. In many cases the vulnerabilities were caused by simple coding errors. Clearly, as with the emergence of the commercial internet in the 1990s, these are enormous teething problems, but where great resources are being focused on solving any security vulnerabilities that are emerging. High-profile security hacks that have led to losses for users, as well as initiatives to deploy DLT solutions in enterprises, central banks and the wider economy have all added to the impetus for getting in front of and finding solutions to any vulnerabilities.

Some of the vulnerabilities include entities and individuals who connect to the network and have an address, which includes consumers and merchants; miners, validators, forgers, minters who process and confirm transactions on the network; and sets of rules governing the operation of the network, its participants and which blocks are added to the chain.

A large risk in current 'Nakamoto' consensus-based systems, are called 51% attacks and selfish mining attacks. A malicious actor by accumulating 51% of mining power can conduct a double spend attack and so threaten the health of the system by allowing the possibility for blocks to be revoked. Arbitrageurs may find it financially attractive to rent hashing power in order to perform 51% attacks.[209]

Cyber-security challenges are far greater in a public, permissionless DLTs where there are no walled gardens which only allow access to known, trusted participants. This creates a challenging environment where everyone has access but no one can be trusted.

There have been very high-profile intrusions into the 'vaults' that store Bitcoins, resulting in huge losses for Bitcoin holders.[210] But while Bitcoin storage facilities have been compromised, there are no reports to date of the Bitcoin blockchain *itself* being compromised.[211] Nonetheless, the underlying code in any blockchain may be a security issue: The exploitation of a flaw in the Ethereum blockchain led to the immutability paradigm of blockchain being necessarily violated by its creators to restore (potentially) lost funds.[212]

Despite the use of strong cryptography, DLTs are not necessarily a panacea for security concerns people may have.[213] Indeed, there is a tradeoff between replacing costly—and often risky—intermediaries with cryptographic key-only access distributed across nodes.[214] For example, for permissioned ledgers replacing centralized intermediaries, the cost-benefit in using blockchain is somewhat ameliorated by the need to trust permissioned authors rather than relying solely on the nodes who offer the guarantee of ledger integrity.[215]

The issues are said to be thus: the more trusted parties per node that are needed, so too does the compromisable 'surface area' of a distributed network increase.[216] Also, requiring a third party private key management function is contradictory—and possibly even nugatory—to the core 'disintermediation' principles of DLTs. In all, these tradeoffs may arguably reduce the utility of DLTs. POS solutions require nodes to staking value. The 'staker' though must be online all the time, exposing their 'hot wallet' and IP addresses, a honeypot for hackers.[217] Staking in a crypto-currency pool has similar vulnerabilities. Cold staking may be a solution, functioning through a smart contract that delegates the staking powers of a particular wallet to a staking node.

Authorized access is also an issue: Nodes on the blockchain are—using current protocols—said to be unable to distinguish between a transaction by an authorized, actual user and a fake transaction by someone who somehow has gained access to the blockchain trusted party's private key. This means that if a bad actor gains access to a comprehensive banking blockchain that itself accesses all or part of a core banking network blockchain—or a real-time gross settlement system—then this breach would in effect be compromising all banks' databases simultaneously. To circumvent or mitigate this type of risk, private key management functions or biometric linked private keys have been suggested.

The issue of longevity of the security of blockchain-based data may also be an issue. For example, the possibility of 'old' transactions on a particular blockchain may be vulnerable to advances in cryptography over a period of years or decades such that 'old' transactions can be undetectably changed. A type of equivalence to this issue would be security compromises of the circa-1980s GSM mobile technology standard—and later generations of—mobile communications encryption specifications affecting feature (non-smart) phones whose firmware cannot easily be updated with a fix for any vulnerabilities. The ability then to upgrade the cryptographic techniques used for 'old' transactions should be considered in DLT designs.

DLT-based solutions intrinsically rely upon multiple users for achieving critical mass: Nodes need more nodes to distribute the data, to do the validation of the blocks in the process of being added, and to do the processing itself.[218] Widespread adoption then is essential for the positive network effect of DLTs to be truly harnessed as a single entity using blockchain could be seen as analogous to a centralized database, Although good and important work is being done by the various DLT consortia, this may yet lead to siloed—and incompatible—blockchain initiatives.[219] So-called 'forking' of existing DLTs may also introduce fragmentation and slow down transaction processing speeds.[220] There are a number of classifications of 'forks,' which include forks, hard forks, soft forks, software forks, or git forks.[221]

Although the various DLT initiatives may address different market sectors and thus require nuanced design and implementation, some level of consistency between at least similar implementations is desirable to avoid unnecessary fragmentation that would delay the emergence of industry 'standards' for a sector. Besides, interoperability required to connect these silos may introduce security and efficiency risks to the respective blockchain operations number of initiatives to enhance interoperability between DLTs to facilitate secure communication between separate and independent chains.[222]

5.6 Trust in 'Oracles'

There is concern generally about the validity of information inputted/outputted through the natively 'off-chain' oracles, particularly as it affects smart contracts. Although the data on a blockchain itself is said to be secure, and any block additions approved by consensus, this a blockchain cannot in of itself—at least with current technology—address the reliability or accuracy of the data input. Blockchain thus only addresses a record's authenticity by confirming the party or parties submitting a record, the time and date of its submission, and the contents of the record at the time of submission,[223] and not the *reliability* or *accuracy* of the records contained in the blockchain.

If a document containing false information is hashed—added to the blockchain—as part of a properly formatted transaction, the network will and must validate it. That is, as long as the correct protocols are utilized, the data inputted will be accepted by the nodes on a blockchain. This is the DLT incarnation of the unfortunate mantra of 'garbage data in, garbage data out' which is usually characteristic of some databases in the non-DLT world.

The possibility has also been raised of an individual participant on a blockchain showing their users an altered version of their data whilst simultaneously showing the unedited (genuine) version to the other participant nodes on the blockchain network. Others may only be able to trust the data on the blockchain if they can cross-validate data across multiple user nodes.

5.7 No Standardized Rating Systems

There do not appear to be reliable crypto ratings, akin to a Moody's. Investors have no reliable way to determine whether a crypto-asset or the issuer is reliable.

C *Trading*

5.8 Trading Platform Risks

5.8.1 Overview

A number of risks relate to specially centralized crypto trading platforms can be identified, some of which may require regulatory intervention. These risks include lax security leading to hacking and theft; omnibus accounts versus segregated accounts; lack of deposit insurance; lack of AML/KYC processes; business models, counterparty risk, and conflicts of interest.

5.8.2 Lack of Safety in Crypto Asset Key Custody

There have been prominent hacks and thefts from centralized crypto trading platforms. More than often these are not regulated, nor is there any insurance or compensation to investors for their loss. Traditional markets have investor protection, surveillance—but not necessarily in the crypto-economy.

Centralized platforms require users to deposit their assets with the platform prior to trading. In the crypto-asset world, this means providing the exchange with their private keys. Similarly, fiat money must be deposited to pay for any fiat-crypto pairings. In most cases, these are fungible, in that users do not see their 'wallets' housed in the exchange: rather a wallet balance is a database entry updated by the exchange itself, with all the funds in the exchange are commingled,often with the exchange's own funds. This makes it the exchange's responsibility to be the keepers of the records of ownership. The exchange though become the only 'trusted' source of wallet 'balances.' There is no way for any outside auditor or party to verify this in the absence of mandatory regulations.

This concentration of keys makes these platforms represent a single point of failure where clients have made these exchanges a honeypot for hackers. The amount of stolen crypto-currency from exchanges in 2018 has increased 13 times compared to 2017, reportedly USD 2.7 million in crypto assets stolen every day, or USD 1,860 each minute.[224] The exchanges are usually fintechs, with poor operational security commensurate with the levels of assets they are meant to have custody of. Simply, any regulated (legacy) instruction with such poor levels of security would have been sanctioned or liquidated by regulators.

5.8.3 Technology Reliability, Standardization and Scaling

Most exchange-based trading today is done off-chain, with settlement done on-chain. This, under current technology constraints, is notoriously slow. So while DLTs transparent, but don't scale as yet for settlement. The challenge is how to trade fast akin to legacy systems while the asset movement is slow. Similarly, there is concern on the longevity of such DLTs: no one worried about gold turning into lead, but the DLT technology might. Contingencies to 'rescue' data on obsolete DLTs must be devised. A Gartner report warned that 90% of blockchain technology used by enterprises in 2019 will, because of fragmentation and lack of interoperability, be at risk of becoming obsolete or insecure by 2021.[225] At the organizational level is where resource management and general business operations traditionally occur, and who may control and govern this process varies and can be unclear.[226]

5.8.4 Competition-Related

Akin to de-risking of correspondent banks in developing countries because of ostensible AML/KYC concerns,[227] there are reports of banks refusing to service crypto businesses. Ironically providers in Malta—with its innovative crypto asset framework that attracted many crypto-focused fintechs to the island—have been refused service by many Maltese banks. Some suspect coordination between the banks in decision making.[228]

Exchanges have been shown to act in concert to remove some tokens from trading.[229] Lack of practical on-chain interoperability between DLT also raises competition concerns, with balkanization of DLTs and with exclusion from technologies and data possible across vertical asset classes. Similarly, mining pools undertaking POW could monopolize some DLTs or change the underlying protocols.

5.8.5 Veracity of Trading Data

Accurate data to measure and monitor the safety and soundness for systemic and investments purposes is required, but to some degree not altogether trusted.[230] Sources differ with regard to the methodologies used, the completeness of coverage, and access to the underlying raw information, while processing of raw information (when available) is also surrounded with uncertainty related to the lack of (or only partial) regulation pertaining to the various players along the crypto-asset value chain, which operate unsupervised in a borderless environment often hindering access to reliable information. Similarly, as noted above, reports indicate that data may be inflated through 'wash trading' and unsophisticated reporting tools[231] with one report submitted to the US SEC in March 2019 claiming that some 95% of all reported Bitcoin trading volume is either fake volume or wash-trading.[232] Data must thus be handed with caution.

5.8.6 Counterparty Risk

In most cases, only deposit/withdrawal is recorded on-chain by exchanges. This means that the settlement of trades is not dependent on DLT, which may have some benefits such as no congestion risk and no scalability issues. The downside is that there is counterparty risk vis-à-vis the platform.[233] And while crypto markets are very liquid on a retail basis, they do not attract institutional investors to any large degree. For them, deposits of large values to unregulated exchanges with demonstrably poor security and with turnkey offerings—custody, clearing and settlement, for example—that each attract risk is a no-go for institutions. Unless there is market oversight surveillance and data is verified, the attendant risks of trading large institutional funds is too large.

As a result, institutional investors have shied away from direct investment in crypto-assets, effectively reducing trading liquidity and a viable secondary market for crypto-assets. Exchanges are clearinghouses and settlement at the same time. This model leads to illiquid markets as one needs to differ between clearing and settlement. That is, for the crypto-asset ecosystem to scale, there is a need to build trust for institutional level, for example needing custodian who cans sell trades without being a party to it. There is additional heightened concern as a big difference with legacy is that crypto transactions are not reversible: hence there is some counterparty risk of sending value to the wrong addresses.

D Technology Risks

5.9 Speed and Scalability

Many public, permissionless blockchains aspire to achieve a fully decentralized operation.[234] The blockchain scalability trilemma represents a widely held belief that the use of blockchain technology presents a tri-directional compromise in efforts to increase scalability, security and decentralization.[235] All three cannot be maximized at one time and increasing the level of one factor results in the decrease of another. Hence DLT's goals of striving to reach maximum levels of decentralization inherently result in a decrease in scalability and/or security. This is, we suggest, a new trilemma: the 'crypto-economy trilemma,' an adaptation of Vitalic Buterin's original 'blockchain trilemma.'[236] These are shown in **Exhibit 12**.

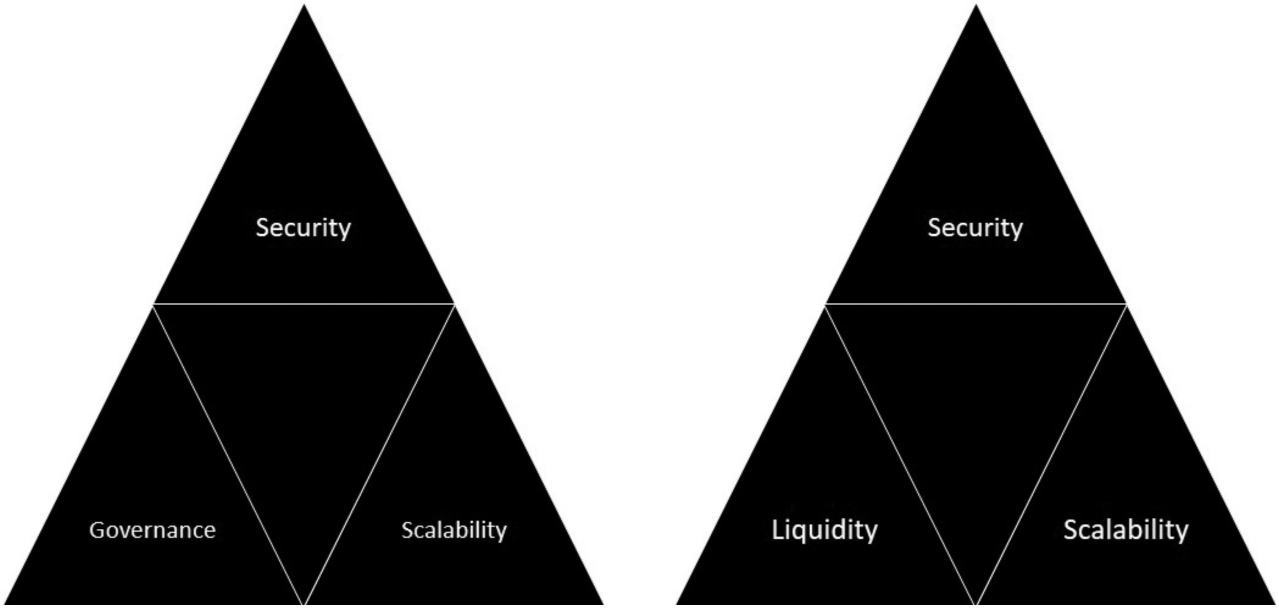


Exhibit 12: The 'trilemmas' in the DLT world. Left, the original 'blockchain trilemma' developed by Ethereum founder Vitalik Buterin. Right, an emerging 'crypto-economy trilemma.' In both cases, two but not all three conditions may exist at the same time. Security and scalability is a common feature of both 'trilemmas.' In this understanding and depending on the type of DLT, both 'trilemmas' can exist simultaneously.

5.10 Lack of Technology Standardization

As noted above, the lack of practical on-chain interoperability between DLTs also raises concerns of the balkanization of DLTs and with exclusion from technologies and data possible across vertical asset classes. Given the state of DLT technologies, this may be both a feature and a bug: the market may decide which DLTs are best suited for use, although this experimental phase will invariably result in wasted investments in some DLTs and the potential that data may be lost if a provider (usually) a fintech goes out of business. Reporting requirements may also be impacted by this fragments and non-use of standards.

6 Regulatory Approaches to the Sample Financial Components of the Crypto-economy

6.1 Overview[237]

A challenge for regulators is to understand the impact of DLT in their utilitarian function and similarly, the impact of the range of new crypto-assets and their often hybrid nature in linking not only to 'real world assets' but to other native crypto-assets. Not all raise the same risks and regulatory and oversight issues.

Regulators in their approaches may suffer from inertia, either because of capacity to develop new policy around new asset classes, or public policy issues based on regulatory arbitrage, or even regulatory capture. In the case of the nascent crypto-economy, it is more likely that the capacity and arbitrage issues prevail.

For efficient regulation and to avoid regulatory arbitrage though, regulators to understand where they have remit, and the concomitant regulatory touch points. In particular what parts, if any, of the entire life cycle of a crypto asset may need oversight, be it from one of more regulators. Some asset classes may, natively, be of a type that has multiple regulators involved. The life cycle may mean the development of the underlying Layer 1 code, protocol development and any downstream alterations, then the issuance of token containing the assets, their distribution, custody, trading and clearing and settlement. Or for that matter, given the decentralized and often anonymous and pseudo-anonymous nature of the crypto-assets, whether some types and trading thereof can even be regulated.

Of course, the DeFi ecosystem may remove by design or by natural conflation some of these parameters/actors (for example the custody and clearing and netting actors). Anonymity and decentralization may confound application of the rules, particularly in public blockchains, although permissioned blockchains may provide more proximate touch-points as the parties may be identifiable. Similarly, the new actors in the DeFi ecosystem—particularly the miners—may provide additional touch points. Even so there may be gaps.[238] In that context, omnibus restrictions or 'one size fits all' approaches may stifle innovation.

We stylize the potential regulatory approaches as no action; forbearance; restrictive; bring into scope; bespoke and hybrid. And we simply note here, but do not discuss, the impact of the most prominent legal families—common, civil, Germanic, Roman Dutch, and Sharia law—on regulatory approaches and philosophies.

6.2 Regulatory Philosophies

Banking, payments and investments and indeed the entire financial ecosystem are some of the most regulated and supervised economic sectors.[239] Central banks especially guard their usual remit over the financial ecosystem a lens of systemic effects of the introduction of new technologies and processes, especially since the sinew of the global financial system is such that most, if not all, of the financial institutions are connected in some way or another, and are, at a minimum, buffeted by systemic events in other countries or other sectors of the financial world. Therefore, elaborate sets of interconnected regulations are imposed on many components of the financial system.

The financial sector's 'crash' in 2007-8 set off a pandemic of associated crises around the world and highlighted the weaknesses, and the gaps, in the regulation of this sector. The inadequacies of the contemporary model of financial regulation were exposed at national and global levels.[240]

Regulation here may refer to governmental actions to grant or place conditions upon the rights of firms to provide goods and services in particular areas of economic enterprise with the purpose of preventing decisions by private agents that would take insufficient account of the 'public interest.'[241] Available regulatory tools and models that provide answers to these regulatory challenges range from general principles to detailed rules.

Two theories of regulation of industry are widely held: positive theories of regulation and normative theories of regulation.[242] Positive theories of regulation examine why regulation occurs[243] while normative theories of regulation are based on a theory of market failure.[244] Famed economist Joseph Stiglitz notes that regulation begins with a simple question: Why is regulation needed and followed, and why do markets by themselves not suffice?; and then: If there is to be government intervention, why does it take the form of regulations?[245] Some would see the need for regulation[246] as a response to market failure, others as the need to provide the groundwork for growth and consistency in rule-making and policy. The argument is not yet settled and puts into relief what has been called the 'regulator's dilemma' which exists where a balancing act is required whereby the regulator enables innovation whilst still having to mitigate any existent risks.[247]

These dilemmas arise because financial regulators are charged primarily with maintaining system stability as the price of systemic disruption is so high and the interdependencies great. Network externalities and the need for competition efficiency—which may be from market failure—[248]may greatly influence policy.[249]

The regulatory rationale could be placed under the heading of public interest, which allows the public or some subclass of the public to interact with financial institutions with a degree of safety by increasing consumer awareness and information.[250]

Regulation too is an instrument of social policy[251] intended to influence and control market and business behavior, which may amount to strata of regulations, usually forms of self-regulation, co-regulation or pure statutory regulation.[252] The latter especially is informed by public policy goals, which may in turn be influenced by national, regional or international trends. The need for consumer protection is especially considered to be a public policy response to a market failure. Regulators must, however, balance the need to protect consumers whilst avoiding over-regulation[253] or for that matter, effectively impractical regulation that may have the opposite of what is intended.[254]

Generally, though, regulators will not act in a vacuum, but will undertake consultation with industry and impact analysts beforehand, usually as Regulatory Impact Assessments (RIA) which check on the cost, practical implementation effects, and generally any benefits or hazards of any proposed regulations.[255]

Regulators however, may be caught in the vice of what famed economist and Nobel prize winner George Stigler termed 'Regulatory Capture,'[256] variously defined as the possibility that the regulated institutions may have inordinate influence[257] on their own regulator such that the 'captured' regulator acts primarily in the interests of those that it should regulate independently, rather than in accordance with their putative mandate to promote the common good, that is, the 'public interest' option identified by Breyer and MacAvoy. Often, regulation may be necessary where contractual remedies may be seen to be insufficient to produce equitable results possibly due to the substantial inequality of one contracting partner.[258] Many of the newest products and services are processed through private networks subject only to private rulemaking from which consumers are excluded.[259]

The resultant call for public law to step in may be explained in behavioral science where it is thought that, if economic agents are subject to behavioral biases, then there is scope for some 'paternalism' in the form of the choice of default rules, usually determined by normative rules and regulations. If these defaults can be easily changed, this new form of paternalism is thought to have no cost, but possibly to have substantial benefits to the actors and society.[260]

6.3 Types of Regulatory Foci[261]

There have been and are two broad approaches to the issue of regulation and concomitant consumer and financial system protection: the *institutional* and *functional* approaches. Each may reflect variation in legal frameworks in a particular jurisdiction.

The functional approach places the focus on the service received by the consumer regardless of the type of institution providing that service. This broad protection may be the remit of specific consumer protection agencies, competition authorities, or ministries of trade and industry. The issue however, is that while this 'catch-all' appears to provide recourse insofar as all institutional types[262] are concerned, the reality is that these entities may ultimately lack the necessary institutional capacity and specialized knowledge to pronounce on, for example, complicated aspects technologies such as DLTs. Thus, multiple regulators may have (ineffective) remit over the same entity for different reasons, and may result in consumer ambivalence, corporate intransigence and posturing, and thus the effective maintenance of the status quo.

In contrast, the institutional approach focuses not on the service *per se*, but on the institutions providing any financial service. It supposedly leaves the regulation in the hands of specialized bodies, for example, the central bank, which may implement provisions in relation to regulated financial institutions. However, this approach may distort market dynamics by fragmenting responsibilities amongst too many regulators to the extent that some entities are not captured. Implementation may also be challenging insofar as multiple regulators with varying levels of capacity may be required.

6.4 Approaches

There is often no one-size-fits-all solution to the design of a legal framework for new technologies in the financial sector. It should reflect the structure of the financial system and the nature of each economy's overall legal framework. That said, regulatory approaches to the relatively sudden introduction into an economy of transformative systems and technologies can take one of a number of forms. Here we stylize them into the approaches below and expand thereafter:

- No action
- Forbearance
- Restrictive
- Bring into Scope
- Bespoke
- Hybrid

6.4.1 No Action

Here the regulator does not see the need to take action against an entity or person who has planned to or has introduced a new technology and product/service to the market that regulator has specific remit over the entity (institutional approach) or the product/service (functional approach).

In many cases, the regulator will issue a No Action Letter (also called a Letter of No Objection) to a party who seeks clarity from that regulator if they can proceed without fear of action by the regulator, with the introduction of their product/service.

6.4.2 Regulatory Forbearance

Forbearance has been the hallmark of a number of regulatory approaches to the emergence of crypto-asset products and services. Here the regulator takes a 'wait and see' approach to a situation it may or should have taken action in response. Regulatory forbearance is not necessarily about supervisory incompetence though but, rather, the potential for a fully briefed regulator to decide not to intervene. The degree and period of forbearance may depend on the impact foreseen, but may result in some regulatory activity, often an enforcement action and/or new sets of regulations

6.4.3 Restrictive

Here the regulator takes action to restrict or ban the introduction and/or use of introduction of a product/service, or indirect restrictions on others from providing supporting services to those using or introducing the product/services. A number of countries have banned or restricted the use, or mining, trading, provision of products and services related to crypto-asset products/services and the underlying technologies. Some have restricted banks from providing financial services to companies providing these services or have banned consumers from using their bank savings to buy crypto-assets.

6.4.4 Bring into Scope

While some crypto-assets may already fall within the scope of financial regulation, others may not and regulators need to consider whether there is a need to bring them into scope. This assessment should be undertaken while considering the risks that they may pose to their objectives of investor protection, financial stability and market integrity.[263] This invokes the need to distinguish where possible between the characteristics and purpose of a crypto-asset as existing regulatory framework may, most likely, not have been designed with these crypto-assets in mind, even if a functional, principles-based approach to regulation was used in creating the existing regulations. Regulators may then need to build a taxonomy of these services and products—much like has been done in this paper—that ventilate their design and purpose for that jurisdiction.

Similarly, a functional approach to regulation may capture new actors where the institutional approach does not. That is, services in the crypto-economy that are not directly regulated by name but offered by similarly 'uncodifed'—that is, undefined or not mentioned in existing regulations—actors may nonetheless be captured (and brought into scope) by existing regulations. However, the regulatory reach may be tenuous and fluid, defined by the degree to which a system is decentralized, not necessarily that it is decentralized *per se*. This may turn on whether there is a central party which controls (governs) a platform. Identification as such may trigger a host of intertwined requirements.[264] But if there is no central party or figure left—termed a 'moonrot'[265]—but the product is live and being used, then does the control ('governance') depend on how many distributed nodes there are or is there some other metric needed for this assessment?

The obvious issue though is whether, in a truly decentralized environment, how the market operator could be identified.[266] This is not an easy determination as the number of nodes on a public dApp are fluid by nature. Purposive regulatory regimes may be more reflexive to undertaking this assessment, although it is made easier with permissioned DLTs which usually have some semi-centralized governance structure.

There is also the issue of how to bring into scope new actors into existing regimes. Crypto-miners and validators for example are the newest actors in this domain. Australia appears to be the first jurisdiction to codify that miners/validators are subject to securities regulations under certain circumstances.[267]

From a product portfolio perspective, tokenization of assets—now styled as crypto-assets—means that legacy assets under a separate regime may be brought into a new regulatory scope as a new asset class. For example, use of STOs process to tokenize legacy assets such as real estate. Similarly, legacy assets could simply be tokenized with a crypto-wrapper, but not in a manner that creates a new asset class as is the case with STOs.

Shoehorning of new actors and products/services should be applied consistently or risk creating regulatory arbitrage. If a modicum of shoehorning to bring these services into scope may however expose gaps and issues in the current rules, that leave certain risks unaddressed or that may not be adapted to DLTs.[268]

6.4.5 Bespoke

As regulators in some jurisdictions struggle to bring into scope of existing regulations, they have created bespoke regulatory regimes that incorporate—new crypto assets and the actors that provide or support them. These are ostensibly designed to create proportional rules relative to the specific risks and issues posed by those crypto-assets, as well as serve as a magnet for investment by fintechs who can essentially provide these services to anyone on the planet.[269] These include Malta and Abu Dhabi.

From a survey of jurisdictions that have launched such specific crypto-asset frameworks, all address and incorporate the known, major crypto-assets by function, although they may be called something else.[270] That is, these usually incorporated in some form at least CC, ICOs, UTs, and ST. Recent 'innovations' such as IEOs and ETFs that have a basket of crypto assets do not appear to be incorporated as yet.

6.4.6 Hybrid Approaches

Hybrid approaches may contain elements of restrictions and forbearance, but not necessarily any shoehorning in the absence of specific enabling regulations, nor any provision of no action letters.

6.5 Stylized Application of the Approaches

6.5.1 Exchanges

Overview

Automated matching of buy and sell orders by electronic communications and information processing systems is a feature of almost all modern economies, using algorithmic trading and 'matching engines.'[271] Usually though the exchanges and platforms are licensed by regulators to do just this one thing, and do it transparently, reliably and efficiently. New crypto-exchanges that break through this functional firewall, offering a range of services to a nascent industry.

Legacy

It is trite that 'legacy' trading platforms—here, exchanges—have specific functions of trading, with other entities involved in trading of legacy assets—such as broker-dealers, clearing house, custodians—being regulated separately according to their function. Regulations fastening on exchanges relate to fidelity in their structure and services and market integrity, for example having the necessary resources to effectively conduct its activities and address the risks that may arise from them; whether it has established and maintains adequate arrangements and procedures to ensure fair and orderly trading; whether it has adequate measures to prevent conflicts of interest and whether it provides non-discriminatory access to its services.[272] Similarly there are mechanisms in place to ensure sufficient and reasonably accurate price discovery mechanisms and to ensure and include whether pre- and post-trade information made available by the platform is sufficient to support market efficiency, fair and orderly trading and whether the platform has adequate rules, surveillance and enforcement mechanisms to deter potential market abuse. Regulators in most jurisdictions will apply some or all of these criteria in licensing and supervision of exchanges.

Crypto-Economy

Exchanges in many jurisdictions operate in a twilight world of regulation, reflecting in many cases in gaps in regulation where they may not regulated at all because of lack of remit by a regulator or through regulatory forbearance; or where there is regulatory arbitrage resulting in effective light touch regulation, bespoke regulation designed to recognize the unique nature of exchanges and variations—centralized and decentralized, or simply connecting counterparties without being involved in the transaction. In many cases, exchanges have moved to 'crypto-friendly' jurisdictions such as Malta to allow them to not only act as a exchanges (once a token is issued), but also as turnkey lunch pads and service providers for issuance of tokens themselves, usually as part of and ICO.[273] There are often very few (transparent) rules on whether or not an exchange can unilaterally choose to remove or prevent a token from listing or trading on its platform, raising potential competition issues.[274]

While exchanges 'democratize'[275] access to trading by allowing investors to access the trading platforms directly without an authorized intermediary through outright and direct ownership rather than through a personal right to an intermediary. And given the large anonymous or pseudo-anonymous nature of at least crypt-crypto trading pairs, this may market integrity issues if for example there is a lack of proper KYC.

Further, after issuance token liquidity may be weak, preventing fast liquidation of the token. The siloed nature of some exchanges and the absence of a broker dealer in the life cycle of that asset may also affect price discovery across exchanges of the same asset type.

Stylized Regulatory Approaches

- While they may continue to be unregulated in environments where regulation is not possible or where the political economy is such that is not desired, to decrease volatility in crypto-asset value, to enhance consumer protection; and to mitigate in advance any systemic effects of crypto-asset-linked funds being linked to unregulated, volatile assets, regulation may be needed.
- This may take the form of regulation equivalent to that currently fastening on public, regulated exchanges of securities and funds, or as part of an exploratory, interim sets of regulations as part of a regulatory sandbox.[276] Exchanges though have been shown to be very susceptible to hacks and thefts, with little collateral to insure investors that tokens stored with an exchange for eventual trading would not be lost.
- While some centralized exchange trading crypto-assets purport to undertake the entire life cycle of issuance and trading on a DLT, the current state of the technology is that most trade settlement typically occur on the books of the platforms (off-chain) in the case of centralized platforms. For decentralized platforms, this is done on-chain. In that sense, many of the rules relating to who is authorized to do off-chain clearing, netting and settlement could be applied to the centralized platforms, through including the functions in the existing regulatory silos of C&S and custody. Indeed, at one end, some platforms

adopt practices from traditional security trading platforms[277] while others use simple systems bootstrapped to support crypto-assets.[278]

- The alternative, as has been done in some jurisdictions, is to create class of providers who can undertake all the legacy activities in one turnkey authorization, but with safety and soundness criteria modified to reflect the trading of crypto-assets. For example, clarity may be needed on how to apply the existing rules to models that use smart contracts to match orders and/or conclude transactions, because the exchanges are still relatively new and with limited resource and a platform operator may not exist or be needed.
- Exchanges commingling customer funds with the exchange's own funds should be avoided.
- Similar rules may be required for business continuity in times of high volatility and financial stress.[279] That may lead to insolvency of the platform and loss of investors' funds.[280] Some mandates for insuring investor's funds in case of a cyber-attack for example may be required.[281]
- Less certain is how to regulate, if at all, truly decentralized exchanges where the only participants are the retail counterparties using smart contracts. In this case, regulatory forbearance may be appropriate until these trading methodologies become a mainstream reality.

6.5.2 Data Reporting and Record Keeping

Overview

Investors trading strategies invariably require access to for example, trading volumes and values that reflect the popularity, history and liquidity of any tradable asset class. The classifications to allow for easy comparison are usually in standard formats.

Legacy

Legacy reporting regimes use common identifiers and classifications, usually ISO-generated codes for financial instruments, for example ISO 10962 CFI code[282] for classifying financial instruments, and ISO 4217 for currency code. The CFI code is a cornerstone of many reporting regimes that allows to prescribe precise rules for data reporting,[283] validation and processing dependent on specific classification of instruments, taking into account distinct characteristics of different asset classes.

Crypto-economy

Crypto assets too have generated their own 'interim' classification codes for trading, for example BTC for Bitcoin and ETH for Ethereum as an unofficial application of ISO codes. While ISO and other legacy classification systems have not (yet) produced specific crypto-assets codes, making domain, SIX Interbank Clearing—a Maintenance Agency of ISO—is currently studying the impact and role of crypto-currencies and other independent currencies on ISO 4217.[284] The CFI standard however does not yet have a specific classification of crypto-assets and does not allow for differentiating them from traditional instruments, nor distinguishing between various crypto-assets and their specific characteristics. Problematic too is that data reporting is not standardized nor verifiable and thus some exchanges volumes are, according to some recent studies, apparently fake.

Stylized Regulatory Approaches

- In many cases, standardized ISO codes can only be used for (officially) recognized financial instruments. The definition per country of a financial instrument per jurisdiction may differ, making standardization of instruments and potential linkage of crypto-assets difficult and tenuous. This means, *ab initio*, even if they are recognized, some assets may not necessarily be able to comply with (standard) data reporting requirements without these codes.
- As the regulations on reporting were designed to capture traditional instruments and not crypto-assets, the information to be reported as per the existing rules might be not sufficient/appropriate to describe the particularities of crypto-assets and transactions in those; thus, hindering the fulfilment of the objectives of the respective regulatory reporting regimes. Some supervisory rules would also need to be revisited to provide clarity on the issues related to crypto-assets. Not just crypto asset exchanges but any 'legacy' systems using hybrid products—for example tokenized securities—would have to use these (still evolving codes) for their own reporting requirements.

6.5.3 Custodial and Safekeeping Services

Overview

Safekeeping and record-keeping of ownership of securities and rights attached to securities (and law of negotiable instruments) is a critical component of any functioning economy. It not only proves ownership of assets, but also determines the negotiability of any instrument and their use as collateral for credit or for securing, for example, counterparty risk.

Legacy

In many jurisdictions, assets to be traded, held as collateral or as proof of ownership are held by authorized entities such as custodian banks, registrars, notaries, depositaries or CSDs. These are variously known as custodial and safekeepers who hold them on behalf of others to minimize the risk of their theft or loss. A 'custodian' holds securities and other assets in (usually) unencrypted electronic or physical form.[285]

Crypto-economy

Crypto-assets are, in effect, native digital bearer instruments. The DNA of the crypto-economy is that assets are held on tokens that are only accessible through the use of a private digital key available to the owner, or someone the owner provides the key to, for example, an exchange. The evolving debate amongst regulators is whether having control of private keys on behalf of clients is the equivalent to custody/safekeeping services,[286] and if so, whether the existing requirements should apply to the providers of those services.[287] There are significant hurdles to overcome if traditional custody banks are to engage with this emerging asset class, including operating models, technology, risk, compliance, and legal and regulatory frameworks.[288]

Stylized Regulatory Approaches

- As has been noted, there are significant weaknesses in warehousing systemic risk in modern Financial Market Infrastructure (FMI) as a result of a market failures and structural flaws deeply ingrained in modern financial markets. The regulations that have developed therefrom have also shifted direct investor control over their investments to a custodial paradigm with a range of Central Counterparties. Custody costs money and removes direct ownership. The potential for use of DLTs for securities and derivatives could increase investor control, improve the efficiency of systemic risk distribution, and create a more diverse and resilient financial ecosystem.[289] The use of DLT for these purposes however still needs to be mandated, in particular what defines custody as well as forms of custody—that is allowing the assets to be placed on a DLT.[290]
- From a crypto-asset perspective (that is native crypto), the first issue that arises is about the interpretation of what constitutes safekeeping services.[291] One view is that having control of private keys on behalf of clients is the same as safekeeping services and that rules to ensure the safekeeping and segregation of client assets should thus apply to the providers of those services. Multi-signature wallets, where several private keys held by different individuals instead of one are needed for a transaction to happen, will also require consideration.[292] There may be a need to consider some 'technical' changes to some requirements and/or to provide clarity on how to interpret them, as they may not be adapted to DLT technology.[293]
- The attribute of a crypto-asset generally being native digital bearer instruments may alter laws of negotiable instruments in so far as this confers super-negotiability on a crypto-asset since it is no longer in the hands of an intermediary such as custodian but is fully owned by the owner as its holder of its private keys. The US state of Wyoming has already recognized and codified this shift in ownership and thus negotiability.[294]

6.5.4 Clearing and Settlement, and Settlement Finality

Overview

Key to financial transactions is transfer of assets to a counterparty, to the extent that all right, encumbrances attaching to that asset are extinguished after transfer. There are large, and emerging differences between legacy systems of clearing, netting, and settlement as part of an FMI, versus the relatively truncated process involving transfer of crypto-assets.

Legacy

For the most part, financial transactions transferred to counterparties must go through a process where the value (and instrument, if applicable) are done through a process of clearing, netting, and settlement. Each of these components of a financial market infrastructure consisting of the various systems, networks, and technological processes that are necessary for conducting and completing financial transactions.[295] These are all highly regulated to ensure the safety and soundness of the financial system.[296] Key though for any FMI—be it for payment or securities or any other asset—is the requirement for settlement finality, meaning that the counterparty is sure that the transaction will complete, and the value or asset will effectively be in the hands of the counterparty. Any equivocation that settlement finality may not occur could fundamentally affect the stability of financial ecosystem.

Crypto-economy

Given the nascent nature crypto assets and the methodologies for transferring value between counterparties and the lack of institutional support for any crypto-assets and its 'trading rails,' exchanges have been the focal point of value transfer of crypto-assets. To a large degree these are unregulated, often firmly ensconcing themselves in jurisdictions where there are no directly applicable standards for C&S.

Two issues are dominant here. First, given that the exchanges do custody, issuance, C&S, all risk is concentrated there. Secondly, given the design of some blockchains such as Ethereum, settlement finality is not determinislistic, that is, is not guaranteed. Instead it is probabilistic as consensus must be reached for a block to be added by nodes containing that settlement transaction (transfer of 'ownership' to the counterparty. The essence of the issue is that the risk is concentrated in the exchange,

Stylized Regulatory Approaches

- Coincident with issues of trading is how to ensure that the clearing, netting settlement processes are sufficiently sound and safe that funds and assets are not at risk. To be sure, for the crypto-economy to evolve, institutional investors need to be sure that there are regulations that create the environment for safety and security.
- Centralized exchanges—particularly those where fiat-crypto pairing are undertaken—currently provide some touchpoints for regulators to fasten these safety and soundness criteria.
- Given that there is interest in some financial institutions to perform custody solutions, there is a need for certainty of transposing current regulations.
- An interim measure could be allowing existing exchanges to undertake some of the clearing and settlement components 'off-chain' under regulation that fastens on legacy providers of these services. These may not, however, be practical in all cases as technology evolves to undertaking all transactions as gross settlement, with no clearing or netting *per se* required. Similarly, the near horizon of decentralized exchanges—or atomic swaps—where trading is effectively 'exchange-less' will ensure in this context keep all these transactions on-chain and the settlement near instantaneous.
- Greater certainty around the concepts of settlement and settlement finality applied to crypto-assets is needed.
- There may be a need to distinguish between permissioned and permissionless DLTs in that respect, in particular, specific governance issues with permissionless DLTs, which makes them less suitable to the processing of financial instruments, at least in their current form.[297]

6.5.5 Underlying Technology Use and Development

Overview

Besides the policy issues—that is, how far (if at all) can DLTs and their applications—such as decentralized finance (DeFi)—can be implemented in specific sectors, there are a number of open legal issues in DLTs to consider. The legal response, though, would be determined by the legal system in use in a country, for example, if it is a common law or civil law jurisdiction. The crisp legal issues relate to how specific DLTs and their applications would 'interact' with current laws and regulations governing (these) specific sectors, and common law rules (where used) that are needed where laws and regulations are silent or non-existent. All these open (and evolving) legal issues suggest that embracing of DLT for mainstream commercial and public use requires both doctrinal and legislative shifts.

Legacy

Doctrinal and legislative shifts came to the fore in the 1990s with the use of electronic forms of communications in mainstream commerce. Legislatures and regulators globally changed their instruments to allow electronic records to be used in place of paper documents for storage and record keeping, and electronic signatures to replace wet signatures. This was known as functional equivalence. Many of these changes were based on the United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce of 1996 in furtherance of its mandate to promote the harmonization and unification of international trade law, so as to remove unnecessary obstacles to international trade caused by inadequacies and divergences in the law affecting trade.[298] In the US, the Uniform Electronic Transactions Act (UETA) was similarly passed as a model law intended to harmonize rules governing electronic commerce transactions in 47 states.[299] Legacy systems, as they are now, benefited fundamentally from these changes.

Crypto-Economy

A sample of the legal issues that would appear to be most pertinent to DLTs include the legality and enforceability of smart contracts; time and place of contracting using a blockchain and smart contracts; the 'chain' of legal liabilities in the sector; competition issues in a decentralized environment; criminal use and liability; and which court may have jurisdiction over a matter involving DLTs and their applications in a 'distributed' multi-national nodes environment. Without certainty as to the use of DLTs in mainstream commerce, many of these system and innovations could labor under a cloud of not being recognized for the purposes the parties intended, as well as halting the use of DLTs with legacy non-crypto-asset types and data.

Stylized Regulatory Approaches

- Laws and regulations could be changed to apply functional equivalence to use of DLs in everyday commerce, provided that a DL meets certain requirements. These requirements should be specified. This would put smart contracts and blockchain records and signatures on equal footing with written contracts, subject to express limitations on blockchain records in cases when:
  - The blockchain record is not in a form for retention and later accurate reproduction
  - The law requires a record to be posted or displayed by a specific method
  - Access to store or retrieve information to or from the blockchain is limited by a party
  - A notice with respect to certain cancellations or defaults is required.
- Similarly, legislation could be provided that smart contracts may not be denied legal effect, validity or enforceability because they contain smart contract terms or are in the form of code. For the same effect, laws could be amended to recognize that signatures, records and contracts secured by a party through DL technology should be deemed to constitute an electronic signature and electronic record. These may be given effect based upon the context and surrounding circumstances of electronic signature or record.
- Coincident with these changes, existing laws of evidence could be tested to indicate whether courts may accept DL-based evidence and also what weight should be afforded to this evidence. In particular, it should be determined whether in some or all cases, a record on a DL serves as the equivalent of a notarization of the data and if so, who or what would be the notary equivalent. If needed, laws could be amended to ensure that a smart contract, record or signature created, stored or verified on a blockchain may be enforceable or given legal effect, and may be admitted as evidence, with the weight of that evidence to be deduced from surrounding circumstances.
- Another related issue is the role of 'miners' and how they would be handled under the existing rules given their novel and fundamental role in the settlement process.[300] This however touches on controversial issues of holding coders and developers liable as 'fiduciaries for transactions they help settle for reward.[301] While these could conceivably be achieved under existing regulations relating to technical services providers providing critical serves to C&S operators,

practically identifying and then fastening any rules on their activities given largely decentralized nature of public blockchain could be regulatory overreach. Some regulators have, however, proposed making coders liable for any breaches of regulatory norms. For example, the Australian securities regulator issued rules in May 2019 that in effect, makes miners (and transaction processors) automatically and vicariously part of the regulatory regime where their mining activities are part of the C&S process for tokens that are financial products. This is likely to have a chilling effect on incentives for miners to undertake mining activities where any measure of risk (liability) may fasten on them where there was none before. Less mining means the DLT becomes more inefficient and concentrates hashing power to the degree that the DLT may be subject to a '51% attack' described earlier.

- A more practical regulatory innovation—and far less chilling on the incentives to miners to mine, and innovators to innovate—would be that modifications of existing rules could be fastened on permissioned DLTs only, specifically those federated types in financial verticals such as banking and insurance. The reason is simply that these miners and innovators are specifically employed—rather than compensated on an *ad hoc* basis as in some public DLTs—to process blocks or to develop system enhancements, as the case may be.
- Some countries have introduced what are known as 'regulatory sandboxes' that provide a light-touch regulatory space for fintech to test their innovations.[302] While most sandboxes include fintechs developing DLT-based solutions. India however has formally excluded them from its sandbox.[303]

6.5.6 Security of Transaction Systems and Data

Overview

In the current climate of increased cyber-attacks, cyber-security is by design and by default, in most entities, not an afterthought or a shortcut. Emerging and nascent sectors—especially those with startups with limited resources—have historically however not applied sufficient resources to these threats.

Legacy

Almost all sectors in an economy are vulnerable to cyber-threats and have acted accordingly. In most cases, the responsible regulator for a sector will mandate sets of rules for effective cyber-security and cyber-resilience. Supervised entities usually have large IT staff and budgets dedicated to the task.

Crypto-Economy

DLTs show great promise in use in DeFi context, from secure disbursement of funds, to secure and transparent access to assets and record; raising of funds using crypto-based tokens; tracing of trade finance payments for small enterprises; to secure identities that can be used to access funds and credit. Especially with a financial component to their use, security of DLTs and the tokens they enable is vital and necessary. However while there do not appear to be major vulnerabilities in the Bitcoin Blockchain and Ethereum internal technologies, the nascent technologies and implementation thereof invariably introduce vulnerabilities. These emanate in particular from the abundance of new protocols that vary the initial design with new features and complex logic to implement them This is exacerbated by the distributed nature of DLTs and the associated wide attack surface and in many cases, and a rush to implement solutions that are not properly tested or are developed by inexperienced developers, and third-party dependencies.

These create an opportunity for design 'bugs' where, although the functionality works as intended, they can be abused by an attacker. These further allow software bugs, which are software errors allow the DLT—possibly a smart contract—enter an insecure state, unintended by the designer or design. Security audits before deployment are critical to the safe functioning of DLTs.

The nascent DLT ecosystem also offers a rich attack source for directly stealing value—as tokens—from 'wallets', often stored in exchanges that use basic security unrelated to the more robust DLT that spawned the tokens. DLTs in the current state of development are also resource-intensive with backend running the DLT needing to be secure end-to-end, including uptime requirements for validation nodes required to implement consensus mechanisms in the chosen DLT design. This creates challenges, especially in developing countries where communications networks may not be robust or fast enough to allow nodes to be available at all times for these purposes. The less nodes, the more a DLT could be subject to a '51%' attack. Similarly, POS and the need for 'stakers' to be online 24/7 exposes their IP addresses and potentially also their online custody of staked assets.[304] And while integration of IoT devices with DLTS show great promise—especially in the agricultural value chain ecosystem—these IoTs acting as DLT oracles are often not secure and create the opportunity for injection of incorrect data in a DLT that could set off a chain of incorrect smart contract 'transactions.'

Stylized Regulatory Approaches

- Policy makers may have a role in DLT deployments in so far they could develop (or even mandate) principles rather than specific technologies or standards that those involved in developing and implementing DLTs need to abide by. Security audits for example could be mandatory, as well as 2FA methodologies if available in a particular environment. As programs running on DLTs, smart contracts may have security vulnerabilities caused by bugs.
- Policy makers could boost their use by creating rules and regulations in these principles—or in separate contract law provisions—that provide clear guidance on how, in case of smart contract-related bugs, to navigate liability trees and on how to assess damages. Similarly, data protection laws or regulations could also protect data on DLTs by adopting best practices for securing and restricting access to data such as using 2FA and restricting access permissions.

7 Regulation of the Crypto-Economy: Select Country Focus Summaries

7.1 Overview

We have selected recent country approaches to regulation of crypto-assets, DLTs and the general crypto-economy, several of which appeared to us to have received lesser coverage. We categorize each of the regulatory approaches in the regulatory classification scheme introduced in Section 6. That is:

- No action
- Forbearance
- Restrictive
- Bring into Scope
- Bespoke
- Hybrid

This section is intended to be a concise summary of regulatory activity related to crypto-assets. Extended summaries for each country with complete citations are placed in Annex C. Note also that the classification terminology used in each country is generally as used by that country and, as such, may not necessarily match with the taxonomy introduced and used in this paper. A study of terminology differences and expositions in terminologies in various jurisdictions can be found in a recent study from Cambridge University.[305]

7.2 Africa

7.2.1 Kenya

Approach: Forbearance.

A Central Bank of Kenya 2015 circular clarified Bitcoin and VCs are not legal tender and warned about related dangers and risks of use. The Capital Markets Authority issued a 2019 warning about ICOs and, specifically, the fraudulent Kenicoin ICO. A taskforce investigating the use of DLTs and artificial intelligence generated an unreleased report to parliament (expected 2019) reportedly recommending implementation of a CBDC and tokenization of the economy.

7.2.2 South Africa

Approach: Forbearance.

The South African Reserve Bank (SARB) stated that they don't regulate or supervise VCs, CCs, VC trading and ICOs and that no specific laws/regulations directly governing such exist. SARB's 2014 Position Paper is its primary guidance document in which it, among other things, provides general warnings about VCs and distinguishes fiat-based e-money from VCs but recognizes them as a payment form. South African Reserve Bank's (SARS) 2018 tax guidance treats CCs as intangible assets. The Intergovernmental Fintech Working Group recommended in January 2019 that: 'crypto' tokens and CAs should not constitute legal tender or e-money; and CA service providers should register with the local FIU and trading platforms registering at a central point, also requiring AML/CFT compliance.

7.3 Asia

7.3.1 China

Approach: Restrictive.

The People's Bank of China (PBC) circulars of 2013 and 2017 declare Bitcoin a virtual commodity and not a currency. ICOs are prohibited. Financial and payment institutions are restricted from conducting Bitcoin transactions. Financial and non-bank payment institutions are prohibited from conducting business related to token financing transactions. The PBC, with agencies and local governments, are reportedly engaged in discouraging Bitcoin mining (such as resource/electricity pricing increases.) The Cyberspace Administration of China's 'Blockchain Rule' requires websites and/or app operators using blockchain technology to register within ten working days of service provision or face fines and criminal sanctions.

7.3.2 India

Approach: Restrictive.

The Reserve Bank of India's (RBI) mandate does not include direct regulation of CAs, only indirectly in its supervision of the industry and assessment of exposure of financial institutions. VCs are not currency or legal tender. The RBI issued 2013 and 2017 warnings of the dangers and risks of ICOs and decentralized VCs. The RBI 2018 circular prohibits regulated entities from dealing with VCs and from providing services anyone dealing with or settling VCs. Several petitions challenged the 2018 circular, seeking to declare it unconstitutional, with the Supreme Court of India poised to issue a decision in July while giving the RBI a prior opportunity to issue VC/CC regulation. RBI's 2019 draft framework for its regulatory sandbox explicitly omits certain CC, CA, and ICO related products and services from eligibility. An Inter-Disciplinary Committee is expected to deliver its report on VC regulatory recommendations in 2019.

7.3.3 Pakistan

Approach: Restrictive.

The FATF placed Pakistan on its 'grey list' in 2018 due to weak AML/CFT regulation and compliance. The State Bank of Pakistan's (SBP) 2018 circular declared VCs and ICO tokens as not constituting legal tender. Banks, payment system operators and payment service providers were generally prohibited from dealing with VCs and ICO tokens. The SBP issued its Electronic Money Institutions (EMI) regulation which license non-banks to provide 'innovative payment services to the general public', which comprises of part of a plan to monitor and regulate VCs and further effective AML/CFT measures. EMIs must meet specific capital and KYC compliance such as collection of customer information and detailed transaction reporting. The SBP announced in 2019 its intention to implement its own digital currency by 2025.

7.3.4 Thailand

Approach: Bespoke.

Two Royal Decrees (adopted May 2019) regulate: (i) offerings of digital tokens and the operation of Digital Asset Businesses (DABs) such as brokers/dealers, exchanges under the Thai SEC remit; and (ii) taxation of profits of DABs, which is regulated by the Revenue Department. 'Digital Assets' consist of CCs and Digital Tokens and determine Token holder rights such as in investments (securities) or receipt of products/services (utilities.) DAB approved CCs in Thailand include the Thai baht, Bitcoin Core (BTC), Ether (ETH), Ripple XRP (XRP) and Stellar (XLM). Offering of Digital Tokens (ICOs and STOs) is regulated under the Decree. In 2018, the Finance Minister announced the Thai SEC should regulate CCs (and not the Bank of Thailand (BOT)) since CCs are not legal tender. Concurrently, the BOT circular of 2018 had restricted CC transactions, and explicitly banks, until regulation could be established. Digital Assets are treated as intangible assets. In 2019, the Thai SEC granted four DAB licenses and approved its first ICO portal.

7.3.5 Vietnam

Approach: Restrictive

A State Bank of Vietnam (SBV) 2014 notice provided general warnings about Bitcoin and VCs, identifying them as unapproved payment forms. Credit institutions were prohibited from trading Bitcoin and use as money or a form of payment with clients. The ban was expanded in 2017 to payment instruments, with non-cash payment forms not approved by the SBV deemed illegal and subject to civil and criminal sanctions. Notable ICO frauds in 2018 (Pincoin and Ifan) led to the State Securities Commission (SSC) directing securities businesses to refrain from several CC related activities and prohibiting investment funds and public, securities and fund management companies from securities issuance, transaction and brokerage activities related to CCs. The SBV and the Ministry of Industry and Trade banned crypto mining hardware imports, such as ASICs. The SBV announced it will create a fintech regulatory sandbox considering CC innovation. A 2017 court ruled local law doesn't consider Bitcoin an asset, which meant it was thus not under the tax authority's remit and gains not taxable.

7.4 Europe

7.4.1 Italy

Approach: Forbearance.

VCs are not legal tender although used locally for payments. VC service providers must file with the currency exchange register. In 2015, BdI issued several general warnings concerning VCs, declaring existing law didn't require AML/CFT compliance for VC exchanges, discouraging VC use until an appropriate framework was established. The 2019 Simplification Decree affords smart contracts equivalent legal recognition and enforceability as written contracts if essential terms are provided (electronic identification of the parties and information stored with a legally acceptable time stamp.) In 2016, the ADE stated that Bitcoin transactions by 'economic operators' are VAT exempt and being treated as foreign currency although VCs are taxable as speculative investments.

7.4.2 Liechtenstein

Approach: Bespoke.

The Token and Trustworthy Technology Service Provider Act; TVTG (the 'Blockchain Act') of May 2019 introduces a regulatory framework establishing a fully tokenized ecosystem and regulation of applications such as CCs, ICOs and CAs. The FMA provides 'Fact Sheet' guidance applicable to crowdfunding, ICOs and VCs. Tokens constituting 'financial instruments' are subject to FMA licensing, rules and any AML/KYC obligations. Creation/use of VCs may require licensing and CC exchanges are also subject to existing law. Determination whether financial and securities law may apply to a token offering is dependent upon the rights attached to the token. All business models evaluated on a case-by-case basis by the FMA, whose website invites innovators to prior discuss their intentions with the authority to obtain insight into licensing and requirements. VCs are not legal tender but can be exchanged for and used in the same functional manner as legal tender.

7.5 Latin America

7.5.1 Brazil

Approach: Forbearance.

VCs are not legal tender nor a currency and differentiated from fiat-based 'e-money.' A 2017 Brazilian Securities and Exchange Commission (CVM) circular prohibited offerings of VAs qualifying as securities through ICOs and VC exchanges and providing general warnings about ICOs. While the Department of Federal Revenue (RFB) treats virtual currencies as financial assets (generating tax reporting requirements), the CVM does not (prohibiting investment funds from direct acquisition.) An RFB May 2019 Instruction requires 'Digital Currency Exchangers' to send detailed monthly operational reports for transactions, including party identification. A 2019 government request was made to establish a special commission to study crypto-currency regulation, including reviewing draft Bill No. 2,303/2015 which regulates VCs/CCs along with 2,060/2019 which separates decentralized CCs (Bitcoin) from centralized VCs (air miles.)

7.5.2 Mexico

Approach: Bespoke.

The Law to Regulate Financial Technology Institutions (Fintech Law), adopted in 2018, establishes a regulatory framework governing the organization, operation and activities of 'Financial Technology Institutions' (ITFs). ITFs, which may be authorized to engage in VA related activities, including crowdfunding and Electronic Payments Funds Institutions (CC exchanges, e-wallets, PSPs.) Supplemental secondary provisions are being issued by relevant authorities (Bank of Mexico (BdeM), National Banking and Securities Commission (CNBV), etc.) establishing characteristics of VAs, eligibility criteria for and approval of ITFs along with boundaries of permissible operation. A regulatory sandbox is to be established for financial sector innovators. Prior to Fintech Law, the BdeM issued warnings about the risks and dangers of VAs, noting that they are not legal tender nor treated as foreign currency and should be treated as a commodity.

7.6 North America

7.6.1 Canada

Approach: Hybrid.

CCs are permitted but are not legal tender. Tax rules apply to all DC transactions and treated as commodities for income tax purposes. Goods or services exchanged for DCs are treated as barter. A 2014 AML/CFT amendment treating those dealing in crypto-currencies as a money service business (requiring registration and compliance with Financial Transactions and Reports Analysis Centre (FINTRAC), Canada's FIU) is still not yet in force. Canadian Securities Administrators (CSA) Staff Notice 46-307 (2017) and 46-308 (2018) constitute primary regulatory guidance on classification of tokens, such as whether an offering is considered a security and subject to securities law. The four prong *Pacific Coast Coin Exchange* test should be used as guidance towards making a determination as to whether any coin/token offering constitutes an offering of securities. There have been ten crypto-asset decisions authorizing entry into the CSA regulatory sandbox.

7.6.2 United States of America

Approach: Hybrid.

The US has a split regulatory regime for financial services: the federal government and each of the 50 states. There is no consensus of approach towards regulating CAs on federal and state levels. Limited federal action has led to some states zealously taking restrictive and friendly approaches. Financial Crimes Enforcement Network (FINCEN) guidance declares VCs as not constituting legal tender in any jurisdiction and VC exchanges are subject to registration, due diligence and reporting requirements under the US Bank Secrecy Act. The Internal Revenue Service (IRS) defines and considers VCs as property, not currency, declaring mining income taxable. The US SEC prosecuted at least a dozen ICO and CA related cases in 2018 and issued guidance in an April 2019 framework, which aids in identifying utility token characteristics which would not consider them to be investment contracts and subject to securities laws. To make such a determination, the *Howey* test is used along with a holistic substance over form analysis which governs classification. DAs which are 'consumptive' are less likely to be considered securities but not if marketed with profit/speculative messaging. The US SEC issued its first 'letter of no action' in April 2019 for an ICO selling utility tokens for flight service. Several states have enacted token laws governing state securities similar to the US SEC. States vary on how to treat transmission of VCs and whether such activities should trigger requirements related to money service businesses.

8 Conclusions

The goal of this paper has been to describe in some detail the technical components of emerging distributed ledger technologies, their strengths and weaknesses; their potential business application and risks in the area of what are termed crypto-assets used in a nascent crypto-economy; the open legal, regulatory and policy dilemma this all presents to regulators, authorities and lawmakers; as well as to provide some suggested strategies, approaches, and solutions.

The issues are complex and potentially disruptive, but as a challenge, are not unlike those that were faced with the emergence of the commercial Internet in the early 1990s as well as the development of digital financial services in the 2000s.

We now know that Bitcoin and its underlying technology 'blockchain' represented the transformational vanguard of a new method of sharing data and processes and contracting in a decentralized, traceable and secure manner and, in many cases, without the need for using intermediaries. The family of blockchains and its analogues are now known as distributed ledger technologies (DLTs).

Whatever their form, DLT-derived and focused products and services are here to stay, with billions of dollars being invested by venture capitalists, banks and even regulators. DLT offers the tantalizing potential of making data transfer and storage more efficient, reliable and transparent, with a decentralized motif that removes or reduces the need for often costly centralized intermediaries.

The main DLT flavors that have emerged are public or private DLTs, with access to the DLT being permissioned or permissionless. Bank-type DLTs, for example, are private and permissioned, reflecting the provenance and type of data they incorporate. The Bitcoin DLT is public and permissionless. There are hybrid iterations, with some privacy components called zero-knowledge proofs being built atop even the open public, permissionless DLTs.

The DLT system though is relatively new and immature, with the first iteration—the Bitcoin 'blockchain'—only first appearing in 2009.

Some clear trends are evident though, which we submit will inform regulatory responses, either reactive or proactive in nature.

Overall, there is a bifurcation of interest in DLTs, between retail and enterprise. First, enterprise and consortium blockchains are being developed by sector consortia of banks, or shipping companies, or food supply networks. Billions of dollars are being invested in development and prototypes and trials of the underlying technologies, as well as in the commercial applications in the financial sector. Most of the patents in DLTs belong to brand name financial groups. Their focus though is on the utilitarian features of DLTs, presenting a potential of secure, transparent, tamper evident, decentralized data storage and automated contracts. The DLT features are being used to improve settlement times, supply chains, or trade finance. While many trials are promising, there are as yet however few successful major live commercial implementations of the technology itself and its applications. The primary regulatory momentum, glacial at best, in this area is to *proactively* provide a pathway to ubiquitous use of DLTs in the economy through a modicum of legacy certainty, for example by affording functional equivalence to DLTs in relation to current technologies used in commerce.

The enterprise side also has some activities on crypto-currency futures and ETFs. With a nod to the movement towards tokenization of assets, but with an eye sideways to regulatory uncertainty, and given the issues around the underlying provenance of some of many of the emergent crypto-assets, only a light-touch interest in tokenization of assets through STOs.

Comparatively, on the retail side, the momentum is towards trading and development of new asset classes such as ICOs, UTs, and STs, and CCs. Here the concomitant regulatory momentum is mostly reactive, especially in relation to embracing of ICOs and CC trading by individual investors. Some proactive regulatory activity in some jurisdictions has been to develop bespoke crypto-asset regulatory frameworks that recognize and regulate these classes. There is some measure of forbearance in some jurisdictions.

While many enterprises are developing consortia DLTs within the confines of their specific design goals, for many public DLTs the underlying technologies—known now as 'Layer 1' technology—in use are open source, enhanced primarily through the 'wisdom of the crowd' and unidentified coders. Despite this decentralized and often chaotic development process, there have been some remarkable improvements in reliability, adaptability, security, scalability and speed of DLTs from technology generation to generation. Ethereum, launched in 2014, is the most popular of the public DLTs, using its native programmatic component called ERC-20 to launch a number of innovative decentralized applications generally called decentralized applications, or dApps. So-called smart contracts represent the business end of DLTs dApps, automating manual process in what the maximalists understand to be 'code as law.'

The caveat though is that these parallel developments have resulted in the balkanization of the 'Layer 1' enabling technologies and platforms, including the dApps and PTs only being usable on one type of DLT. Each DLT class then is an island of excellence. This trend we see as being likely to continue for a number of years until, at least, some measure of reliable and secure interoperability between DLTs is ensured through, as yet, mainstream innovation. This lack of interoperability and standardization introduces elements of inconsistency in use, which may affect the longevity of storing data on a DLT, with resultant security, privacy and compliance implications.

This shows there is a bright line trend between the utilitarian end-use of DLTs in enterprises and its overall business potential, the latter more so at the retail level.

The leading edge of these retail components are the malleable 'crypto tokens'—a type of 'programmable money'—generated by and native to each type of DLT. Tokens generated through the ERC-20 process on Ethereum are particularly popular. Seen through the prism of financial services, these tokens may form the backbone of a nascent 'crypto-economy' as we dub it, forming new verticals, notably the production and use through tokenization of novel 'crypto-assets' that offer the transformative potential of democratization of access to financial products.

This democratization includes enabling, for the first time, fractional ownership of legacy and new crypto-inspired asset classes of any (legal) asset class by anyone with access to the technology. This offers the potential of a transformational change in societal behavior not seen since the dawn of the commercial web-based Internet in the 1990s and its later mobile analogue.

Concomitant with the new asset classes is the emergence of new actors that provision these enabling technologies and crypto-assets. Emblematic of their 'maximalist'—anti-central control—ethos, many of these new actors, though, covet an entrepreneurial spirit rather than a fealty to current regulatory norms. Many of the first capital-raising initial coin offerings (ICOs) of 2017-2018 by fintechs were, for example, legally dubious and attracted regulatory opprobrium. The impact thereof has been that public confidence in the new asset class has waned, evidenced by the lack of liquidity in these new asset classes and a 'crypto-winter' of 2018 where crypto-asset prices largely collapsed. This sobering reality, however, catalyzed the emergence of new crypto-asset classes, such as STOs, to provide a 'fresh' (and less legally dubious) start.

While these asset types, new actors and the crypto-economy generally currently represent a small fraction in size and activity compared to the 'legacy' economy. In the long run we could experience the gradual disappearance or waning role of current 'legacy' actors—such as broker-dealers and centralized exchanges—in the financial ecosystem. DLT may be to these legacy actors what the digital camera was to the eponymous Kodak.

While these technologies, products, services and even the participants and actors providing services are novel and offer the prospect of a fundamental change in business practices and access to financial products, they notably test the perimeters of current sets of laws, regulations, principles and norms as well as the remits and capacity of financial and associated regulators and authorities.

This is particularly so with the emergence, currently glacial though, of institutional investors in portions of the crypto-economy. While the crypto-economy as measured in capitalization does not as yet pose any systemic concerns for any national economies, the emergence of institutional investors may alter that calculus. Regulators need to be vigilant and prepared for this.

There are, however, many open (and evolving) legal and regulatory issues that still need to be addressed in their totality. These regulatory foci can be classed first as bringing certainty to role of the underlying enabling technologies, and secondly the nature, role and compliance requirements of the actors providing services in the crypto-economy and products/services used atop its enabling technology.

These include as enumerated earlier *inter alia* issues of legal and contractual certainty in the use of so-called smart contracts, the nature of legal custody of crypto-assets in the age of the possession of private keys; the safety and soundness of exchanges facilitating fiat-crypto and crypto-crypto trading; whether some crypto-assets can be classed as securities; security of the

DLT technologies and implications for record-keeping, data protection and privacy; and the role of new actors such as miners and validators in the crypto-economy.

This growing list of open regulatory issues suggests that to catalyze and embrace DLT for mainstream commercial and public use as a nascent crypto-economy, both doctrinal and legislative shifts are required. This to bring certainty to the innovation at minimum, and interventions where there are certain harms. In the face of dealing with the particular type of technological innovation with its omnibus but seeming effects on many sectors and verticals, the regulator and lawmaker's usual 'toolkit' of applying functional and/or principles-based regulation may be sorely tested and will need to be calibrated.

While the issues tend to be disruptive and challenging to dovetail into current regulatory norms, regulators may suffer from inertia, either because of capacity to develop new policy around new asset classes, or public policy issues based on regulatory arbitrage, or even regulatory capture. In the case of the crypto-economy, it is more likely that the capacity and arbitrage issues prevail.

The study categorized the potential regulatory responses as the following: no action; regulatory forbearance; restrictive; bring into scope of existing legal and regulatory frameworks; a new bespoke crypto-asset regulatory framework; or a hybrid approach that uses any of these types depending on the type of actors and product/services. Of the approaches, a hybrid approach of some sort may be necessary to bring into scope elements of the crypto-economy, alongside a new crypto-asset regulatory framework that addresses the new crypto-assets and enabling actors. A novel model crypto-asset regulatory framework is presented in Annex D and, by its omnibus nature, we recognize it may not always be practical in jurisdictions like the US with its fragmented regulatory structure.

In summary, we categorize the open issues relating to crypto-economy-related risks and regulatory in the planes below, outlining potential strategies, methodologies, and approaches by regulators, authorities and policy makers. These issues and strategies are not confined to financial regulators and financial matters though. They also involve, *inter alia*, issues of contractual formation; use and weight of evidence; data protection and privacy.

Regulatory Strategies

Scoping

- **Create A Taxonomy of DLTs and Crypto-Assets**
  As was done in this paper, a taxonomy of all technologies, hierarchies, actors and products and services should be undertaken to understand, at a macro and micro level, the many moving parts and trends in the 'crypto-economy.' Comparisons to and superimposition over legacy systems should be undertaken to understand any changes, gaps and similarities. A systematic approach should be used, possibly using a standard set of definitions from standard setting bodies—or this paper. This process will probably involve cooperation between multiple regulators. There must be awareness though of the innately fluid nature of crypto-assets as they are currently classified. That is, what may be decentralized at one instant, may be centralized in another or what is a utility token at one moment may be an ICO in another.
- **Create A Taxonomy of DLT and Crypto-assets Risks Per Sector Actor**
  The challenge for regulators is to understand the range of crypto-assets, their often hybrid nature in linking not only to 'real world assets' but to other native crypto-assets, of which not all raise the same risks and regulatory and oversight issues. As was done in this paper, a taxonomy of all technologies and associated risks should be undertaken. Comparisons and superimposition over legacy systems should be undertaken to understand any changes, gaps and similarities. A systematic approach should be used, possibly using a standard set of definitions from standard setting bodies—or this paper. This will probably involve cooperation between multiple regulators.

Collegiality

- **Conduct Colloquiums with Industry Actors**
  As the multifaceted technical, legal and regulatory scope of this paper demonstrates, the emerging DLT and crypto-economy is complex with lots of moving parts. Regulators should initiate outreach to supervised entities and any other entity and experts that can contribute to an understanding of new technologies, trends, risks, challenges in implementation of existing regulations and general wish lists. These can and should be ventilated in colloquiums between these interested parties.
- **Undertake Regulatory Impact Assessments**
  Good regulatory practice before releasing final rules is to undertake regulatory impact assessments. This is especially needed in the omnibus regulation of elements of the crypto-economy. Each regulator—or clusters of regulators in a specific sector, say financial—should produce or contribute to such an assessment.
- **The Government Should Create a DLT Working Group**
  As has been done in some countries and US states, government should create a working group to investigate the trends, actors, risks, usability, utility, challenges and impact of DLTs, and by extension, the nature of the crypto-economy.
- **To Avoid Arbitrage, Devise MOUs Between Regulators**
  Where their enabling law allows this, regulators should closely interact with other regulators who may have overlapping remits so as to prevent regulatory arbitrage. This may take the form of a memorandum of understanding to carve out, as needed, remits. The novel digital financial services ecosystem[306] in use, especially in developing countries, and the arbitrage it initially precipitated between financial and telecommunications regulations and regulators is a contemporaneous and useful model for this close interaction.
- **Introduce Regulatory Sandboxes**
  Some countries have introduced what are known as 'regulatory sandboxes' that provide a light-touch regulatory space for fintech to test their innovations. Most sandboxes include fintechs developing DLT-based solutions.

Efficiency

- **Investigate Use of DLT for Regulatory and Supervisory Activities**
  Although not in the scope of this paper we suggest that, beyond creating the necessary regulatory frameworks to consider DLTs and other innovative technology/processes, regulators investigate DLTs for their utilitarian purposes

in so far as embracing their manifestly positive attributes—not just for an evolving commercial industry but also for internal use, *inter alia*, as regulatory technology (regtech) solutions and central bank digital currencies/digital fiat currencies.

Guiding Principles in Strategizing

- **One Size Fits All is not a Practical Regulatory Strategy**
  For efficient regulation and to avoid regulatory arbitrage, regulators need to understand where they have remit and the concomitant regulatory touch points. In particular, what parts, if any, of the entire life cycle of a crypto asset may need oversight, be it from one or more regulators. Some asset classes may, natively, be of a type that has multiple regulators involved. The life cycle may mean the development of the underlying Layer 1 code, protocol development and any downstream alterations, then the issuance of token containing the assets, their distribution, custody, trading and clearing and settlement.

  Of course, the DeFi ecosystem may remove, by design or by natural conflation, some of these parameters/actors (for example the custody and clearing and netting actors). Similarly, anonymity may confound application of the rules, particularly in public blockchains, although permissioned blockchains may provide more proximate touch-points as the parties may be identifiable. Similarly, the new actors in the DeFi ecosystem—particularly the miners—may provide additional touch points. Even so there may be gaps.[307] In that context, omnibus restrictions or 'one size fits all' approaches may stifle innovation. Of the potential responses, new bespoke crypto-asset frameworks may provide the most functional and purposive approach but requires regulatory interaction with the private sector to create an accurate functional taxonomy.
- **DLTs Introduce A Perimeter to Regulatory Forbearance**
  As the technology and business models evolve, often but not always, regulatory forbearance may be the best or appropriate policy. Nor is it always the clear (and only) choice: regulatory—particularly financial regulators - informational asymmetry is not purposive when faced with rapidly emerging technology like DLTs that can impact all sectors of an economy. Regulators also have symmetrical challenges in so far as they may not wish to give too much guidance, lest they later be boxed into a policy rapidly made redundant, contradictory and thus ineffective by changes in technologies.
- **DLTs Introduce A perimeter to Principles-based Regulation**

Data Privacy

Often strict applications of principles (frequently based on ambiguous definitions in rules) have unintended consequences. The effective nullifying of general application of the first EU's e-money directive based on a faulty definition is a case in point, Similarly, the EUs data protection and privacy regulation implemented in 2018 codifying the principle of 'data subjects' (individuals) being able to simply command the removal of their personal data from 'data controller' systems hit headwinds in the face of DLTs, which by design cannot delete data. At best they can *hide* data. This distinction has tested the application of the principle in a number of countries. The larger point is that any regulation needs to be seen with the prism of whether it can be ubiquitously applied to DLT, which as noted above, are here to stay.

Payment Finality

The nature of payment finality—the bedrock of financial systems worldwide—may need to be revisited in so far as 'irrevocability' must be refined. Here concepts of the nature of a payment around payment finality are at play. In the DLT world, the payment finality issue is conjoined with the payment delay issue. Equivocation in a determination of finality and irrevocability may be created where there is a fork where, what was apparently irrevocable, ultimately turned out not to be. This was the case in the 'The DAO' attack, that being payment finality and irrevocability.

Governance and Responsibility

As noted above, anonymity and decentralization as a by-design feature of DLTs may confound application of rules of governance and liability in financial systems. This is particularly in quixotic public blockchains, such as Bitcoin core, although permissioned blockchains may provide more proximate touch-points as the parties may be identifiable Nonetheless, decentralization is a fluid concept and like the grabbing of the proverbial slippery eel, may allow actors to slip in and out of regulatory and even civil liability depending on any time in point. Fluidity easily enabled or caused by technology is one cause. For example, a product or service classified as an ICO may morph into a UT simply by changes in the use of its programmable token by the participants, the difference between a pre-functional token sale and that of a functional token. Or a platform seemingly decentralized—and regulated as such—at one time point may become centralized simply through the ebbs and flows of the number of nodes participating in that DLT. How to apply a qualitative and quantitative measure to this and classify other actors and circumstances is woven into the tapestry of the regulator's dilemma.

Legal and Regulatory Certainty

- **Improve Legal and Regulatory Certainty in Use of DLTs and dApps**
  There a tension between innovation and regulation, with a public policy distinction needed to pass laws and regulations simply to bring regulatory force and certainty to an evolving sector that (potentially) restricts its development and which may define the boundaries of the applications that could be used. A sample of the legal issues that would appear to be most pertinent to DLTs include the legality and enforceability of smart contracts; evidential weight of DLT-derived data; property rights in crypto-assets; time and place of contracting using a blockchain and smart contracts; the 'chain' of legal liabilities in the sector; competition issues in a decentralized environment; criminal use and liability; and which court may have jurisdiction over a matter involving DLTs and their applications in a 'distributed' multi-national nodes environment.

- **Functional equivalence:** Laws and regulations could be changed to apply functional equivalence to use of DLs in everyday commerce provided that a DL meets certain requirements. These requirements should be specified. This would put smart contracts and blockchain records and signatures on equal footing with written contracts, subject to express limitations on blockchain records in case:
  - The blockchain record is not in a form for retention and later accurate reproduction
  - The law requires that the record to be posted or displayed by a specific method
  - Access to store or retrieve information to or from the blockchain is limited by a party
  - Of a notice required with respect to certain cancellations or defaults

Similarly, legislation could be provided that smart contracts may not be denied legal effect, validity or enforceability because they contain smart contract terms or are in the form of code. For the same effect, laws could be amended to recognize that signatures, records and contracts secured by a party through DL technology should be deemed to constitute an electronic signature and electronic record. These may be given effect based upon the context and surrounding circumstances of electronic signature or record.

- **Laws of evidence:** Coincident with these changes, existing laws of evidence could be tested to indicate whether courts may accept DL-based evidence and also what weight should be afforded to this evidence. In particular, it should be determined, whether in some or all cases, a record on a DL serves as the equivalent of a notarization of the data and, if so, who or what would be the notary equivalent. If needed, laws could be amended to ensure that a smart contract, record or signature created, stored or verified on a blockchain may be enforceable or given legal effect, and may be admitted as evidence, with the weight of that evidence to be deduced from surrounding circumstances.

- **Clarify, if Needed, Nature of Fiduciary Responsibility:** Another related issue is the role of 'miners' and how they would be handled under the existing rules given their novel and fundamental role in the settlement process.[308] This, however, touches on controversial issues of holding coders and developers liable as 'fiduciaries for transactions they help settle for reward.[309] While these could conceivably be achieved under existing regulations relating to technical services providers providing critical services to C&S operators, practically identifying and then fastening any rules on their activities given largely decentralized nature of public blockchain could be regulatory overreach. Some regulators have, however, proposed making coders liable for any breaches of regulatory norms. For example, the Australian securities regulator issued rules in May 2019 that, in effect, makes miners (and transaction processors) automatically and vicariously part of the regulatory regime where their mining activities are part of the C&S process for tokens that are financial products. This is likely to have a chilling effect on incentives for miners to undertake mining activities where any measure of risk (liability) may fasten on them where there was none before. Less mining means the DLT becomes more inefficient and concentrates hashing power to the degree that the DLT may be subject to a '51% attack' described earlier.

A more practical regulatory innovation—and less chilling on the incentives to miners to mine, and innovators to innovate would be that existing rules—with some adjustments to take into account new actors and asset classes—could be fastened on permissioned blockchains only, specifically those federated types in financial verticals such as banking and insurance.

- **Define Nature of Crypto-Assets**
  The attribute of a crypto-asset, generally being native digital bearer instruments, may alter laws of negotiable instruments in so far as this confers super-negotiability on a crypto-asset since it is no longer in the hands of an intermediary such as custodian but fully owned by the owner as its holder of its private keys. The US state of Wyoming has already recognized and codified this shift in ownership and thus negotiability. This should serve as a model for other US and international jurisdictions.
- **Smart Contracts**
  While their utility as automated, deterministic execution of instructions is novel, the code-as-law motif applied by maximalists to smart contracts does not fit into legal norms surrounding contract formation in most legal families. We find that they are not always so smart nor legally sound as an analogue of contracts written in natural language. Legal certainty needs to be fastened on them in some fashion, at least in recognizing that agreements in some form placed on a DLT are the functional equivalent of other electronic forms. Substantively, though, and in according legal effect and weight to the 'code as law,' in the absence of the smart contract being able to assess situations autonomously to determine compliance with the intention of the parties, 'dumb' contracts in natural language should accompany them as a failsafe.
- **Where Possible, A New Crypto-Asset Regulatory Framework is Desirable**
  Where the jurisdiction allows for it and where possible, a new crypto-asset framework for crypto-asset regulation is desirable. Attempts to shoehorn new products, services and asset classes by attempting to bring them into scope of existing laws and regulations may seem appropriate at one time point in technology evolution and for public policy considerations of that time. However, they may quickly become redundant and/or contradictory at another. Policymakers should consider and pursue strategies consistent with that new reality. At the very least, affected regulators should embark on creating a taxonomy of the (crypto) asset classes, as well as any laws and regulations that may be affected by the emergence and use of the technologies. This will prevent the inevitable regulatory arbitrage. Where there are gaps, however, common and civil law may offer some although imperfect solutions. Similarly, to encourage and reflect emerging institutional and enterprise use, a risk-based guidance for financial institutions to assess and adopt new use crypto-assets should be encouraged. Our model crypto-asset regulatory framework is presented again in **Annex D**.

Annex

A. Summary of Country Approaches to DLTs and Crypto-Assets

Proof of Work

The proof of work consensus algorithm used most often for public, permissionless blockchains such as Bitcoin and Ethereum, allows anyone to become a participating transaction processor and validator and who is known as a 'miner.' In general,[310] miners compete in a P2P network compete to find a numeric solution (a 'nonce')[311] to a mathematical question concerning hashing[312] and earn the right to add a block of validated transactions to the blockchain and a reward for an amount of native currency.[313] The energy expenditure by 'miners' to perform the 'work' is substantial and intentional by design.[314] It dis-incentivizes miners from committing bad acts which would undermine a substantial investment in mining hardware, electricity and operational costs.[315] Acquiring sufficient computational or 'hashing power'[316] needed to take majority (51%) control over the network could be prohibitive in a large blockchain system[317] and easily observable by others monitoring the network. The most popular crypto-currencies using POW are Bitcoin Core and its variants, Ethereum (Homestead), Litecoin and Peercoin.[318]

Proof of Stake

Proof of Stake (POS) is designed to be a more energy efficient consensus mechanism which is lower in resource consumption than POW.[319] POS generates consensus using an algorithm that is based upon the ownership of native crypto-currency in relation to others in the system along with some weighting mechanism such as how long the currency has been held by the stakeholder.[320] This may also include a deposit of currency which, collectively, consists of the 'stake' in the system.[321] Some POS variants deal with this issue by requiring an actual stake of currency to be deposited.[322] The ability of a stakeholder to 'forge' or 'mint' a new transaction block to the blockchain is the result of pseudo-random assignment which is based on the size of the stake and the POS algorithm. DLTs using POS include Peercoin,[323] Nxt, Blackcoin, Shadowcoin, Cardano, Novacoin[324] and soon Ethereum's Caspar.[325]

Delegated Proof of Stake

Delegated Proof of Stake (DPOS) is a variation of POS where token holders vote for a certain number of delegates (defined by the consensus protocol and called 'Witnesses,' who are given the authority to validate transactions and blocks. Stakeholders such as coin holders have weighted votes[326] on electing the witnesses who can validate transactions and add blocks to the blockchain. DPoS is currently used by EOS, Bitshare, Steem, Ark, and Lisk.

Practical and Federated Byzantine Fault Tolerance (PBFT)

A consensus algorithm for private (mostly enterprise consortiums) or permissioned DLTs and blockchains which may not have as many participants in its walled garden as compared to openly accessible public, permissionless blockchains.[327] It is suited to enterprise consortiums where members are partially trusted. These are important because malicious attacks and software errors are increasingly common and can cause faulty nodes to exhibit arbitrary behavior (Byzantine faults). Adoption includes Neo,[328] Tendermint, Polkadot, Hyperledger Fabric,[329] and Zilliqua.

Proof of Elapsed Time:

POET is a lottery system used in permissioned blockchain networks to decide the mining rights or the block winners on the network using. Every participant in the network is assigned a random amount of time to wait, and the first participant to finish waiting gets to commit the next block to the blockchain.[330] All nodes are equally likely to be a winner.

B. Stablecoin Varieties

Fiat-Backed Stablecoins

This is the most common form of stablecoin, fully backed by fiat money. Fiat-backed stablecoins are backed 1:1, meaning USD 1 of stablecoins is equivalent to say USD 1 of fiat money. The most prominent is Tether, whose stablecoin is called USDT.[331] JPMorgan has announced a plan for an internal, price-stable crypto-currency called 'JPM Coin.'[332] Facebook too is investigating what is believed to be its own stablecoin, under the name 'Project Libra.'[333]

Commodity-Backed Stablecoins

The Digix Gold Tokens (DGX) is an ERC-20 token backed by physical gold that it says is stored in a vault in Singapore, known as The Safe House, and is fully redeemable at any point of time. The value of each token is fully dependent on the market value of gold.[334]

Crypto-currency-Backed Stablecoins

These are backed by other crypto-currencies, usually the top-ranked crypto-currencies with large market capitalization for better risk distribution. Most common crypto-backed stablecoins require users to stake (and lock-up) a certain amount of crypto-currencies into a smart contract which will then result in the creation of a fixed ratio of stablecoins.[335]

Seigniorage-style Stablecoins

These coins reflect the only category of stablecoins not backed by any asset but use an algorithmically governed approach to expanding and contracting a stablecoin's money supply, just like how a central bank prints or destroys money.[336]

C. Regulatory Approaches in Various Regions

1 Introduction

We have selected recent country approaches to regulation of crypto-assets, DLTs and the general crypto-economy, several of which appeared to us to have received lesser coverage. We categorize each of the regulatory approaches in the regulatory classification scheme introduced in Section 6. That is:

- No action
- Forbearance
- Restrictive
- Bring into Scope
- Bespoke
- Hybrid

Note that the classification terminology used in each country is generally as used by that country and, as such, may not necessarily match with the taxonomy introduced and used in this paper. A study of terminology differences and expositions in terminologies in various jurisdictions can be found in a recent study from Cambridge University.[337]

2 Africa

2.1 Kenya

Overall

Authorities have refrained regulating crypto-assets, watching the industry develop while issuing limited guidance.

Regulators and Authorities

- Central Bank of Kenya (CBK)
- Capital Markets Authority (CMA)

Approaches

- *Forbearance*
- In March 2018, the Kenyan government created a Distributed Ledgers and Artificial Intelligence taskforce to investigate and provide recommendations to parliament on the adoption and use of these technologies in the marketplace.[338] While the taskforce reportedly recommended creation of a CBDC[339] and tokenization of the Kenyan economy,[340] the official report has still not yet been released.[341]

Official Actions on Crypto-Assets and Technology

- The CBK issued a 2015 circular clarifying that Bitcoin and 'virtual currencies' are not legal tender along with general notice of dangers and risks of their use.[342]
- A 2015 court ruling found that crypto-currency represents monetary value and that a mobile network operator (Safaricom) could justifiably shut down services to a remittance services provider who was dealing in Bitcoin and lacked the prior approval of the CBK.[343]
- In 2019 the CMA warned the public about the Kenicoin ICO offered by Wiseman Talent Ventures which was under investigation for fraud.[344]

2.2 South Africa

Overall

The authorities have primarily acted as spectators watching the crypto industry develop. The country's IFWG fintech working group recently published a comprehensive study and recommendations for crypto-asset regulation.

Regulators and Authorities

- South African Reserve Bank (SARB)—central bank
- South African Revenue Service (SARS)—tax authority
- Financial Intelligence Centre (FIC)—financial intelligence unit
- Financial Sector Conduct Authority (FSCA)
- National Treasury (NT)

Approaches

- *Forbearance.* A working group has recently issued recommendations for crypto-asset regulation.

Official Actions on Crypto-Assets and Technology

- As per SARB, there are presently no specific laws or regulations which directly govern the use/trading of virtual and crypto-currencies in South Africa.[345] Accordingly, SARB does not presently supervise or regulate such currencies nor related activities such as ICOs and trading.[346]
- SARB's perspective and treatment of decentralized virtual currencies (such as Bitcoin) is still consistent with its 2014 Position Paper[347] in that virtual currencies are distinguishable from e-money (electronically stored monetary value, typically fiat currency, which can be used to make payments.) While virtual currencies can possess similar attributes to e-money,[348] they are not considered legal tender and may be refused or accepted at the recipient's discretion as a means of payment.[349]
- While the Position Paper warns about dangers and risks of virtual currencies, SARB experimented with crypto-currencies using DLT as an interbank payments and settlement system 'Project Khoka' sandbox.[350]

Taxation

- SARS published tax guidance in April 2018 which establishes that crypto-currencies should be treated as intangible assets.[351] Generally, income tax rules are to be applied in a similar fashion to crypto-currencies.

Policy Recommendations for Regulation

- South Africa's Intergovernmental Fintech Working Group (IFWG)[352] published the results of its crypto-currencies and crypto-asset regulation workshop in April 2018[353] and subsequent consultation paper on policy proposals and recommendations in January 2019.[354] The group recommended:
    - Updating naming conventions from 'digital tokens or assets' and 'virtual currency' to 'crypto tokens' and 'crypto assets' for definitional clarity and proposed a definition of crypto assets;[355]
    - An intention to regulate rather than ban the use of crypto assets which is based upon the landscape, levels of adoption and market conditions;
    - Crypto assets should remain as not being recognized as legal tender or electronic money;
    - Registration of crypto asset service providers with the Financial Intelligence Centre (its FIU) with legal obligations to comply with AML/CFT requirements, including crypto asset trading platforms, digital wallet providers, safe custody service providers, payment service providers;
    - Registration at a central point should be required for crypto asset trading platforms and vending machine owners/providers, digital wallet providers, safe custody service providers, payment service providers and merchants and service providers who accept crypto asset payments;
    - The SARB should publish a detailed registration process in a policy paper in 2019.

3 Asia

3.1 China

Overall

While China appears to be investing in DLT, regulatory action has stifled activities relating to decentralized crypto-assets. The central bank banned ICOs outright and substantially discourages Bitcoin mining. It is also investigating the establishment of its own CBDC.

Regulators and Authorities

- People's Bank of China (PBC)—central bank and primary regulator of crypto-currencies
- China Securities Regulatory Commission (CSRC)—securities and capital markets regulator
- Cyberspace Administration of China (CAC), regulator/monitor of crypto-assets of online
- Several other acting authorities also supervise related activities[356]

Approach

- *Restrictive.* Significant bans on crypto-currencies and ICOs exist and measures have been taken to discourage growth of decentralized crypto-assets. Attention appears to be placed on establishing a CBDC.

Official Actions on Crypto-Assets and Technology

Crypto currencies and ICOs

- A 2013 PBC circular[357] along with a 2017 update[358] issued collectively with several other regulators[359] represent China's two primary regulations impacting crypto-assets. Bitcoin is explicitly treated as a virtual commodity, not as a currency and should not be used as a currency.[360] Furthermore, financial institutions and payment institutions are restricted from conducting Bitcoin transactions.
- The 2017 circular also prohibited individuals and companies from engaging in ICOs and token financing trading platforms exchanging legal tender and virtual currencies or tokens. Financial institutions and non-bank payment institutions are prohibited from conducting business related to token financing transactions.
- The PBC reiterated its ban in a 2018 circular stating that ICOs constituted unauthorized illegal public financing.[361] Subsequently, WeChat (an instant messenger service) effectuated a ban on large and influential public accounts which had been influential in the promotion of ICOs and crypto-currency trading under the guise of an unspecified violation of instant messaging services laws.[362] The following year WeChat banned merchants from accepting crypto payments.[363]
- While the use of decentralized crypto-currencies and tokens are being vanquished, the governor of the PBC announced in March 2018 that they were developing a central bank digital currency (CBDC) called the 'Digital Currency for Electronic Payment' (DCEP) based upon DLT or blockchain technology.[364]

Mining Activities

- While not banning mining activities outright, the PRC has made overtures to discourage them. In 2018, the Office of the Special Rectification Work Leadership Team for Internet Financial Risks was reported to have issued letters to local governments requesting their assistance with discouraging Bitcoin mining (through resource rate and price increases such as for electricity and rental property.)[365] In April 2019, the National Development and Reform Commission released a paper for public comment on industries marked for elimination which includes crypto-currency mining (emphasizing Bitcoin which is often deemed resource inefficient with its high level of electricity consumption.)[366]

DLT/Blockchain General Use

- In 2019 the CAC published its 'Regulation for Managing Blockchain Information Services' known as the 'Blockchain Rule'. It requires those operating a 'blockchain information service' (such as using websites and/or apps 'based on blockchain technology or systems') to register their business within ten working days of service provision or face fines and potential criminal sanctions.[367]

3.2 India

Overall

A cautious approach has been undertaken, with the central bank restricting the banking and financial services industry from engaging in certain activities relating to crypto-assets. Legal adjudication and a committee report may prompt authorities to imminently take a clearer position and the release of potential crypto-asset regulation.

Regulators and Authorities

- Reserve Bank of India (RBI)—central bank. The RBI does not have a legal mandate to directly regulate crypto-assets but it may assess the exposure of financial institutions under its remit to crypto-assets and supervise their operations.[368]

Approaches

- *Restrictive*—a banking and financial services sector ban exists on dealing with virtual currencies.
- In April 2017, the Department of Economic Affairs, Ministry of Finance announced the formation of an Inter-Disciplinary Committee to determine the local and global status of virtual currencies; examine local and international regulations and frameworks; and provide recommendations on dealing with virtual currencies in all respects (including consumer protection, AML/CFT measures, etc.); and any other relevant matter.[369] It has been reported that the Committee is poised to deliver in a final report in 2019.[370]

Official Actions on Crypto-Assets and Technology

- India does not consider crypto-currency to be currency or legal tender.[371] While it has not been formally banned outright for all, its use has been substantially restricted in the banking and financial services sector. The RBI issued several warnings (once in 2013 and twice in 2017) on the dangers and risks of ICOs and generally the use of decentralized 'virtual currency.'[372] The 2017 notices explicitly referenced Bitcoin, Litecoin, bbqcoin, dogecoin and altcoins and all entities engaged in related activities as not having received any license or authorization to operate.
- In June 2017, a public interest litigation petition was filed to declare crypto-currencies and decentralized digital currencies illegal, seeking to ban all such purchases and acquisitions.[373] Shortly after the aforementioned RBI's second crypto-currency warning in December 2017, India's Finance Minister stated in his Union Budget Speech that the country 'will take all measures to eliminate the use of these crypto-assets in financing illegitimate activities or as part of the payment system.'[374]
- An RBI April 2018 circular prohibited entities under its purview from dealing in 'virtual currencies'[375] or providing services for 'facilitating any person or entity in dealing with or settling virtual currencies.' The impact on crypto-currency related activities, such as exchanges, prompted several additional legal challenges.[376] In August 2018, a petition was filed by four cryptocurrency exchanges[377] seeking to declare the 2018 RBI Circular unconstitutional.[378] These cases were consolidated and reached the Supreme Court of India in February 2019. The Court presented the government an ultimatum to issue regulations or face a July decision by the Court on whether to place a stay on the 2018 RBI circular.[379]

Technology

- The Indian government has been exploring the use of blockchain technology in the evolution of the country's digital economy.[380] The RBI released a 2017 white paper[381] exploring the use of DLT for a national payments system platform including a Central Bank Digital Currency (CBDC).
- The RBI draft framework for its regulatory sandbox, released in April 2019, explicitly excludes certain crypto-currency, crypto asset and ICO related products and services from eligibility.[382]

3.3 Pakistan

Overall

After a cryptocurrency ban in the banking and financial sector was implemented (concurrent with international concerns regarding deficiencies in its AML/CFT efforts), the government recently adopted 'digital currency' regulations intended to cover crypto-currency while also addressing stronger AML/CFT regulation.

Regulators and Authorities

- State Bank of Pakistan (SBP)—central bank

Approaches

- *Restrictive*—a financial sector ban followed by recently adopted 'digital currency' regulations.
- In June 2018, Pakistan was officially placed on the Financial Action Task Force (FATF)[383] 'grey list' due to findings of unacceptable progress in taking adequate AML/CFT measures.[384] While the country has been challenged to meet 2019 deadlines,[385] it recently released e-money

regulations to address money laundering and financing of terrorism concerns which contain significant KYC and reporting provisions.[386]

Official Actions on Crypto-Assets and Technology

- In an April 2018 circular the SBP declared[387] that 'virtual currencies'[388] and ICO tokens were not legal tender and related activities would be curtailed. Banks, payment system operators and payment service providers were prohibited from holding, transacting, investing, promoting and otherwise dealing with crypto-currencies and ICO tokens, both for activities on its own behalf and from facilitating customers.[389]
- In April 2019, the SBP issued regulations for licensing 'Electronic Money Institutions' (EMIs),[390] non-banking entities providing 'innovative payment services to the general public.' The regulations are intended to monitor and regulate digital currency,[391] including crypto-currency,[392] and combat money laundering and financing of terrorism. Under the regulation, licensed EMIs are required to meet specific capital requirements, threshold levels of customer due diligence such as collection of customer information.[393]
- The deputy governor of the central bank announced in April 2019 that the SBP intends to issue its own digital currency by 2025 to promote financial inclusion, increase efficiency and combat money laundering and terrorism financing.[394]

3.4 Thailand

Overall

Prior to its current crypto-friendly regulatory approach, Thailand instituted two periods of Bitcoin and crypto-currency trading restriction in 2013 and 2018.[395] Thailand implemented formal crypto asset regulation in 2018.

Regulators and Authorities

- Bank of Thailand (BOT)—central bank
- Securities Exchange Commission (Thai SEC)
- Revenue Department

Approaches

- *Bespoke*

Official Actions on Crypto-Assets and Technology

Digital Asset Regulation. Two predominant laws regulating digital assets were established in May 2018:[396]

- Royal Decree on Digital Asset Businesses B.E. 2561 (C.E. 2018)[397] regulating (1) offerings of digital tokens (ICO/STO related activities) and (2) the operation of Digital Asset Businesses (brokers/dealers, exchanges, other specified businesses), which are regulated by the Thai SEC; and
- Royal Decree on the Amendment of the Revenue Code (No. 19) B.E. 2561 (C.E. 2018) which taxes profits related to Digital Assets and which is regulated by the Revenue Department.
- 'Digital Assets' consist of electronic data generated on an electronic system or network consisting of either:
  - Crypto-currencies[398]—which serve as a medium of exchange, such as for the acquisition of goods, services, rights and Digital Assets;
  - Digital Tokens[399]—which serve as a determinant of the rights of a Token holder, such as the rights of an investor to participate in an investment or project (often called investment or security tokens) or the rights to receive specified products or services (often called utility tokens).[400]
- Violations of the Digital Asset Businesses Decree are subject to both civil and criminal sanctions.
- Approved Crypto-currencies. The Thai SEC periodically publishes a list of approved currencies which may be used as base currency trading pairs or as consideration for Digital Tokens being offered in an ICO. In February 2019, the Thai SEC removed Bitcoin Cash (BTH), Ether Classic (ETC) and Litecoin (LTC) from the list, leaving four active currencies, those being Thailand's national currency (baht), Bitcoin Core (BTC), Ether (ETH), Ripple XRP (XRP) and Stellar (XLM).[401]
- Offering Digital Tokens/ICOs/STOs. Thailand's regulatory framework provides flexibility to mimic the operation of traditional primary (offering) and secondary (trading) markets.

All Digital Asset Businesses are 'Financial Institutions' under the Decree and require licensing from the Ministry of Finance and must be compliant with Thai SEC regulations.

- In the primary market, an issuer of Digital Tokens must file with and obtain prior approval of the Thai SEC before using a Thai SEC[402] approved ICO Portal, which acts as a screening, due diligence and compliance mechanism. Digital Tokens may only be acquired by institutional or retail investors using fiat currency or an approved crypto-currency.[403] Secondary markets involve investors and licensed Digital Asset Business Operators[404] (brokers, dealers and exchanges) where any crypto-currency may be used for trading.

- Crypto-asset Historical Background. Thailand's journey to crypto-asset regulation is significant. In 2013, the Minister of Finance stated that Bitcoin is not within their legal jurisdiction.[405] Bitcoin Co. Ltd meetings with the Foreign Exchange Administration and Policy Department led to the suspension of Bitcoin trading.[406] In February 2018, Thailand's Finance Minister stated that the government will not ban cryptocurrency trading and that the release of a regulatory framework for digital currencies is imminent. Furthermore, it clarified that the Thai SEC is the most appropriate authority to manage the governance of digital currencies and not the BOT since cryptocurrencies are not recognized as legal tender.[407] Concurrently, the BOT issued a circular requesting that financial institutions refrain from engaging in cryptocurrency transactions and explicitly prohibited banks from 'investing or trading in cryptocurrency, offering cryptocurrency exchanges and creating platforms for cryptocurrency trading.'[408]

Taxation

- Digital Assets are treated as intangible assets and fall under the specific tax provisions of the Royal Decree. Gains from holding, possessing or disposing of Digital Tokens constitutes taxable income and subject to a 15% withholding tax in addition to any applicable personal or corporate income tax (less the withholding).

Technology

- A May 2019 press release announced the completion of the first phase of Project Inthanon, a BOT initiative (a consortium with eight participating banks) to build a blockchain-based solution to enable decentralized interbank payments using a wholesale CBDC.[409]

Developments

- The Thai SEC granted four Digital Asset Business licenses in January 2019 to three crypto-currency exchanges and one broker-dealer.[410]
- In March 2019 the Thai SEC approved the country's first ICO Portal.[411]

3.5 Vietnam

Overall

Crypto-currencies are banned as a payment method with significant restrictions placed on financial sector entities.

Regulators and Authorities

- State Bank of Vietnam (SBV)—central bank
- State Securities Commission (SSC)

Approaches

- *Restrictive*

Official Actions on Crypto-Assets and Technology

Crypto-currencies & ICOs

- The SBV provided a general warning in 2014 about the risks and dangers of engaging in Bitcoin and virtual currency transactions, identifying them as not lawfully approved forms of payment. Credit institutions were prohibited from trading Bitcoin and using it with clients as money or a form of payment.'[412]
- The SBV expanded the ban in October 2017, announcing that its updated legal framework now applied to payment instruments, which effectively banned the issuance, supply and use of Bitcoin and 'virtual currencies' as payment instruments.[413] Payment forms not included within Clause 6, Article 4 of Decree No. 101 of 2012 on non-cash payments (checks, bank cards, payment orders,

collection orders and payment instruments as prescribed by the SBV) were deemed illegal and subject to civil and criminal sanctions.[414]

- Several notable local ICO frauds attracted the attention and concern of Vietnamese authorities. Modern Tech, a company located in Ho Chi Minh City, launched two ICOs (Pincoin and Ifan) in early 2018 which allegedly victimized 32,000 investors for more than VND 15 trillion (USD 656 million).[415] These were reported to be a pyramid scheme scam which attracted the attention of Vietnamese regulators[416] and may have led to the country's subsequent bans of crypto-mining hardware and ICOs.
- The SSC declared in a January 2018 notice that securities business organizations should refrain from participating in 'operations related to advisory, brokerage, issuance, crypto-currency transactions as well as other financial technology products' while waiting for the appropriate authorities to update relevant legal frameworks.[417] Subsequently, the Prime Minister issued Directive No 10/CT-TTg in April 2018[418] on the 'strengthening of management of activities related to Bitcoin and other similar crypto-currency.' The SSC followed with a July 18 notice[419] which declared 'public companies, securities companies, fund management companies and securities investment funds shall not be permitted to carry out securities issuance, transaction and brokerage activities related to unlawful crypto-currency, compliance with the law of anti-money laundering.'[420]

Crypto-mining

- In July 2018, the SBV announced an agreement with the Ministry of Industry and Trade (MoIT) to ban imports of crypto mining hardware such as Application-specific Integrated Circuits (ASICs).[421]

Technology

- SBV announced in September 2018 its intent to create a Fintech Regulatory Sandbox. The Deputy Head of Payment Systems Oversight Division stated that the Bank intended to create a sandbox to enhance their legal framework and analyze a myriad of banking issues including those involving crypto-currencies.[422]
- KRONN Ventures AG announced that it had formed an international consortium and signed a memorandum of understanding with the Linh Thanh Group (the largest local distribution company) to create and establish a licensed blockchain-based cryptocurrency exchange in the Vietnam.[423] The legal status of crypto exchanges is unclear at present in light of the SSC notice of 2018.[424]

Taxation

- In September 2017, a Vietnamese court ruled that the Vietnam Department of Taxation had no authority to prosecute a local citizen for tax evasion relating to substantial gains realized from Bitcoin trading. The justification for the decision arose from Vietnamese law which does not consider Bitcoin an asset which would be subject to governmental taxation.[425]

4 Europe

4.1 Italy

Overall

Action by authorities as been limited with measures of forbearance, possibly needing to consider approaching application and redevelopment of the country's existing regulatory framework.[426]

Regulators and Authorities

- Bank of Italy (BdI)—central bank
- The Revenue Agency (ADE)—tax authority
- Ministry of Economy and Finance (MEF)
- Agency for Digital Italy (AGID)—technical agency of the Presidency of the Council of Ministers[427]

Approaches

- *Forbearance.* The country has recently adopted a 2019 law to formally recognize smart contracts.

Official Actions on Crypto-Assets and Technology

- Virtual Currency. 'Virtual Currency' per Legislative Decree 231/2007 (amended in AML Law amendment, 90/2017) is defined as a 'digital representation of value that is neither issued by a central bank or a public authority, nor attached to a legally established fiat currency which can be used as a means of exchange for the purchase of goods and services and transferred, stored and traded electronically.'[428]
- While virtual currency is not legal tender, it still can be used for payments.[429] Service providers for virtual currencies (use, exchange, storage and wallets) are required to register with the currency exchange register.[430] Investment products and services are considered 'Investment Services' and subject to existing investments and securities laws.[431] The amendment also subjects virtual currency providers to AML compliance requirements.[432]
- Italy has issued sparse guidance on treatment of virtual and crypto assets although developments have recently accelerated. In 2015 the BDI issued several general warnings about the dangers and risks of virtual currencies, including a declaration that existing law did not create AML/CFT compliance requirements for virtual currency exchanges.[433] The BDI discouraged use of virtual currencies until a formal regulatory framework was in place.[434]
- In December 2018, Italy signed a declaration joining the 'Mediterranean Seven' EU countries,[435] a coalition formed to educate, encourage and promote the use of DLT/blockchain technologies. Malta is in a leadership role, having taken the initiative to become one of the early blockchain-friendly countries which established a comprehensive virtual asset framework.[436]
- Simplification Decree of 2019. The Italian Parliament published an amendment to the law in the Official Gazette in February 2019,[437] which provides a specific definition and official legal recognition and enforceability for DLT[438] and smart contracts.[439] Commonly referred to as 'Decreto semplificazioni' or 'Simplification Decree', the law affords smart contracts the same legal recognition as written contracts provided that all essential terms are included.[440] Upon electronic identification of the parties, written form requirements for contracts will be met and the storage of the document information will produce a legally acceptable time stamp under Article 41 of the EU Regulation n. 910/2014 (eIDAS Regulation.)[441] Specific requirements and guidelines to accomplish these measures are to be adopted within 90 days by AGID.

Taxation

- At present there is a question of whether Italy's tax regulations are consistent. The ADE Resolution n. 72 of 02 September 2016 stated that Bitcoin transactions by 'economic operators' are considered Value Added Tax (VAT) exempt[442] and falling within the context of foreign currency.[443] However, when used in the context of speculative investing, virtual currencies appear to generate taxable income.[444]

4.2 Liechtenstein

Overall

Liechtenstein is one of the first countries to create a regulatory framework for crypto-assets, recently adopting its 'Blockchain Law' in May 2019.

Regulators and Authorities

- Financial Market Authority (FMA)—the primary regulatory authority supervising matters relating to fintech and tokenization of assets/crypto-assets.[445]

Approaches

- *Bespoke*– legislation and harmonization with existing laws and regulations.

Official Actions on Crypto-Assets and Technology

- **Blockchain Act of 2019.** The Liechtenstein government adopted the Token and Trustworthy Technology Service Provider Act; TVTG (the 'Blockchain Act')[446] in May 2019 in the interest of creating a 'token economy.' The act introduces a regulatory framework to establish and provide legal certainty for a fully tokenized ecosystem, to regulate applications such as crypto-currencies and ICOs as well as other forms of digital and crypto assets.'

- **FMA Fact Sheets.** The FMA issued 'fact sheets' for projects which may involve the use of DLT and crypto-assets. Innovators are welcome to contact the FMA to obtain greater clarity on how existing law and regulations may apply to their endeavors.
  - **Crowdfunding.** The FMA Fact Sheet on Crowdfunding[447] states that while no dedicated law exists on such endeavors, the application of existing law may require licensing which can be discussed directly with the authority.
  - **ICOs.** The FMA Fact Sheet on ICO[448] clarifies that tokens may constitute 'financial instruments' subject to FMA licensing, compliance with FMA rules and applicable AML/KYC obligations, all of which can be discussed directly with and a white paper reviewed by the FMA. Characterization of tokens (and whether they are subject to financial and securities laws and regulations) depends upon the specific circumstances and the rights attached to the token. The FMA has a process which expedites these issues.
  - **Virtual Currencies.** The FMA Fact Sheet on Virtual Currencies[449] explicitly identifies Bitcoin and provides general warnings about the inherent risks of dealing with virtual currencies. It also notes that the creation and use of virtual currencies are not subject to specific legislation, although certain business models may require licensing and compliance with existing laws and regulations (such as AML/CFT), which the FMA welcomes contact for discussion.
- **Cryptocurrency and Crypto Exchanges.** The FMA acknowledges that, 'in principle', exchanges of crypto-currency and legal tender do not require a license.[450] It does not officially recognize the term 'crypto exchange' and clarifies that all business models are evaluated on a case-by-case basis and that such exchanges would be subject to Liechtenstein due diligence law.
- **Definition of 'virtual currencies.'** A 2008 amendment to AML/CFT law added a definition for the use of virtual currencies, which are 'understood to be digital monetary units, which can be exchanged for legal tender, used to purchase goods or services or to preserve value and thus assume the function of legal tender.'[451]

5 Latin America

5.1 Brazil

Overall

Crypto-currency related activities exist and are generally unregulated, with regulators primarily observing and providing periodical guidance. The tax authority recently enacted new reporting rules for crypto exchanges and draft crypto-currency regulations are tabled for review.

Regulators and Authorities

- Central Bank of Brazil (BCB)
- Securities and Exchange Commission (CVM)
- Department of Federal Revenue (RFB) (tax authority)

Approaches

- *Forbearance.*

Official Actions on Crypto-Assets and Technology

Crypto-currencies

- BCB has provided general warnings about the risks and dangers of dealing with crypto-currencies, which are considered neither legal tender nor a currency.[452] BCB policy statements in 2014 and 2017[453] differentiate e-money (stored in a device or electronic system capable of payment transactions in the national currency) from 'virtual currencies' (not issued nor guaranteed by a monetary authority or payable in national currency.)

- An RFB notice of April 2014[454] stated that Bitcoin and altcoins are not a currency and should be treated as a financial asset which generates annual reporting requirements and potential capital gains tax.[455] However, the CVM stated in 2018 that they would not treat crypto-currencies as financial assets.[456] Accordingly, direct investment in crypto-currencies by Brazilian investment funds was prohibited and indirect investment discouraged by the regulator due to high risks. The CVM subsequently issued clarification guidelines for fund managers explaining that indirect investment was not prohibited, and emphasis was intended on the importance and necessity of due diligence in such endeavors.[457]
- A request was made May 30, 2019, to assemble a special commission for recommendations on virtual and crypto-currency regulation, including a review of draft Bill No. 2,303/2015 which would regulate Bitcoin, crypto-currencies and virtual currencies.[458] A new draft Bill No. 2,060/2019 was also reported which separates decentralized currencies (Bitcoin) from the centralized virtual currencies (air miles).[459]

Crypto-currency Exchanges

- A 2017 CVM circular[460] stated that securities offered through ICOs are prohibited from being traded on virtual currency exchanges, whom the CVM has not authorized for such purpose. RFB published a 2018 public consultation which required 'Digital Currency Exchangers' to send detailed monthly operational reports for transactions (including identification of the parties) with fines for non-compliance.[461] This led to RFB Instruction No. 1888 being passed in May 2019, effective August 1,[462] with first filings required in September 2019.[463]

ICOs, STOs and Tokens

- The CVM stated in a 2017 circular that ICOs and offers of 'virtual assets' which qualify as securities would place such offerings under CVM jurisdiction and the requirements of the Brazilian Securities Act.[464] It also explained the differences between ICO "white papers" and a proper prospectus with full disclosures and listed associated risks of ICOs. Noncompliance is considered illicit behavior subject to sanctions and penalties. CVM memorandums in 2017 and 2018 found that the Niobium Coin ICO[465] did not represent a public offering of securities or a financial asset.[466] The coin was classified as a utility token which was not considered a security since the purchaser was 'not promised any gain, profit or participation; but only the acquisition of an asset that may have a specific utility in the future...'[467]

Technology

- The BCB announced that, in 2019, it intends to use a blockchain-based platform and regtech solution called 'Information Integration Platform for Regulators' (Pier) for secure information sharing with other regulators of the Brazilian Financial System.[468] The Bank explained that the use of blockchain technology will reduce costs and provide tamper evident operation and greater efficiencies which would allow bypassing the need for a centralized entity.

Legal Action

- In February 2019, the Brazilian Federal District Court ruled against Banco do Brasil and Santander, requiring them to reopen the financial accounts of a cryptocurrency exchange (Bitcoin Max) which were closed without warning or explanation.[469] The ruling was subsequent to an earlier investigation by the Council for Economic Defense (CADE), Brazil's agency which investigates and prevents anti-competitive behavior, for the alleged de-risking activities of six banks[470] who abruptly closed the financial accounts of several cryptocurrency brokers and exchanges. The banks claimed closure was the result of a lack of AML compliance by its clients.[471] In 2018, a crypto exchange (Walltime) was awarded a preliminary injunction after its accounts were closed and over R$800,000 (USD 212,000) frozen by bank, Caixa Econômica.[472]

5.2 Mexico

Overall

Mexico has enacted new legislation to regulate across a variety of fintech activities and entities, including regulating crypto-assets. Action is needed by regulators to fully define, develop and implement secondary provisions supporting the primary legislation.

Regulators and Authorities

- Bank of Mexico (BdeM)—central bank
- National Banking and Securities Commission (CNBV)
- Ministry of Finance and Public Credit (SHCP)

Approaches

- *Bespoke regulation*

Official Actions on Crypto-Assets and Technology

Fintech Law

- In March 2018, Mexico adopted the Law to Regulate Financial Technology Institutions (known as the 'Fintech Law')[473] which establishes a regulatory framework governing the organization, operation and activities of entities involved in the financial technology industry. It sets a minimum set of regulations which are intended to be supplemented by secondary provisions, to be issued imminently following adoption by relevant authorities (such as the BdeM and CNBV, etc.)
- Virtual Assets are recognized and defined in Fintech Law Article 30 as 'the representation of value electronically registered and used among the public as a payment instrument in any type of legal transaction and which can only be transferred through electronic means.'[474]
- Fintech Law establishes two different types of 'Financial Technology Institutions' (ITFs)
    - *Joint Funding Institutions* which engage in crowdfunding activities; and
    - *Electronic Payments Funds Institutions (IFPE)* which include entities such as crypto-currency exchanges, e-wallet and payment service providers.
    - *Innovative models/regulatory sandboxes* is a separate category comprising of entities whose innovative business models, technologies, methodologies or tools depart from what currently exists in the marketplace.
- Fintech Law also sets the boundaries for operation by ITFs which have received prior authorization from the BdeM and CNBV.[475] The BdeM has the authority to determine the characteristics of Virtual Assets in addition to which specific Virtual Assets ITFs are permitted to operate. Eligibility, reporting requirements and compliance criteria for IFT applications and authorizations are set by the CNBV. The SHCP is authorized to issue AML/CFT policies for ITFs approved to transact with Virtual Assets, such as those relating to Know Your Customer (KYC) and information gathering and transaction reporting requirements.[476]
- For disclosure purposes, ITFs authorized to operate with Virtual Assets must explicitly inform customers:
    - A Virtual Asset is not legal tender and not supported by the Federal Government or BdeM;
    - It is impossible to reverse operations once executed, where applicable;
    - The value of Virtual Assets is volatile;
    - There are technological, cybernetic and fraud risks inherent in Virtual Assets.
- General provisions applicable to the Fintech Law were issued by the CNBV in September 2018.[477]

Bank of Mexico

- In 2014, the BdeM issued several warnings to the general public regarding the risks and dangers of dealing with Virtual Assets.[478] Virtual currencies have historically been deemed as not constituting legal tender nor treated as a foreign currency.[479] This sentiment was reiterated by the BdeM governor in 2017, who reasoned that Bitcoin should not be considered a virtual currency since it does not meet the existing definitions of a currency (supported by a government or central bank) and should thus be treated as a commodity.[480]

6 North America

6.1 Canada

Overall

Authorities have released extensive guidance on the application of crypto-assets to existing laws. The country's regulatory sandbox has approved almost a dozen crypto-assets related innovators. A substantial AML/CFT amendment introduced in 2014 which subjects money service businesses using crypto-currencies to registration and reporting to the country's FIU is still not yet in force.

Regulators and Authorities

- Bank of Canada—central bank
- Canadian Securities Administrators (CSA)
- Financial Transactions and Reports Analysis Centre (FINTRAC)—FIU and AML/CFT regulator
- Financial Consumer Agency of Canada (FCAC)—consumer protection regulator
- Ontario Securities Commission (OSC)—securities regulator of Ontario

Approach

- *Hybrid*—primarily adapting the use of crypto-assets to existing law through guidance.

Official Actions on Crypto-Assets and Technology

Crypto currencies and ICOs

- 'Digital currency' (DC) and crypto-currencies are permitted. Crypto-currency is not legal tender.[481] The Canadian Revenue Agency (CRA) has stated tax rules apply to all DC transactions and are treated as commodities for income tax purposes. Goods or services exchanged for DCs (assets not constituting not legal tender) are treated as barter.[482] Bill C-21, introduced in 2014 but not currently in force, amends the Proceeds of Crime (Money Laundering) and Terrorist Financing Act[483] and would subject money service businesses dealing with digital currencies to FINTRAC registration, reporting and compliance requirements.[484]

ICOs, ITOs, Utility and Security Tokens

- The Canadian Securities Administrators (CSA) issued CSA Staff Notice 46-307[485] and 46-308[486] in 2017 and 2018, which constitute the primary source of regulatory guidance[487] offered relating to the application of existing security laws to crypto-currency exchanges, ICOs and 'initial token offerings' (ITOs). The CSA found that many ICOs/ITOs involved coin/token offerings tantamount to sales of 'investment contracts' and subject to OSC security laws (and that the four-prong test from case law (*Pacific Coast Coin Exchange*).[488] Staff Notice 46-308 examined utility tokens and provided insight and example situations to aid in determining whether any coin/token offering constitutes an investment contract. Determinations are made on a case-by-case basis.

Crypto-asset Trading

- The Investment Industry Regulatory Organization of Canada (IIROC) issued a March 2019 joint consultation paper with the CA[489] seeking public feedback (until May 15) 'on how requirements may be tailored for Platforms operating in Canada whose operations engage securities law.'

Crypto Mining

- Hydro Quebec announced in May 2019 that Régie de l'énergie, a Quebec public interest and consumer protection regulator,[490] issued a decision on criteria to be used to allocate additional electricity to local blockchain operators.[491]

Regulatory Sandbox and Innovation

- Ten decisions authorizing entry into the CSA regulatory sandbox[492] have been issued relating to token distribution, crypto-asset offerings and investment funds and ICOS[493] (the latest being the May 21, 2019 decision on ZED Network Inc. concerning distribution of tokens.) 'Project Jasper' is a collaborative research project of the Bank of Canada (with Payments Canada and R3) exploring the use of DLT as a wholesale payments system, including clearing and settling of interbank payments.[494]

6.2 United States of America

Overall

The US has a split regulatory regime for financial services: the federal government and each of the 50 states. There is no consensus of approach to crypto-asset regulation on federal and state levels. Federal authorities have taken limited action while some state governments have been zealous to enact DLT and crypto-friendly legislation. This may lead to national harmonization challenges. Judiciary decisions and guidance issued by authorities may provide additional clarity on what token offerings are not subject to securities laws.

Regulators and Authorities

- Financial Crimes Enforcement Network (FINCEN)—bureau of the US Department of the Treasury, FIU, AML regulatory authority.[495]
- US Securities and Exchange Commission (US SEC)—independent regulatory agency of the securities markets which has statutory authority over digital assets deemed securities as defined under US federal securities laws.[496]
- Commodity Futures Trading Commission (CFTC)—independent regulatory agency with statutory authority over the commodities markets.[497]
- Internal Revenue Service (IRS)—the tax authority and tax collection agency.[498]

Approaches

- *Hybrid.* There is no consensus of approach to crypto-asset regulation in the US, which takes place on both federal and state levels. Approaches to state regulation can vary greatly, such as exemplified by New York and Washington states being more restrictive jurisdictions while Arizona and Wyoming are among the most permissive.[499]

Official Federal Actions on Crypto-Assets and Technology

- Virtual Currencies, Crypto-currencies. While the federal legislature has not issued crypto-asset definitions, several federal regulatory authorities have at present. FINCEN guidance issued in 2013 declares (i) 'virtual currency' is similar to currency 'but does not have legal tender status in any jurisdiction';[500] and (ii) 'virtual currency exchanges and administrators are money transmitters' and accordingly must comply with the US Bank Secrecy Act and registration, onboarding, due diligence and reporting requirements.
- The CFTC uses the IRS definition of 'virtual currency' which is a digital representation of value exhibiting the same characteristics as currency but not constituting legal tender.[501] CFTC jurisdiction over virtual currencies is generally limited to their use in derivatives contracts or incidents of fraud involving interstate commerce.[502]

ICOs, STOs, Utility & Security Tokens.

- The US SEC set forth guidance with its April 2019 release of a framework for analysis, a tool to aid in determination whether a digital asset should be classified as one type of security (an 'investment contract') which is subject to US SEC jurisdiction and applicable laws.[503] The framework clarifies that the *Howey* test (set forth in 1946 U.S. Supreme Court decision) and relevant case law[504] should be used to determine whether any crypto-asset or token is tantamount to being an "investment contract" and thus considered a security. Of key importance is making a determination using the substantive nature of the entire offering and not just focusing on form. While digital assets with 'consumptive characteristics are less likely to be tantamount to 'investment contracts' (and ostensibly deemed a 'utility token'), this conclusion is not absolute. The SEC has found that tokens offered under an ICO as utility tokens can qualify as securities.[505]
- During 2018, the US SEC issued public warnings 'to send messages to the ICO and digital asset marketplace on issues such as the potentially unlawful promotion of ICOs by celebrities and others and the risks associated with online trading platforms for digital assets.'[506] The SEC further noted that it investigated dozens of allegations and brought over a dozen enforcement actions in 2018 related to ICOs and digital assets, with many involving fraud.

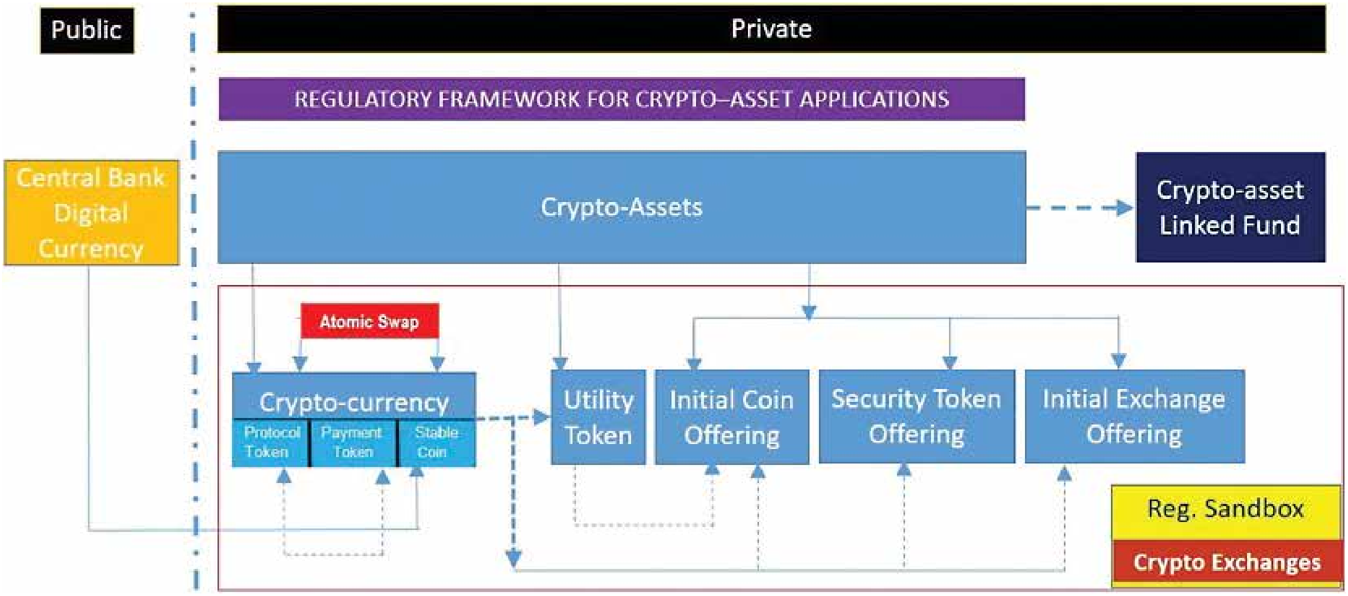
- In April 2019, the US SEC issued its first 'letter of no action' to TurnKey Jet, Inc. who sought to 'sell blockchain-based digital assets in the form of "tokenized" jet cards' which were consumptive in nature, provided that it met with several conditions.[507]
- Notable US SEC actions include the SEC chairman stating that Bitcoin and Ether are differentiated from most ICOs and would not be considered a security (while also having stated that virtually every ICO is tantamount to a security offering);[508] issuing an investigative report finding DAO Tokens to be securities.[509]
- Taxation. A 2014 IRS Notice defined 'virtual currency' (explicitly using Bitcoin as one example) and declared it taxable as 'property' and not as a currency.[510] The Notice provides extensive guidance on tax reporting, including declaring mining income as taxable.

Official State Actions on Crypto-Assets and Technology

Regulatory approaches at the state level vary greatly. By way of example, the states differ on whether virtual and crypto-currency exchange platforms trigger registration and compliance requirements as money transmitters/money service businesses.[511] Pennsylvania and Texas[512] are examples of states taking a more relaxed approach to embrace crypto innovation while New York (with its 'BitLicense')[513] and Washington (with its 'Uniform Money Services Act')[514] take a more cautious and stringent approach. (New York's BitLicense has been notably challenging to crypto innovators,[515] although a first license was awarded in 2019.)[516] The following is a select list of state bills passed in 2019 along with relevant regulatory guidance issued.

- **Colorado.** The 'Digital Token Act' (Bill SB023) defines digital tokens as exempt from local securities laws provided certain conditions are present (consumptive purpose, not offered as investments, etc.)[517]
- **Montana.** Bill HB0584 defines a 'utility token' which is not considered a security under local law provided it is 'primarily consumptive' in nature, not marketed as an investment and other conditions.[518]
- **Pennsylvania.** The Department of Banking and Securities issued guidance declaring virtual currency exchange platforms not 'money transmitters' under the state's Money Transmitter Act as they never directly handle fiat currency.[519]
- **South Dakota.** Bill HB1196 provides an official definition of blockchain technology as 'technology that uses a distributed, shared, and replicated ledger, either public or private, with or without permission, or driven with or without tokenized crypto economics where the data on the ledger is protected with cryptography and is immutable and auditable.'[520]
- **Texas.** Crypto-currency is generally not considered money under the state Money Services Act. Accordingly, it is not subject to money transmission requirements when it is transmitted. However, when sovereign currency is involved such as sovereign backed stablecoins, it may fall under the state's money transmission laws.[521]
- **West Virginia.** Marketplace facilitator tax applies where 'virtual currency'[522] is used. The state defines virtual currency and it explicitly excludes from the definition ring-fenced, centralized currencies ('used solely within gaming platforms; have no market application outside of those gaming platforms; cannot be converted into, or redeemed for, Fiat Currency or Virtual Currency.')
- **Wyoming.** Bill SF0125 classifies digital assets within existing laws; classifies them as property under the state Uniform Commercial Code; authorizes security interests in digital assets; establishes an opt-in framework for banks to provide custodial services for digital assets; and clarifies the jurisdiction of the state courts relating to digital assets.[523] Bill HB0185 permits the issuance of tokenized stock certificates.[524] Bill HB0057 creates a state authorized financial technology sandbox and establishes certain waivers, standards and procedures for operation, eligibility requirements and other rules and conditions.[525]

D. Model Crypto-asset Regulatory Framework



Key: UT = Utility Tokens; ST = Security Tokens; CC = Crypto-currencies; ICO = Initial Coin Offerings; IEO = Initial Exchange Offering; DLT = Distributed Ledger Technologies; dApps = Distributed Applications.

This model framework was published by the author in December 2019. The lines show methodologies for value transfer, A more detailed explanation is available in the original paper.[526]

Endnotes

1. DLT technology could have made the 2008 crisis response much less aggravated had it existed then. See remarks thereto by United States Commodity Futures Trading Commission Chairman Christopher Giancarlo, at The Block (2019) *Blockchain could have led to faster regulatory response in 2008 global crisis, CFTC official says*, available at www.bit.ly/2KxXSOW
2. The term 'legacy' here is meant to draw a bright line distinction between entities (if so classed) and products/services that are not natively DLT-based—that is, all-DLT. See below for a more detailed discussion.
3. On May 22 2010, one Laszlo Hanyecz in Florida traded 10,000 Bitcoin for some pizza in what is widely believed to be the first real-world transaction involving Bitcoin. Bitcoin then was worth less than a cent. Today his payment would be worth around USD 82 million. Bitcoin enthusiasts celebrate 'Bitcoin Pizza Day' on May 22 every year. See CBS (2019) *Meet the Man Who Spent Millions Worth of Bitcoin on Pizza*, available at www.cbsn.ws/2VwLPTK
4. In many cases, the visceral regulatory response has been to curtail or ban possession, use or trading of crypto-currencies insofar as domestic regulations may apply domestically and ex-territorially.
5. Daily Beast (2013) *Hitman Network Says It Accepts Bitcoins to Murder for Hire*, available at www.bit.ly/2EY1tCa
6. The Financial Action Task Force, also known by its French name, Groupe d'action financière, is an intergovernmental organization founded in 1989 on the initiative of the G7 to develop policies to combat money laundering. In 2001 its mandate expanded to include terrorism financing. See www.fatf-gafi.org
7. Indeed, for maximalists, identity is a bug, not a desired feature.
8. Folkinshteyn, D & Lennon, Mark M. & Reilly, T (2015) *A Tale of Twin Tech: Bitcoin and the WWW*, available at www.ssrn.com/abstract=2601617
9. *ibid.*
10. The emergence thought of permissioned, controlled 'consortia' DLTs for use in banking and other verticals has altered this 'totally decentralized' paradigm.
11. Mitra, R (2019) *What is Web 3.0? The Evolution of the Internet*, available at www.blockgeeks.com/guides/web-3-0/
12. Since it was released in 2009, Bitcoin has undergone many transitions and improvements—or 'forks'—as the process known in the DLT ecosystem. Where Bitcoin is referred to in this paper, it refers to the Bitcoin blockchain version most approximate to the original, Bitcoin Core. The trading symbol on exchanges for this crypto-asset is BTC.
13. Rohr, J & Wright, A (2017) *Blockchain-Based Token Sales, Initial Coin Offerings, and the Democratization of Public Capital Markets*, available www.ssrn.com/abstract=3048104
14. Also called validators.
15. For example, as a means for accounting with its native ecosystem such as the number of API-calls in a smart contract.
16. Not to be confused with airdrops in the Apple ecosystem, an ad-hoc service for transfer of files among supported Macintosh computers and iOS devices over Wi-Fi and Bluetooth without using mail or a mass storage device. REF
17. There was never any token sale for Bitcoin. The only way to acquire new Bitcoin is via mining.
18. An exception may be so-called stablecoins as well as STOs, both of whose values can be based on real assets.
19. For analogous legacy financial market comparisons, see Stellinga, B & Mügge, D (2017) *The regulator's conundrum. How market reflexivity limits fundamental financial reform*, available at www.bit.ly/2HPfZyc
20. Actors here are those involved in any process which generates, values, issues, stores, or trades a crypto-asset. See Exhibit 5 on how these actors fit into a stylized crypto-economy environment.
21. Prediction markets using DLTs for example betting on whether a politician will be assassinated may approach illegality in many jurisdictions, but natively be manifestly unethical.
22. Initial reactions to the emergence of these technologies have been their legal and regulatory impact. The visceral reaction—besides trying to understand the technology and their import—has been towards whether for example the initial blockchain application, Bitcoin and its trading—are whether the types and use of these DLT systems are 'legal.' These discussions have mostly been whether the systems and applications are permissible in terms of existing regulatory frameworks, most proximately whether licenses are required to send and receive value, and similarly whether the pseudonymous or anonymous nature of many of the initial iterations of DLT implementations comply with KYC and Anti Money Laundering regulations and procedures.
23. De, N (2019) *Over 40 Central Banks Are Considering Blockchain Applications: Davos Report*, available at www.bit.ly/2FXhaKQ
24. As noted by the Committee on Payments and Market Infrastructures CPMI, CBDCs are potentially a new form of digital central bank money that can be distinguished from reserves or settlement balances held by commercial banks at central banks. The CPMI indicates that there are various design choices for a CBDC, including: access (widely vs restricted); degree of anonymity (ranging from complete to none); operational availability (ranging from current opening hours to 24 hours a day and seven days a week); and interest-bearing characteristics (yes or no). For a comprehensive treatise, see CPMI (2018) *Central bank digital currencies*, available at www.bis.org/cpmi/publ/d174.pdf

25. See on FMIs and the role they play in the global financial ecosystem, BIS (2019) *Principles for Financial Market Infrastructures (PFMI)*, available at www.bis.org/cpmi/info_pfmi.htm

26. On the macro-economic impact of crypto-currencies, see Noam, E (2019) *Macro-economics of crypto-currencies* (forthcoming). For an EU-wide assessment, see European Central Bank (2019) *Crypto-Assets: Implications for financial stability, monetary policy, and payments and market infrastructures*, available at www.bit.ly/2MroPWY

27. For a central bank view on their potential systemic impact, see European Central Bank (2019) *Crypto-Assets: Implications for financial stability, monetary policy, and payments and market infrastructures*, available at www.bit.ly/2MroPWY

28. See Annex E: Model Crypto-Asset Regulatory Framework. This was originally published by the author in December 2018 and revised in June 2019.

29. Mitra, R (2019) *What is Web 3.0? The Evolution of the Internet*, available at www.blockgeeks.com/guides/web-3-0/

30. For insights into the regulators dilemma in making policy and rules around transformative financial products and ecosystems, see Perlman, L (2012) *Doctoral Thesis: Legal and Regulatory Aspects of Mobile Financial Services*, available at www.papers.ssrn.com/abstract=3174463

31. There is also the Ripple DLT, which is not viewed as 'blockchain' technology. See www.ripple.com

32. Portions of the sections that follow are drawn from Perlman, L (2017) *Distributed Ledger Technologies and Financial Inclusion*, available at www.bit.ly/2nyxpBG; and from Perlman, L (2017) *Security Aspects of Distributed Ledger Technologies* (forthcoming)

33. Full decentralization was the initial DLT design and policy goal. Some DLTs—particularly those known as 'permissioned blockchains' have a measure of control, so while they are not fully decentralized, the data is still 'distributed.' DLTs used by financial institutions like banks are for example more centralized.

34. Bitcoin is a consensus network that enables a new payment system and a completely digital money or 'crypto-currency.' It is thought to be the first decentralized peer-to-peer payment network that is powered by its users with no central authority or middlemen. The first Bitcoin specification and proof of concept (POC) was published in 2008 in a cryptography mailing list by one 'Satoshi Nakamoto.' It is not known if this is a pseudonym, The Bitcoin community has since grown exponentially, but without Nakamoto. See Bitcoin (2019) *FAQs*, available at www.bitcoin.org/en/faq#what-is-bitcoin.

35. The concept 'crypto-currency' was first described in 1998 in an essay by Wei Dai on the Cypherpunks mailing list, suggesting the idea of a new form of money he called 'b-money.' Rather than a central authority, it would use cryptography to control its creation and transactions. See Dai, W (1998) *b-money*, available at www.weidai.com/bmoney.txt.

36. The technology, in the words of Bitcoin's apparent creator, is: '[A] system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party.' See Nakamoto, S (2008) *Bitcoin: A Peer-to-Peer Electronic Cash System*, available at www.bitcoin.org/bitcoin.pdf. Note that Nakamoto's 2008 paper does not use the terms 'blockchain' or 'distributed ledger.' These are terms others later used to describe the technology Nakamoto designed.

37. Term coined by Vitalik Buterin, Ethereum Founder. NeonVest (2018) The Scalability Trilemma in Blockchain, www.bit.ly/2Y3dEpb

38. See Mills, DC *et al* (2016) *Distributed Ledger Technology in Payments, Clearing, and Settlement FEDS Working Paper No. 2016-095*, available at www.ssrn.com/abstract=2881204; and UK Government Office for Science (2016) *Distributed Ledger Technology: Beyond Block Chain*, available at www.goo.gl/bVg0Vq. The term Distributed Ledger Technology is often used interchangeably with 'Shared Ledger Technology.' DLT though will be used throughout this study. SLT was coined by Richard Brown, CTO of blockchain company R3, available at www.goo.gl/gaeDRU; and Hoskinson, C (2016) *Goodbye Mike and Some Thoughts About Bitcoin*, available at www.goo.gl/bGVN0R.

39. There is also the Ripple DLT, which is not viewed as 'blockchain' technology. See www.ripple.com

40. This used to be known as 'Immutability of the data record', but since the attack on The DAO, this is no longer the case. See below.

41. Not all DLTs have smart contract capabilities. For example, Bitcoin lacks smart contract capabilities.

42. A common concern is that current DLTs processes are much slower than what is needed to run mainstream payment systems or financial markets. Also, the larger the blockchain grows, the larger the requirements become for storage, bandwidth, and computational power required to process blocks. This could result in only a few nodes being able to process a block. However, improvements in power and scalability are being designed to deal with these issues. See Croman, K *et al* (2015) *On Scaling Decentralized Blockchains*, available at www.goo.gl/cWpQpF; and McConaghy, T *et al* (2016) *BigchainDB: A Scalable Blockchain Database*, available at www.goo.gl/IBcGv0.

43. This is also known as interoperability.

44. There are, of course, a number of broader technical and other issues relating to DLTs and their *inter alia* advantages and disadvantages, as well as their legal, regulatory, security, privacy, and commercial implications. They are noted or discussed briefly but are generally beyond the scope of this paper and will not be detailed in depth.

45. While DAG is often termed Blockchain 3.0, it is actually an entirely new technology using a graph data structure that uses a topological ordering, and which does not use blocks or chains. At their core DAGs have the same properties as a blockchain in so far as they are still distributed databases based on a peer-to-peer network and a validation mechanism for distributed decision making. Examples of the still-evolving DAG technology are the IOTA Tangle and *Hedera Hashgraph*. Hedera (2019) Hedera Hashgraph, available at www.bit.ly/2IrUnHj

46. There have been more than 2,500 blockchain related patent filings and billions of dollars in investments by enterprises and in startups, while at least 24 countries are investing in the technology, 50 corporations have joined consortia around it, and 90 banks are in discussions about it worldwide. See IFC (2019) *Blockchain: Opportunities for Private Enterprises in Emerging Markets*, available at www.bit.ly/2XoLgwZ

47. del Castillo, M (2018) *Big Blockchain: The 50 Largest Public Companies Exploring Blockchain*, available at www.bit.ly/2wAOZMf

48. Tsao, P (2019) *Blockchain 2.0 and Ethereum [Blockchain Basics Part 3]*, available at www.bit.ly/2WkHof8

49. *ibid.*

50. Any data that is placed on the block is said to be 'on-chain' and any data that derives from the blockchain, but which for some reason must be swapped with another party not using blockchain technology is said to be 'off chain.' See also Mills *et al* (2016) *ibid.*

51. Depending on the DLT, the consensus method may be called Proof of Stake (POS), or Proof of Work (POW). For example, with crypto-currencies POS is a consensus mechanism used as an alternative to the POW mechanism used in Bitcoin. POS crypto-currencies are 'minted' rather than 'mined,' so avoiding expensive computations and thus providing a lower entry barrier for block generation rewards. For a fuller discussion of these differences, see Bitfury Group (2015) *Proof of Stake Versus Proof of Work*, available at www.goo.gl/ebS2Vo.

52. Some would argue that in practice Bitcoin is basically a closed network today since the only entity that validates a transaction is effectively 1 in 20 semi-static pools. Further, the miners within those pools almost never individually generate the appropriate/winning 'hash' towards finding a block. Rather, they each generate trillions of invalid hashes each week and are rewarded with shares of a reward as the reward comes in.

53. Distinctions between permissioned and permissionless described here reflect the current state of the art. As DLTs mature, many believe that there will be a full spectrum between permissioned and permissionless.

54. Public blockchains are said to be fully decentralized.

55. For faster 'block times'—the time it takes to produce one block.

56. Choudhury, K (2018) *What Blockchain Means for Developing Countries*. available at www.bit.ly/2XCxQxT

57. Bitcoin and Ethereum blockchains for example use *probabilistic finality*, in which the probability that a transaction will not be reversed increases as the block which contains that transaction sinks deeper into the chain. The deeper the block, the more likely that the fork containing that block is the longest chain. This means that at least 6 blocks must be placed on the Bitcoin blockchain (taking an hour) to ensure irrevocability. See Gauba, A (2018) *Finality in Blockchain Consensus*, available at www.bit.ly/30NydY8

58. For Ethereum, its 30 blocks. Leung, D and Camacho, P (2019) Understanding Delayed Finality in Off-Chain Transactions, available at www.bit.ly/2KttPb6

59. Leung, D & Camacho, P (2019) *Understanding Delayed Finality in Off-Chain Transactions*, available at www.bit.ly/2KttPb6

60. There is also absolute finality characteristic PBFT-based protocols such as on the Tendermint blockchain, in which a transaction is immediately considered finalized once it is included in a block and added to the blockchain.

61. Hays, D (2019) *Blockchain 3.0 The Future of DLT?*, available at www.bit.ly/2ImI8M6

62. State channels are two-way pathways opened between two users that want to communicate with each other in the form of transactions. Each participant in the channel signs these transactions with his private key to ensure that they are undeniably true and authorized. These channels are off-chain and private, known only to its participants. *See* Antonio Madeira (2017) What are State Channels, available at www.bit.ly/2EWr6mU

63. Cointelegraph (2019) *What is Lightning Network and How It Works*, available at www.bit.ly/2Ku2UMt

64. Sharding refers to splitting the entire Ethereum network into multiple portions called 'shards'. Each shard would contain its own independent state, meaning a unique set of account balances and smart contracts. *See* District0x (2019) *Ethereum Sharding Explained*, available at www.bit.ly/2WUmmZ8

65. Hays, D (2019) *An Overview of the Evolution of Blockchain Technology, Blockchain 0.0 to 3.0*, available at www.bit.ly/2QS5ZqK

66. But see Ethereum co-founder Vitalik Buterin's concern on how to implement POS in Ethereum to improve scaling. He identified 4 possible hurdles: (i) Having lower than expected participation rates invalidating (ii) Stake pooling becoming too popular (iii) Sharding turning out more technically complicated than expected and (iv) Running nodes turning out more expensive than expected, leading to (1) and (2). See Maurya, N (2019) *Vitalik lists down four hurdles proof of stake*, available at www.bit.ly/2WtTzLO

67. Mappo (2019) *Blockchain Governance 101*, available at www.medium.com/aelfblockchain/blockchain-governance-101-eb2d769e85c5

68. Hsieh, Y & Vergne, J & Wang, S (2018) *The internal and external governance of blockchain-based organizations: evidence from crypto-currencies*, available at www.bit.ly/2wEGTSX

69. *See* the Bitcoin Core 'Bitcoin Improvement Proposals' voting process. *Ibid.* Heish (2018). *See also* WhaleCalls (2017) *Fact or FUD—"BlockStream, Inc is the main force behind Bitcoin (and taken over)"*, available at www.bit.ly/2ztVnqr

70. For example, Nakamoto for Bitcoin; Buterin for Ethereum.

71. Adapted from www.bit.ly/2MAtdDg

72. *See also* www.bit.ly/2MAtdDg

73. Lack of transparency, as well as susceptibility to corruption and fraud, can lead to disputes.

74. The Depository Trust and Clearing Corporation, the company that serves as the back end for much Wall Street trading and which records information about every credit default swap trade, is replacing its central databases as used by the largest banks in the world with blockchain technology from IBM. See NY Times (2017) *Wall Street Clearinghouse to Adopt Bitcoin Technology*, available at www.nyti.ms/2iac0iM.

75. Partz, H (2019) *Medici Portfolio Firm Partners with Caribbean Bank to Pilot Digital Currency*, available at www.bit.ly/2FOuTDD

76. ZDNET (2016) *Why Ripples from this Estonian Blockchain Experiment may be Felt around the World*, available at www.goo.gl/eaLf3G.

77. Memoria, F (2019) *Canadian Town Starts Accepting Bitcoin for Property Tax Payments*, available at www.bit.ly/2WFnVGN

78. This would, with current developments, be more applicable to identity systems rather than national identity systems. It can be applied then to digital identity, with notes that certain attributes have been attested by certain authorities. The keys associated with the identity, and the details of the attributes and the associated attestations, would be held in a separate secure identity store, under the control of the individual. One of the attributes might be name—attested to by the national identity service. The identity on the blockchain would be derived from that.

79. Bitcoin Magazine (2015) *Estonian Government Partners with Bitnation to Offer Blockchain Notarization Services to e-Residents*, available at www.goo.gl/YdoYKq.

80. As transactions occur and data is transferred, the agreements and the data they individually control need to be synchronized. Often though, the data will not match up because of duplication and discrepancies between ledger transactions, which results in disputes, disagreements, increased settlement times, and the need for intermediaries (along with their associated overhead costs).

81. See also IBM (2016) *Blockchain Basics: Introduction to Business Ledgers*, available at www.goo.gl/dajHbh.

82. As noted above, in some cases, the token and the application may be the same thing. For example, the genesis DLT, the Bitcoin blockchain, also has as its crypto-asset its native 'coin,' Bitcoin. Bitcoin when it was launched in 2009 through the publication of a paper by someone—as yet verified—named 'Satoshi Nakamoto,' the appellation crypto-currency was popularly assigned to it.

83. The most proximate use of tokens in the financial world in their use as crypto-graphic representations of account details for credit cards, designed to mask real account numbers for security reasons. The term has been adopted in the DLT world to be the building block of the crypto-economy.

84. While TCP/IP was the protocol, the Layer 1 now can be monetized too as incentives to process the 'transactions'—adding blocks now reward those—miners—unlike TCP/IP. The protocol layer is thus being monetized.

85. IMF (2018) *World Economic Outlook, October 2018: Challenges to Steady Growth*, available at www.bit.ly/2OeIoT8

86. By contrast, the legacy financial system uses a delayed-net-settlement system involving layers of intermediaries. The key words here are delayed, net and intermediaries.

87. Wright, A & De Filippi, P (2015) *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*, available at www.ssrn.com/abstract=2580664

88. For a taxonomy relating to crypto-assets in the US, see Henderson, MT & Raskin, M (2019) *Regulatory Classification of Digital Assets: Towards an Operational Howey Test for Cryptocurrencies, ICOs, and Other Digital Assets* (Columbia Business Law Review), available www.ssrn.com/abstract=3265295

89. The terms are fluid, with non-fungible tokens (NFTs) being the rage in 2016-2017. By 2018 the term had all but disappeared as a term of art in the 'crypto' world.

90. 8 bit sumo (2019) *What's the Difference between Coin, Token and Protocol?*, available at www.bit.ly/2HZvdkc

91. UK Task Force (2018) *Cryptoassets Taskforce: final report*, available at www.bit.ly/2qgn1Cf

92. 8 bit sumo (2019) *What's the Difference between Coin, Token and Protocol?*, available at www.bit.ly/2HZvdkc

93. Kasireddy, P (2017) *How does Ethereum work, anyway?*, available at www.bit.ly/2fDL2l3

94. The gas fee is a series of incentives: gas is used to pay for computation steps as well as keeping the EVM 'lean' since all operation executes by the EVM is simultaneously affected by every full node. Thus, the gas fee includes a storage fee (on a node) proportional to the smallest multiple of 32 bytes used. If a transaction has a step that clears an entry in the storage, the fee for executing that operation of is waived, and a refund is given for freeing up storage space.

95. Ethereum, though, is a 'Layer 1' protocol with significant speed and scalability challenges. While there is a roadmap to improve Ethereum to use the more efficient POS, new 'Layer 2' protocols that aim to solve these challenges sit atop Ethereum Layer 1 and have their own token and rewards ecosystem. Buck, A (2019) *A Beginners Guide To OmiseGO (OMG)*, available at www.bit.ly/2Wpn8y1

96. Users pay those who process the transactions but setting a maximum gas fee they are willing to pay, with all the gas sent by the sender given to the 'beneficiary' (miners) address.

[97] Wright, A & de Filippi, P (2015) *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*, available at www.ssrn.com/abstract=2580664

[98] Rohr, J & Wright, A (2017) *Blockchain-Based Token Sales, Initial Coin Offerings, and the Democratization of Public Capital Markets*, available at www.ssrn.com/abstract=3048104

[99] For example, to process the additional of blocks on a blockchain, miners or validators are required to be online and to undertake the computational heavy lifting required. They are rewarded in the native 'currency' of that blockchain.

[100] This means that it will execute all computational requests until it can't, and resultantly that Ethereum could conceivably launch into a type of death spiral if given an instruction that could execute indefinitely.

[101] The 'gas' rewards in Ethereum.

[102] Since miners are expending the effort to run computations and validate transactions, miners receive the fee as a reward. The more the sender offers, the more likely a miner will accept the request of adding data.

[103] Ether is the crypto-currency of Ethereum.

[104] Shekhar, S (2018) *Measuring Maker-Dai Stability*, available at www.bit.ly/2K0Iuer

[105] For example, if a payment is triggered by a smart contract term, the payee (a counterparty) would expect X as per that term. Volatility, in a worst case, may result, though, in a fraction of X. Unless the counterparty is fine with the risk, for safety and soundness, most counterparties need some surety that the absolute value promised is the value delivered.

[106] Memon, B (2019) *Guide to Stablecoin: Types of Stablecoins & Its Importance*, available at www.bit.ly/2wBMlWE

[107] The term 'ICO' is derived from the legacy term 'initial public offering' (ICO) used in securities and share listings

[108] 'Functionality' is often seen as a measure of whether something offered in an ICO is an investment or not. The distinction 'functional' versus pre-functional' is often made to determines this. A so-called Simple Agreement for Future Tokens (SAFT) Simple Agreement for Future Tokens (SAFT) was created by layers advising crypt-asset actors in the US to ensure regulatory compliance, It is seen as an investment contract offered by crypto-currency developers to accredited investors. It is considered a security and, thus, must comply with securities regulations.

[109] Singapore and Switzerland treat ICO tokens as assets and not as securities. Malta passed crypto-asset enabling regulations in 2018, leading to an influx of exchanges and ICOs being launched from there. Non-US ICOs are even IP-blocking US residents from participating due to potential legal implications. See **Section 7** and **Annex C** below on regulatory approaches in selected other countries.

[110] The US SEC, for example, officially considers (any) tokens as securities, which means that ICO issuers will have to register as securities and file periodic reports with the SEC. This policy has in turn resulted in very few exchanges being able to provide issuance services in the EU and the US. The policy appears to have some carve-outs though: the US SEC for example has said that Ethereum is not a security; and further, that a process that started out as an ICO which would under current SEC rules attract an enforcement action, could over time morph into a UT or STO which would not attract action. That is, the original ICO activity would not necessarily attract action. This, we suggest demonstrates the fluid nature of crypto-assets adding to the regulator's dilemma. See thereto, CoinDesk (2019) *SEC's Hinman Says Some ICOs May Be Eligible for 'No-Action' Relief*, available at www.bit.ly/2WaCott

[111] Strategic Coin (2018) *The Difference Between Utility Tokens and Equity Tokens*, available at www.bit.ly/2TIbiKy

[112] EFRAG (2019) *Research project—Crypto-Assets*, available at www.bit.ly/2Ml2nii

[113] Strategic Coin (2018) *ICO 101: Utility Tokens vs. Security Tokens*, available at www.bit.ly/2GKRa6T

[114] US SEC (2018) *Two ICO Issuers Settle SEC Registration Charges, Agree to Register Tokens as Securities*, available at www.bit.ly/2Pwc8vs

[115] Finma (2018) *Guidelines*, available at www.bit.ly/2BzA88M

[116] Issuing STs can be done on Layer 1s, or on side-chains. For example, Blockstream's 'Liquid Securities' platform is a dApp that allow users to issue and manage security tokens on top of its Liquid Network side-chain and establish sophisticated rule-sets to conform with regulatory requirements, with no engineering experience required.

[117] A security token has similar characteristics to a security and grants the right or possibility of receiving a pre-defined financial benefit (such as interest or a dividend). EFRAG (2019) *Research project—Crypto-Assets*, available at www.bit.ly/2Ml2nii

[118] A report by PWC indicated that 28 Security Token Offerings (STOs) raised USD 442 million in 2018. PWC (2019) *4th ICO/STO Report*, available at www.pwc.to/2XruH3L

[119] *Liechtenstein Blockchain Act (Act on Transaction Systems based on Trustworthy Technologies (VT) (Blockchain Act; VT Act; VTG)) 2018*, available at www.bit.ly/2P1gCVA

[120] Unlike real wallets, a crypto wallet does not directly include funds, only the key to spend them.

[121] Aumasson, JP (2018) *Attacking and Defending Blockchains: From Horror Stories to Secure Wallets*, available at www.ubm.io/2Ksaqre

[122] Users login into the exchange, who may store credentials so as to allow easy exchange of value without the user needing to log in every time. The tokens may be stored on its hot or cold wallet. This ostensibly also improves trading times as the liquidity is on-tap.

[123] Aumasson, JP (2018) *Attacking and Defending Blockchains: From Horror Stories to Secure Wallets*, available at www.ubm.io/2Ksaqre

124. This could involve for example placing an encrypted USB stick on a safe in an underground vault in another country or region.

125. Not all DLTs support smart contracts. The original Bitcoin—now known as Bitcoin Core—for example, does not support smart contracts. The Ethereum DLT is the prime exemplar of the use of smart contracts.

126. Smart contracts were first described in 1997, relating to vending machines. See Szabo, N (1997) *Smart Contracts: Building Blocks for Digital Markets*.

127. The physical contract signature is replaced by the use of cryptographic keys that indicate assent by participant nodes to the 'legal' terms embedded in the blockchain by the EtherScript.

128. However, compliance rules with one or more of the counterparties—or through peremptory regulations such as those dealing with anti-money laundering (AML) rules or the implication of tax laws—would probably require proper legal counsel. The potential benefits of smart contracts include low contracting, enforcement, and compliance costs. They may make it economically viable to form contracts for numerous low-value transactions. They then could be successfully applied in e-commerce, where they can significantly facilitate trade by reducing counterparty risk and the costs of transacting by minimizing the human factor in the process.

129. PWC (2016) *Blockchain and smart contract Automation: How smart contracts Automate Digital Business*, available at www.pwc.to/2gqOkaT; *Etherscripter (2016) What is Ethereum*, available at www.bit.ly/2I0sUgI

130. Oracles are third party services which are not part of the blockchain consensus mechanism and are effectively 'off-chain' and thus considered insecure in relation to the DL itself. The accuracy of data inputs and outputs by oracles are key as it is near impossible to roll back transactions once executed on a DL.

131. ***Citation Needed***

132. Portions of the sections that follow are drawn from Perlman, L (2017) *Distributed Ledger Technologies and Financial Inclusion*, available at www.bit.ly/2nyxpBG; and Portions of the sections that follow are drawn from Perlman, L (2017) *Security Aspects of Distributed Ledger Technologies* (forthcoming)

133. See further, Kuo Chuen, D and Guo, Li and Wang, Yu (2017) *Cryptocurrency: A New Investment Opportunity?*, available at www.ssrn.com/abstract=2994097

134. Table adapted from Long, C (2019) *Settlement Risks In Crypto/Legacy Hybrid Instruments*, available at www.bit.ly/2WCRc8L

135. *ibid.*

136. See **Annex B**.

137. Long, C (2019) *Settlement Risks In Crypto/Legacy Hybrid Instruments*, available at www.bit.ly/2WCRc8L

138. *ibid.*

139. Decentralized applications (dApps) are applications that run on a P2P network of computers rather than a single computer and have existed since the advent of P2P networks in a way that is not controlled by any single entity. Whereas, centralized applications, where the backend code is running on centralized servers, dApps have their backend code running on a decentralized P2P network. See Blockchainhub (2019) *Decentralized Applications—dApps*, available at www.blockchainhub.net/decentralized-applications-dapps/ The Ethereum white paper splits dapps into three types: apps that manage money, apps where money is involved (but also requires another piece), and apps in the 'other' category, which includes voting and governance systems. CoinDesk (2018) *What is a Decentralized Application?* www.coindesk.com/information/what-is-a-decentralized-application-dapp; and www.github.com/ethereum/wiki/wiki/White-Paper#applications

140. Dantoni, J (2019) *Mapping out Ethereum's DeFi*, available at www.bit.ly/2WQSUU6

141. A 'stable coin' is a crypto-currency pegged to another stable asset such as gold or the U.S. dollar. It's a currency that is global but is not tied to a central bank and has low volatility. Coins like Bitcoin and Ethereum and highly volatile. This allows for practical usage of using crypto-currency like paying for things every single day. See Lee, S (2018) *Explaining Stable Coins, The Holy Grail of Cryptocurrency*, available at www.bit.ly/2EVNPQ1

142. See **Section 4.3** below on Decentralized Exchange (DEXs) platforms.

143. Use case adapted from Hedera (2019) *An introduction to decentralized applications (dapps)*

144. For a list of over 100 live DeFi initiatives globally, see ConsenSys (2019) *The 100+ Projects Pioneering Decentralized Finance*, available at www.bit.ly/2HZQ6M2

145. Norton Rose Fulbright (2016) *Unlocking the blockchain: A global legal and regulatory guide—Chapter 1*, available at www.bit.ly/2XCymvP

146. Blockonomi (2018) *What Is a DAO? Decentralized Autonomous Organizations & the Ethereum Hack*, available at www.bit.ly/2HYJ4ah

147. See also on hedge funds and DLTs, Mokhtarian, E and Lindgren, A (2019) *Rise of the Crypto Hedge Fund: Operational Issues and Best Practices for an Emergent Investment Industry*, available at www.stanford.io/2wBB1Kf

148. An oft-quoted example of a DAO is given as an autonomous car which charges passengers for a journey. After dropping them off, it uses those profits to go to the charging station. See BBC News (2015) *Could driverless cars own themselves?* available at www.bbc.in/2IobMk5

149. These require *signatures* from *multiple* people in the DAO before transferring the funds or executing a transaction.

150. Blockonomi (2018) *What Is a DAO? Decentralized Autonomous Organizations & the Ethereum Hack*, available at www.blockonomi.com/what-is-a-dao/

151. The coding framework was developed open source by the Slock.it team but it was deployed under 'The DAO' name by members of the Ethereum community. CryptoCompare (2016) *The DAO, The Hack, The Soft Fork and The Hard Fork*, available at www.bit.ly/2uIbjEf

152. *ibid.*

153. For selecting projects to invest in, it relied on the ' wisdom of crowds' See CoinDesk (2019) *What is a DAO?*, available at www.coindesk.com/information/what-is-a-dao-ethereum

154. www.solardao.me/

155. Hedera (2019) *Governance*, available at www.hedera.com/council#governance

156. Blockonomi (2018) *What Is a DAO? Decentralized Autonomous Organizations & the Ethereum Hack*, available at www.blockonomi.com/what-is-a-dao/

157. Coindesk (2019) *What Is a DAO?*, available at www.bit.ly/2RIVkSS

158. Zduniak, M (2018) *Blockchain Legal Issues with DAOs*, available at www.bit.ly/2K1pXP0

159. Palmer, D (2019) *JPMorgan Expanding Blockchain Project With 220 Banks to Include Payments*, available at www.bit.ly/2INs6wD

160. JP Morgan (2018) *J.P. Morgan Interbank Information Network Expands to More than 75 Banks*, available at www.jpm.com/x/l/NFSbhzU?source=tw-share

161. JPMorgan added to Quorum a further layer of anonymity to transactions in which the sender may hide herself and the transactions recipients in a larger group of parties. Often though complex zero-knowledge proving schemes slows down blockchains because of computation power required.

162. Khatri, Y (2019) *Over 50 Banks, Firms Trial Trade Finance App Built With R3's Corda Blockchain*, available at www.bit.ly/2HXWZgR

163. ICO bench (2019) *ICO Market Reports*, available at www.bit.ly/2MyjJsj

164. European Securities and Markets Authority (2019) *Advice: Initial Coin Offerings and Crypto-Assets*, available at www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf

165. ICO bench (2019) *ICO Market Reports*, available at www.bit.ly/2MyjJsj

166. Thornton, S (2019) *Practical Applications of Decentralized Prediction Markets*, available at www.bit.ly/2HXsIia

167. Ozimek, A (2014) *The Regulation and Value of Prediction Markets*, available at www.bit.ly/2wEHu75

168. Kolková, A (2016) *Binary options as a modern Phenomenon of financial markets*, available at www.bit.ly/2KybKbS

169. Augur is based on the Ethereum blockchain. A market creator defines any topic, end date, and potential outcomes, plus an adjudicator if wanted. Trading (denominated in ETH) continues until the event-end, at which point Augur token holders (or designated reporter) determines the outcome. Token holders stake their Augur reputation token (REP) on the outcome and receive settlement fees.

170. Augur prediction markets have covered assassinations and terror attacks. Floyd, D (2018) *The First Augur Assassination Markets Have Arrived*, available at www.bit.ly/31awGLX

171. As has been noted, if decentralized prediction markets manage to achieve mass adoption, society will have the power to tap into and leverage the 'Wisdom of the Crowd' at unprecedented scale. Thornton, S (2019) *Practical Applications of Decentralized Prediction Markets*, available at www.bit.ly/2HXsIia; and Kung, S & Yi, M *et al* (2012) *The Wisdom of the Crowd in Combinatorial Problems*, available at www.bit.ly/2QO8ha9

172. Bloomberg (2018) *As Crypto meets prediction markets, U.S. regulators take notice*, available at www.bloom.bg/2n6rkyA

173. Augur though says that it is not a prediction market, but rather a protocol for (crypto-currency) users to create their own prediction markets and that users of the Augur protocol must themselves ensure that the actions they are performing are compliant with the laws in all applicable jurisdictions and must acknowledge that others' use of the Augur protocol may not be compliant. Users of the Augur protocol do so at their own risk.' Augur.net (2019) *FAQ*, available at www.augur.net/faq/

174. Mangu-Ward, K (2013) *The Death of Intrade*, available at http://reason.com/archives/2013/11/25/the-death-of-intrade

175. Adapted from Clark, J & Bonnea, J & Miller A *et al* (2014) *On Decentralizing Prediction Markets and Order Books*, available at www.bit.ly/2EWtzOc

176. See also Micheler, E & von der Heyde, L (2016) *Holding, Clearing and Settling Securities Through Blockchain Technology Creating an Efficient System by Empowering Asset Owners*, available at www.ssrn.com/abstract=2786972

177. The term 'HODLING' is used rather as a crypto-geared description of holding onto crypto-assets. It comes from a typographical error in a blog post by an author who meant to describe his holding of a crypto assets.

178. Renaudin, H (2019) *Why Institutions will not use Centralized Cryptocurrency Exchanges*, available at www.bit.ly/2Z65FY8

179. Coinmarketcap.com listed 258 exchanges/platforms as of May 31 2019

180. European Security and Capital Markets (2019) *Advice: Initial Coin Offering and Crypto-Assets*, available at www.bit.ly/2CXSjFc

181. Castor, A (2018) *Fast footwork: Binance has danced around regulations—and even moved itself—to run its exchange the way it wants*, available at www.bit.ly/2K21lpD

182. William-Grut, O (2018) *Crypto exchanges are charging up to $1 million per ICO to list tokens: 'It's pure capitalism'*, available at www.bit.ly/2HUfuCR

183. *See* www.coincap.io/ for latest market prices and volumes.

184. CryptoHype (2019) *Cryptocurrency Exchanges engaging in High-Level Wash Trading to fake Trade volumes*, available at www.bit.ly/2XAlSEA

185. Exchanges Binance, Bitfinex, Coinbase, Kraken, Bitstamp, BitFlyer, Gemini, itBit, Bittrex, and Poloniex are the only 10 exchanges with real trading volumes, with numbers that align more easily with related real-world statistics, including gross domestic product, wealth, web traffic and blockchain-related venture investments.

186. The US SEC's FinHub issued its analysis framework for digital investment contracts in May 2019. The new framework introduced 65 new tests that stress Howey's 'effort of others' component—akin to the famous Howey test for determining the provenance of a security and also introduced a completely new concept of 'active participants.' SEC (2019) *Statement on 'Framework for 'Investment Contract' Analysis of Digital Assets'*, available at www.bit.ly/2QP96jk

187. Baydakova, A & Hochstein, M (2019) *SEC's Crypto Czar Says Exchanges That List IEOs May Face Legal Risks*, available at www.coindesk.com/secs-crypto-czar-says-exchanges-that-list-ieo-tokens-may-face-legal-risks

188. Binance (2019) *Binance Launches DEX Testnet for the New Era of Peer-to-Peer Cryptocurrency Trading*, available at www.bit.ly/2NBkFZJ

189. It has online order matching, versus offline matching in centralized exchanges.

190. It integrates into crypto-asset wallets—hardware and software types—held by the user. Custodial exchanges may give better rates than non-custodial DEXs, but have additional wait times as they tend to process withdrawals in batches. There is however no inter-chain interoperability in between tokens: rather these DEXs 'peg' a token to a coin, with the peg's token interchangeable for the real crypto-currency.

191. Frankenfield, J (2018) *Atomic Swaps*, available at www.investopedia.com/terms/a/atomic-swaps.asp

192. *ibid.*

193. Noam, E (2019) *Macro-economics of crypto-currencies* (forthcoming).

194. Cambridge Associates (2019) *Cryptoassets: Venture into the Unknown*, available at www.bit.ly/31gadwY

195. For a summary of hacks, see Cermak, L (2019) *Research: Cryptocurrency exchange hacks surpass $1.3 billion all time; 61% coming from 2018*, available at www.bit.ly/2MqmV93

196. 2 keys may be used for some tokens: A spend key for moving assets around; and a staking key (warm) for governance

197. Legacy trades are usually settled T+2 (2 days after trade) while crypto assets can be settled in minutes and are irreversible.

198. Some custodians may work with sub custodian if don't want to work with specific tokens. There may also be cooperation between custodians in crypto-assets and traditional custodians.

199. Suberg, W (2018) *Main Swiss Stock Exchange to Launch Distributed Ledger-Based 'Digital Asset' Exchange*, available at www.cointelegraph.com/news/main-swiss-stock-exchange-to-launch-distributed-ledger-based-digital-asset-exchange

200. Elias, D (2019) *How Does Decentralized Finance Redefine Banking?*, available at www.bit.ly/2MxH795

201. Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purpose of money laundering or terrorist financing and amending Directives 2009/138/EC and 2013/36/EU. Available at www.bit.ly/2JUeq4w

202. Casey, M (2019) *The Cat-and-Mouse Game of Crypto Regulation Enters a New Phase*, available at www.bit.ly/31dnXZG

203. Watchtowers are third-parties that monitor the Bitcoin blockchain 24/7 on behalf of their clients. They identify and penalize malicious actors for cheating other users within channels and evaluate whether or not a participant in a Lightning channel has improperly broadcast a prior channel state, which could be used to reclaim funds after closing the channel with an invalid state. Curran, B (2019) *What Are Watchtowers in Bitcoin's Lightning Network?*, available at www.bit.ly/2WKPxht

204. Norton Rose Fulbright (2016) *Unlocking the blockchain: A global legal and regulatory guide—Chapter 1*, available at www.bit.ly/2QPntUK

205. *ibid.*

206. Dewey, J ed. (2019) *Blockchain Laws and Regulations | Laws and Regulations*, available at www.bit.ly/2wCOstg

207. Governing Council for the Hedera DLT for example consists of up to 39 organizations and enterprises, reflecting up to 18 unique industries globally. Council members are responsible for governing software changes. See www.hedera.com/council

208. Aki, J (2019) *Is this the End for Bitcoin SV? Price Plummets Following Controversy & Delistings*, available at www.bit.ly/2WqQ1d7

209. Xie, A (2019) *51% Attacks for Rent: The Trouble with a Liquid Mining Market*, available at www.bit.ly/2KrP113

210. Baldwin, C (2016) *Bitcoin worth $72 million stolen from Bitfinex exchange in Hong Kong*, available at http://reut.rs/2atByqe.

211. Compromised in the sense that data on the blockchain was altered without consensus of all the user nodes in the blockchain.

212. Hertig, A (2016) *The Blockchain Created by Ethereum's Fork is Forking Now*, available at www.bit.ly/2MtW5Nj

213. For public, permissionless (trustless) blockchains like Bitcoin where the use of nodes on the blockchain are publicly used to verify transactions is a core feature, security of its blockchain—and not the vaults bitcoins are stored in—is ensured by syntactic rules and computational barriers to mining. See also Greenspan (2016b) *ibid.*

214. There is arguably also a trade-off in DLTs between security and transaction processing speeds. For a technical discussion thereof, see Kiayias, A & Panagiotakos, G (2015) *Speed-Security Tradeoffs in Blockchain Protocols*, available at www.goo.gl/bgsTR8.

215. The counterargument could be that a properly designed 'permissioned' network would be designed so that there is no single-point of failure or central administrator who can unilaterally change the state. See Swanson (2015) *ibid.*

216. Credit Suisse (2016) *ibid.*; and Kaminska, I (2016) *How I Learned to Stop Blockchain Obsessing and Love the Barry Manilow*, available at www.goo.gl/mv3Lcy.

217. Sheikh, Y (2019) *Staking Is The New Mining—How People Make Money In Crypto These Days*, available at www.bit.ly/2WjrYbd

218. Metcalfe's Law says that the value of a network is proportional to the number of connections in the network squared. Shapiro, C & Varian, HR (1999) *Information Rules*. Similarly, per Paul Makin, the more people who have an identity on blockchain where nodes can attest to the authenticity of the correct people being identified, the more entities will take the trouble to be part of the acceptance network for that blockchain; that is, entities will join that blockchain to make use of the identity functionality it provides.

219. On the other hand, concentration of use in just one blockchain type could also possibly trigger competition-related issues.

220. Upgrading of a blockchain may require multiple consensus steps. For example, to upgrade the blockchain which Bitcoin uses requires a Bitcoin Improvement Proposal (BIP) design document for introducing new features since Bitcoin has no formal structure. See Anceaume, E *et al* (2016) *Safety Analysis of Bitcoin Improvement Proposals*, available at www.bit.ly/2EWD2Fd

221. Although there is no consensus on terminology, the various types of 'forks' that are generally possible have been classified by the Bitcoin community into forks, hard forks, soft forks, software fork or git fork. A hard fork, classified as a permanent divergence in the blockchain, commonly occurs when non-upgraded nodes can't validate blocks created by upgraded nodes that follow newer consensus rules. A fork is a regular fork where all nodes follow the same consensus rules, so the fork is resolved once one chain has more proof of work than another. A soft fork is a temporary divergence in the blockchain caused by non-upgraded nodes not following new consensus rules. A software fork is when one or more developers permanently develops a codebase—a collection of source code—separately from other developers. A git fork is when one or more developers temporarily develop a codebase separately from other developers. See Bitcoin (2016) *Hard Fork, Hard-Forking Change*, available at www.bit.ly/2WTaJ4I. However, other definitions may be used to describe the type of forks. For alternative classifications, and solutions to the identified forks, see Smith P & Atlas, K (2016) *A Brief History of Bitcoin Forks*, available at www.bit.ly/2ZgZ1yB

222. For example, the Cosmos Network, POS-based network that primarily aims to facilitate blockchain interoperability as the 'Internet of Blockchains' as well as the Polkadot Network. The protocols allow for the creation of new blockchains that are able to send transactions and messages between each other. See Fardi, O (2019) *How Proof Of Stake (POS) Algorithms 'Create Decentralized & Open Networks'*, available at www.bit.ly/2QTn9nL; and Kajpust, D (2018) *Blockchain Interoperability: Cosmos vs. Polkadot*, available at www.bit.ly/2WkgB2D

223. These records may in fact be encrypted.

224. Larcheveque, E (2018) *2018: A Record-Breaking Year for Crypto Exchange Hacks*, available at www.bit.ly/2KrIOT0

225. Simms, T (2019) *Gartner: Blockchain Tech Used by Enterprises at Risk of Becoming Obsolete Within 18 Months*, available at www.bit.ly/2QTko5T

226. Individuals have been passed the torch of leadership from a founder or foundations created by interested stakeholders may influence funding and development efforts. See Van Wirdum, A (2016) *Who Funds Bitcoin Core Development? How the Industry Supports Bitcoin's 'Reference Client'*, www.bit.ly/2tTcPlf; Lopp, J (2016) *Who Controls Bitcoin Core?* www.bit.ly/2IX90Wt; See also the Bitcoin Foundation at www.bit.ly/2K4rUdx

227. To be published in an upcoming paper in 2019 on 'Derisking and its Impact on Financial Inclusion' from the DFS Observatory at Columbia Institute of Tele-Information at Columbia Business School.r

228. Alexandre, A (2019) *Report: Blockchain and Crypto Firms in Malta Face Difficulty in Finding Banking Services*, available at www.bit.ly/2WMN2Lz

229. Aki, J (2019) *Is this the End for Bitcoin SV? Price Plummets Following Controversy & Delistings*, available at www.blockonomi.com/end-bitcoin-sv-price-plumments-delistings/

230. European Central Bank (2019) *Crypto-Assets: Implications for financial stability, monetary policy, and payments and market infrastructures*, available at www.bit.ly/2MroPWY

231. Wash trading is a process whereby a trader buys and sells a Crypto-currency for the express purpose of feeding misleading information to the market. CryptoHype (2018) *Cryptocurrency Exchanges engaging in High-Level Wash Trading to fake Trade volumes*, available at www.bit.ly/2IpIjpN

232. Exchanges Binance, Bitfinex, Coinbase, Kraken, Bitstamp, BitFlyer, Gemini, itBit, Bittrex, and Poloniex are the only 10 exchanges with real trading volumes, with numbers that align more easily with related real-world statistics, including gross domestic product, wealth, web traffic and blockchain-related venture investments.

233. Haene, P (2009) *Optimal Central Counterparty Risk Management*, available at www.bit.ly/2Wt3OA5

234. Blockchain is designed to operate a single distributed ledger in a decentralized manner over a trustless peer-to-peer network but kept reliable through the utilization of cryptographic proofs and a consensus mechanism to reach global agreement as to transactions to be entered into the ledger.

235. Fischer, M & Lynch, N & Paterson, M (1985) *Impossibility of Distributed Consensus with One Faulty Process*, www.groups.csail.mit.edu/tds/papers/Lynch/jacm85.pdf; Gilbert, S & Lynch, N (2002) Brewer's Conjecture and the Feasibility of Consistent, available at http://awoc.wolski.fi/dlib/big-data/GiLy02-CAP.pdf; NULS (2019) *Why it is Impossible to Solve Blockchain Trilemma?*, available at www.bit.ly/2W7Dkzt; See also Kleppmann, M (2015) *A Critique of the CAP Theorem*, www.bit.ly/2W2h0XN

236. Shah, A & Viswanathan, S (2018) *The Scalability Trilemma in Blockchain*, www.bit.ly/2Y3dEpb

237. Portions of the sections that follow are drawn from Perlman, L (2017) *Distributed Ledger Technologies and Financial Inclusion*, available at www.bit.ly/2nyxpBG; Perlman, L (2017) *Security Aspects of Distributed Ledger Technologies* (forthcoming); and Perlman, L (2012) *Doctoral Thesis: Legal and Regulatory Aspects of Mobile Financial Services*, available at https://papers.ssrn.com/abstract=3174463

238. European Securities and Markets Authority (2019) *Advice: Initial Coin Offerings and Crypto-Assets*, available at www.bit.ly/2IrYNOp; and Cambridge Judge Business School (2019) *2nd Global Cryptoasset Benchmarking Study*, available at www.bit.ly/2WcQlqS

239. This may be undertaken using internationally recognized banking principles such as those put forward by the BIS. See generally www.bis.org.

240. See E Avgouleas (2008) *Financial Regulation, Behavioural Finance, and the Global Credit Crisis: In Search of a New Regulatory Model*, available at www.bit.ly/2ZgZL6R; S Agarwal *et al* (2009) *The Age of Reason: Financial Decisions over the Life-Cycle with Implications for Regulation*, available at www.bit.ly/2WNqPNf; SJ Friedman (1984) *A New Paradigm for Financial Regulation: Getting from Here to There*, available at www.bit.ly/2MxAvI2.

241. Breyer, S & MacAvoy, Paul W (1987) *Regulation and Deregulation*, Milgate, M & Newman, P (eds) *The New Palgrave: A Dictionary of Economics*. As Lee notes, government's' duty to safeguard the public interest can be traced to 1690 when John Locke said that governments are able impartially to distinguish between outcomes that are in the public interest and those that are not and, furthermore, are possessed of sufficient information and wisdom to determine the optimal form and level of regulation. See J Locke (1690) *The Second Treatise Concerning Civil Government*, available at www.bit.ly/2WNH1hD; and also Lee, B.C (2002) *Regulation in the New Economy*, available at www.bit.ly/2Z7pajh,

242. RW Hahn (2006) *Theories of Regulation and Deregulation: A Critical Appraisal*, available at www.goo.gl/smnWm; Public Utility Research Center (2011) *Theories of Regulation*, available at www.goo.gl/slr9b; Stiglitz, J E (2009) *Government Failure vs. Market Failure: Principles of Regulation*, available at www.bit.ly/2Kxs90r; see Hertog, J den (1999) *General Theories of Regulation*, available at www.bit.ly/2MtWKyh

243. The positive theories attempt economic explanations of regulation and derive the consequences of regulation. They are said to include theories of market power, interest group theories that describe stakeholders interests in regulation, and theories of government opportunism that describe why restrictions on government discretion may be necessary for the sector to provide efficient services for customers. In general, the conclusions of these theories are that regulation occurs because the government is interested in overcoming information asymmetries with the operator and in aligning the operator's interest with the government's interest; customers desire protection from market power when competition is non-existent or ineffective; operators desire protection from rivals; or operators desire protection from government opportunism.

244. They are called normative because there is usually an implicit assumption that efficient regulation would also be desirable. These theories are said to generally conclude that regulators should encourage competition where feasible, minimize the costs of information asymmetries by obtaining information and providing operators with incentives to improve their performance, provide for price structures that improve economic efficiency, and establish regulatory processes that provide for regulation under the law and independence, transparency, predictability, legitimacy, and credibility for the regulatory system.

245. Similarly, the questions could be phrased as how to fix it? and the form that the solution or fix will take.

246. Regulation can be taken to mean the use of legal instruments for the implementation of social-economic policy objectives.

247. The risk includes balancing the dual objectives of identification and traceability to allow financial integrity.

248. Market failures are departures from the economist's notion of a perfectly efficient market where first, consumers and producers take decisions that reflect all possible, relevant information; secondly, prices reflect all costs, including costs to third parties; and thirdly, firms cannot profitably charge prices in excess of marginal cost, ie where their market power is absent. See Financial Services Authority (FSA) (2006) *A Guide to Market Failure Analysis and High Level Cost Benefit Analysis*, available at www.bit.ly/2EQiYV9

[249] Economists and economic theory greatly affect this debate, to which Keynes caustically remarked that Practical men, who believe themselves to be quite exempt from any intellectual influences, are usually the slaves of some defunct economists. See JM Keynes (1964) *The General Theory* at 383. Economists then especially see the debate of the varying functions of government regulation versus market regulation framed, *inter alia*, by Arthur Pigou who believed that government is assumed to be a neutral arbiter in providing regulation in response to the demand of the public for the correction of inefficient, fragile or inequitable market practices. This contrasts with the economist Ronald Coase who believed that efficient outcomes could be generated without government intervention when property rights are clearly defined. He is said to have invented the field of Law and Economics, also known as the Economic Analysis of Law which is said to differ from other forms of legal analysis in looking at efficiency and incentives. A component thereof is the Positive Theory of legal efficiency which believes that the common law is efficient, while the Normative Theory says that that the law should be efficient. Most economists accept both. Coase believed thereto that markets are more efficient than courts, but when possible, the legal system will force a transaction into the market. When this is impossible however, the legal system attempts to mimic a market and guess at what the parties would have desired if markets had been feasible. See further L Zingales (2004) *The Costs and Benefits of Financial Market Regulation*, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=536682

[250] The public interest approach says that the notion of externalities serves to define the proper role of government and emphasizes the government's role in correcting market imperfections that result from externalities. In this view, regulatory agencies may or may not be well informed, but they are well intentioned. See SE Woodward (1998) Regulatory Capture at the U.S. Securities and Exchange Commission Sand Hill Econometrics Working Paper, available at www.goo.gl/um9Hh. See also Winn who notes that political scientists and economists distinguish between economic regulation aimed at supporting competition in markets and social regulation aimed at protecting the health and safety. Winn notes further that consumer protection laws are now treated as a form of economic regulation in the US insofar as government intervention is appropriate only when it is clear that competition is not doing an adequate job of meeting consumer needs. By comparison, Winn notes further that European Union (EU) lawmakers appear to be skeptical that mere economic regulation provides enough support for online consumer markets in Europe. Winn, J & Webber, M (2006) *The Impact of EU Unfair Contract Terms Law on U.S. Business-to-Consumer Internet Merchants*, available at www.bit.ly/2WjUd9H

[251] Rubin says that legal rules, especially those in the commercial area, are instruments of social policy rather than an autonomous body of doctrine reflecting general and apolitical principles of law. See Rubin, R (1991) *Efficiency, Equity and the Proposed Revision of Articles 3 and 4 42 Albany Law Review* 551 at 553-4, 560, available at www.bit.ly/2K0MoUP

[252] Since network industries like payments can provide socially important or utility services to the public and the economy, they may need to address broad public policy agendas over and above supporting effective competition, such as financial stability and consumer protection.

[253] Over-regulation may occur when the cost of ensuring equality of information for both provider and consumer reduces the availability of products and services in the market and/or drives prices higher.

[254] See Rubin who analyses market failure generated by the structure of the legal system where he says consumers will never be able to enforce their rights against a bank because it is too expensive to do so. Consumers must initiate any legal action, but invariably the action—especially for smallish amounts—cannot be economically pursued. The only thing, he says, that is economically more inefficient than failing to bring an action is when the consumer has an unjustified loss and initiates an action to recover that loss at large expense to himself and possibly costing more to pursue to recover that loss than the initial monetary loss. This, he believes, is effectively a market failure.

[255] Indeed, the UK Department for Business, Innovation and Skills overall regulatory policy is framed by them as being less regulation, better regulation and regulation as a last resort. See United Kingdom, Department for Business, Innovation and Skills (2010) *Reducing Regulation Made Simple*, available at www.bit.ly/31gc0SI. The EU, especially because of its vast constituency and membership, undertakes vast series of consultations, often extending the time frames for the implementation of new rules.

[256] The Regulatory Capture theory was developed by Stigler, outlined in Stigler, G (1971) *The Economic Theory of Regulation*, available at www.goo.gl/CY63C

[257] The influence may be at political and staffing levels. The desire for strict regulation does not stem from the advantage incumbents might gain from restricted competition, but from the risk shifting and moral hazard phenomena that are endemic in financial systems.

[258] There may also be a presumption in regulatory theory that commercial law—both private and state rules—should do for parties what they would otherwise have done for themselves. See Gillette, C & Walt, S (2008) *Uniformity and Diversity in Payment Systems*, available at www.bit.ly/2WjW12g.

[259] This may occur in instances of error resolution, where there maybe mistake by one party in a payment, or fraud visited upon a party. For a consumer perspective on the impact of private rules versus public rules, see Budnitz, M E (2008) *Technology as the Driver of Payment System Rules: Will Consumers be Provided Seatbelts and Air Bags?*, available at https://scholarship.kentlaw.iit.edu/cgi/viewcontent.cgi?article=3678&context=cklawreview.

[260] Thaler, T & Sunstein, C (2003) *Libertarian Paternalism* 93(2) *The American Economic Review* 175-179

[261] All information in this section is adapted from Perlman, L (2012) *Doctoral Thesis: Legal and Regulatory Aspects of Mobile Financial Services*, available at https://papers.ssrn.com/abstract=3174463

[262] For example, banks and nonbanks providing the service.

[263] European Securities and Markets Authority (2019) *Advice on Initial Coin Offerings and Crypto-Assets*, available at www.bit.ly/2CXSjFc

[264] In the EU for example, if a service is identified as settlement platform for example, other requirements may then be trigged in so far as they may need to be an institution, a central counterparty, a settlement agent, a clearing house or a system operator. European Securities and Markets Authority (2019) *Advice on Initial Coin Offerings and Crypto-Assets*, available at www.bit.ly/2CXSjFc The system and its participants would also need to comply with the settlement periods and settlement discipline requirements prescribed

[265] In the crypto-world speak, the 'disappearance' of the founder of a protocol or dApp is known as moon rot, after a successful launch of the product 'Moonshot'

[266] European Securities and Markets Authority (2019) *Advice on Initial Coin Offerings and Crypto-Assets*, available at www.bit.ly/2CXSjFc

[267] Australian Securities and Investments Commission (2019) *ASIC updates information for businesses on ICOs and crypto-asset*, available at www.bit.ly/2wr5HNZ

[268] Cambridge Judge Business School (2019) *2nd Global Cryptoasset Benchmarking Study*, available at www.bit.ly/2WcQlqS

[269] Unless of course the end customer's jurisdiction does not allow the customer to do so. ICOs for example are usually geo-restricted for US-based persons and/or citizens because of the US SEC's effective ban on ICOs in their current form.

[270] For a survey of the nomenclature used, see Cambridge Judge Business School (2019) *2nd Global Cryptoasset Benchmarking Study*, available at www.bit.ly/2WcQlqS

[271] Mahoney, P & Rauterberg, G (2017) *The Regulation of Trading Markets: A Survey and Evaluation*, available at https://corpgov.law.harvard.edu/2017/05/05/the-regulation-of-trading-markets-a-survey-and-evaluation/.

[272] European Securities and Markets Authority (2019) *Advice: Initial Coin Offerings and Crypto-Assets*, available at www.bit.ly/2CXSjFc

[273] In the US, they are regulated either as a Limited Purpose Trust Company such as a bank which cannot lend to its client but can store their funds, for example the Gemini and ItBit exchanges, or as a Money Transmitter—as a Money Service Business—whereby it is a company which transmits funds from one client to another, for example Coinbase and BitFlyer US. Recent FinCen guidance tightens the rules around MSBs, capturing additional crypto business models as being regulated. Crypto-currency exchanges operating in New York or providing services to New York state residents must register with the NY Department of Financial Services and obtain a BitLicense. Only 14 licenses have been issued since the regulation was introduced in 2015. See further Rohr, J & Wright, A (2017) B*lockchain-Based Token Sales, Initial Coin Offerings, and the Democratization of Public Capital Markets*, available at www.ssrn.com/abstract=3048104.

[274] Zmudzinski, A (2019) *Cryptocurrency Exchange OKEx Decides Not to Delist Bitcoin Satoshi Vision*, available at www.cointelegraph.com/news/cryptocurrency-exchange-okex-decides-not-to-delist-bitcoin-satoshi-vision

[275] Rohr, J & Wright, A (2017) *Blockchain-Based Token Sales, Initial Coin Offerings, and the Democratization of Public Capital Markets*, available at www.ssrn.com/abstract=3048104

[276] Lee, G & Yiu, E (2018) *Crypto-currency rules to be unveiled by SFC as Hong Kong aims to become major trading hub*, available at www.bit.ly/2WT1XUg

[277] They may have superior back-office and administrator applications for undertaking reconciliations an auditing as well as KYC/AML functionality.

[278] For example, remote KYC providers who the platforms connect to via APIs.

[279] The 'crypto-winter of 2018 and the collapse of crypto-asset process to doms exchanges ultimately closing down, with similar effects following coordinate hacks of and theft from the exchanges

[280] European Securities and Markets Authority (2019) *Advice: Initial Coin Offerings and Crypto-Assets*, available at www.bit.ly/2CXSjFc: While these issues are not unique to crypto-assets trading platforms they may be exacerbated in the case of crypto-assets because of their high price volatility and often low liquidity.

[281] The Binance crypto-to-crypto exchange for example said it covered customer losses from its own 'Secure Asset Fund for Users' after it was hacked in May 2019. Zhao, W (2019) *Binance Considered Pushing for Bitcoin 'Rollback' Following $40 Million Hack*, available at www.coindesk.com/binance-may-consider-bitcoin-rollback-following-40-million-hack

[282] CFI Code is the code for classifying financial instruments in order to identify the type and characteristics of each financial instrument in accordance with international standards. The International Standard Organization (ISO) has established and maintained the CFI Code. See www.tfiic.org/SiteContent/TH/Info/CFI%20Code_EN.pdf

[283] For example, on transaction volume and type reporting, instrument reference data, and orderbook data.

[284] ClearIt (2015) *SIX Interbank ISO 4217: A controversial standard*, available at http://bit.ly/2Mz9HqR

[285] Pauw, C (2019) *Insured Cryptocurrency Custody Services and Their Potential Impact: The Key to Institutional Investment Growth?*, available at www.bit.ly/31drreI

[286] Avgouleas, E & Kiayias, A (2018) *The Promise of Blockchain Technology for Global Securities and Derivatives Markets: The New Financial Ecosystem and the 'Holy Grail' of Systemic Risk Containment* (December 6, 2018). Edinburgh School of Law Research Paper No. 2018/43, available at www.ssrn.com/abstract=3297052

[287] European Securities and Markets Authority (2019) *Advice: Initial Coin Offerings and Crypto-Assets*, available at www.bit.ly/2CXSjFc; Wight

[288] Cointelegraph (2019) *Insured Cryptocurrency Custody Services and Their Potential Impact: The Key to Institutional Investment Growth?*, available at www.bit.ly/2Mz9HqR

289. Avgouleas, E & Kiayias, A (2018) *The Promise of Blockchain Technology for Global Securities and Derivatives Markets: The New Financial Ecosystem and the 'Holy Grail' of Systemic Risk Containment* (December 6, 2018). Edinburgh School of Law Research Paper No. 2018/43, available at www.ssrn.com/abstract=3297052

290. Here there is an important distinction between STOs and tokenized securities. The former is natively crypto, the latter are simply crypto wrappers of a legacy asset.

291. There is no harmonized definition of safekeeping and record-keeping of ownership of securities at EU-level and the rules also depend on whether the record-keeping applies at the issuer level (notary function) or investor level (custody/safekeeping function). European Securities and Markets Authority (2019) *Advice: Initial Coin Offerings and Crypto-Assets*, available at www.bit.ly/2CXSjFc

292. As noted by the European Securities and Markets Authority, ESMA See European Securities and Markets Authority (2019) *Advice: Initial Coin Offerings and Crypto-Assets*, available at www.bit.ly/2CXSjFc, these requirements may also apply in relation to the initial recording of securities in a book-entry system (notary service), providing and maintaining securities accounts at the top tier level (central maintenance service), or providing, maintaining or operating securities accounts in relation to the settlement service, establishing CSD links, collateral management.

293. European Securities and Markets Authority (2019) *Advice: Initial Coin Offerings and Crypto-Assets*, available at www.bit.ly/2CXSjFc

294. It classifies digital assets as having the same legal status as money- with its 'super-negotiability' rules—under commercial law, allowing crypto-asset lending businesses as transfers are free and clear of for example, liens. It also means that a crypto-asset would have independent legal status, that is without the involvement of an intermediary. See Manning, L (2019) *Wyoming Passes New Friendly Regulations for Crypto Assets*, available at www.bit.ly/2KrK4FI

295. EveryCRSReport (2012) *Supervision of U.S. Payment, Clearing, and Settlement Systems: Designation of Financial Market Utilities (FMUs)*, available at www.everycrsreport.com/reports/R41529.html

296. In many jurisdictions and following BIS leads, FMIs must maintain certain standards with respect to risk management and operations, have adequate safeguards and procedures to protect the confidentiality of trading information, have procedures that identify and address conflicts of interest, require minimum governance standards for boards of directors, designate a chief compliance officer, and disseminate pricing and valuation information.

297. European Securities and Markets Authority (2019) *Advice: Initial Coin Offerings and Crypto-Assets*, available at www.bit.ly/2CXSjFc

298. UN (1996) *UNCITRAL Model Law on Electronic Commerce (1996) with additional article 5 bis as adopted in 1998 and Guide to Enactment*, available at www.bit.ly/2WMP3Y9

299. It governs the validity of e-signatures and grants legally binding status to electronic records and signatures, ensuring the enforceability of electronic transactions. The US federal version is the 'Electronic Signatures in Global and National Commerce Act which validates the use of electronic records and signatures in place of physical documents. Beckham, J & Rosenbaum, A & Sendra, M (2018) *Smart Contracts Lead the Way to Blockchain Implementation*, available at www.bit.ly/2UcGk0L

300. Zetzsche, D & Buckley, R & Arner, D (2018) *The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain*, available at www.illinoislawreview.org/print/vol-2018-no-4/the-distributed-liability-of-distributed-ledgers

301. For holding coders liable as fiduciaries, see Walch, A (2019) *Deconstructing 'Decentralization': Exploring the Core Claim of Crypto Systems*, available at www.bit.ly/2YHoe5R.

302. On regulatory sandboxes, see Wechsler, M; and Perlman, L and Gurung, N (2018) *The State of Regulatory Sandboxes in Developing Countries*, available at www.ssrn.com/abstract=3285938

303. See **Section 7.3.2** on India.

304. BunnyPub (2019) *Staking Is the New Mining—How People Make Money in Crypto These Days*, available at www.bit.ly/2KvRaJm

305. Blandin, A & Cloots, A S & Hussan, H et. al. (2019) *Global Cryptoasset Regulatory Landscape Study*, available at www.bit.ly/2JWDbvM

306. For an outline of DFS and its regulatory impact, see Perlman, L (2018) *An Introduction to Digital Financial Services (DFS)*, available at https://papers.ssrn.com/abstract=3370667

307. European Securities and Markets Authority (2019) *Advice: Initial Coin Offerings and Crypto-Assets*, available at www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf; and Cambridge Judge Business School (2019) *2nd Global Cryptoasset Benchmarking Study*, available at www.bit.ly/2WcQlqS

308. Zetzsche, D & Buckley, R & Arner, D (2018) *The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain*, available at www.illinoislawreview.org/print/vol-2018-no-4/the-distributed-liability-of-distributed-ledgers

309. For holding coders liable as fiduciaries, see Walch, A (2019) *Deconstructing 'Decentralization': Exploring the Core Claim of Crypto Systems*, available at www.bit.ly/2YHoe5R.

310. Some features of the POW consensus include: New transactions are broadcast to all nodes; Each node collects new transactions into a block; Each node works on finding a difficult proof-of-work for its block; When a node finds a proof-of-work, it broadcasts the block to all nodes; Nodes accept the block only if all transactions in it are valid and not already spent; Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash; Nodes always consider the longest chain to be the correct one and will keep working on extending it. All from Consensus achieved using Proof-of-Work, available at www.bit.ly/2Im0BIw

[311] Nadeem, S (2018) *How Bitcoin mining really works*, available at www.bit.ly/2Ky1Ren

[312] Hashing is generating a value or values from a string of text using a mathematical function, enabling security during the process of message transmission when the message is intended for a particular recipient only. A formula generates the hash, which helps to protect the security of the transmission against tampering. From Techopedia (2019) *Hashing*, available at www.bit.ly/31dsco4

[313] Which may be payable in unused currency held in reserve by the system in additional to optional user fees.

[314] Tayo, A (2017) *Proof of work, or proof of waste?*, available at www.bit.ly/2ur4k0R

[315] The 'proof of work' concept' originates from early attempts to throttle email spammers by creating an artificial cost to the sender for each email sent, akin to affixing the cost of a postage stamp on each email. At lower levels the greater effort expended by the email sender is negligible, but costs become substantial at higher volumes, making the cost spam financially unattractive to the mass e-mailer. See Back, A (2002) *Hashcash—A Denial of Service Counter-Measure*, available at www.hashcash.org/papers/hashcash.pdf; Microsoft (2016) *[MS-OXPSVAL]: Email Postmark Validation Algorithm*, available at www.bit.ly/2FwjoAO.

[316] Hashing power is the power that a computer uses to run and solve different 'hashing' algorithms. These algorithms are used for generating new blocks on a blockchain. NiceHash (2019) *What is hashing power and why would anyone buy it?*, available at www.bit.ly/2QX4oA4

[317] As of April 2019, it would require an investment of at least USD 300,000 to rent equipment to potentially have 51% computational power of the entire Bitcoin network.

[318] Cryptoline (2019) *Peercoin uses a combination of POW and POS*. See Peercoin: A coin combining both POW with POS algorithms, available at www.bit.ly/2MzaJTL

[319] Sharma, A (2018) *Understanding Proof of Stake through its Flaws. Part 2—'Nothing's at Stake'*, available at www.bit.ly/2ESw5oz

[320] POS mechanisms vary. Systems add and factor into the computation different weighting measures in an attempt at best measuring the honesty of a forger based upon objective qualifications which identify signs of trust. One example is Peercoin which factors in 'coin age'—the time in which a coin is held or at stake. Zheng, Z; Xie, S *et al* (2017) Blockchain Challenges and Opportunities: A Survey, available at www.bit.ly/2JCt6pn; Bitfallscom (2018) *Peercoin Explained: The Proof of Stake Pioneer*, available at www.bitfalls.com/2018/03/11/peercoin-explained-proof-stake-pioneer/; and the *Peercoin Whitepaper* at www.peercoin.net/whitepapers/peercoin-paper.pdf

[321] A simple example calculates as a validator with 2% tokens at stake translates into being able to validate 2% of transactions In many systems one can only stake a percentage of coins they hold, e.g. 22% which means holding 100 coins allows a maximum of 22 to be staked and also incentivizing the holder to keep a higher amount invested in the system's currency. See Martinez, J (2018) *Understanding Proof of Stake: The Nothing at Stake Theory*, available at www.bit.ly/2I1iRrT

[322] www.medium.com/coinmonks/understanding-proof-of-stake-the-nothing-at-stake-theory-1f0d71bc027

[323] Peercoin (2018) *POS reward, coin age and minting time*, available at www.bit.ly/2HZiePg

[324] This uses a hybrid POW and POS. See www.blackcoin.org/blackcoin-pos-protocol-v2-whitepaper.pdf

[325] Caspar currently consists of two variants which will ultimately become one finalized version for the update. Oliver, D (2018) *Beginner's Guide to Ethereum Casper Hardfork: What You Need to Know*, available at www.bit.ly/2WTdrHq

[326] This is the amount of their stake/ownership of a crypto-currency/token.

[327] Kravchenko, P (2017) *Consensus Explained*, available at www.bit.ly/2WmHPWk

[328] Major, R (2018) *Proof-of-Stake (POS) outperforms Bitcoin's Proof-of-Work (POW)*, available at www.bit.ly/2K0O3d1

[329] Baliga, A (2017) *Understanding Blockchain Consensus Models*, available at www.bit.ly/2K8nfaT

[330] PoET is now the consensus model of choice for Hyperledger Sawtooth's modular framework

[331] Memon, B (2019) *Guide to Stablecoin: Types of Stablecoins & Its Importance*, available at www.bit.ly/2wFCKOx

[332] J.P. Morgan (2019) *J.P. Morgan Creates Digital Coin for Payments*, available at www.bit.ly/2WuhDOw

[333] CoinDesk (2019) *Facebook in Talks to Build Ecosystem for Planned Stablecoin: WSJ*, available at www.bit.ly/2XukUtK

[334] DGX is based on the Proof-of-Provenance algorithm where each gold bar is secured and its ownership/custodianship status is tracked accurately on the Ethereum blockchain.

[335] MakerDAI, for example, is an ERC-20 project which does not rely on a centralized entity or third party since it lives completely on the blockchain. It aims to achieve price stability through an autonomous system of smart contracts—called Collateralized Debt Position (CDP)—that responds to varying market dynamics. To create new coins, Ether (ETH) must be used as collateral and sent to the CDP, which will lock the staked ETH and new DAI's will be minted.

[336] As the total demand for the coins increases, new supply of Stablecoins are created to reduce price back to stable levels. The main objective is to get the coin's price as close as possible to USD 1.

[337] Blandin, A & Cloots, A S & Hussan, H et. al. (2019) *Global Cryptoasset Regulatory Landscape Study*, available at www.bit.ly/2JWDbvM

338. Kenyan Wall Street (2018) *Kenya Govt unveils 11 Member Blockchain & AI Taskforce headed by Bitange Ndemo*, available at www.bit.ly/2ELFXRj; Macharia (2018) *Bitange Ndemo to head task force on block chain and artificial intelligence*, www.bit.ly/29GHuMY

339. Mumo, I (2018) *Kenya Blockchain Taskforce Considers Regulated Digital Currency*, available at www.bit.ly/2HO1muZ/; Muiruri, K (2018) *Blockchain taskforce mulls regulated digital currency*, available at www.bit.ly/2wx0vYZ; Bitcoin Exchange Guide (2018) *Kenyan Distributed Ledgers and Artificial Intelligence Chairman Suggests Tokenizing Local Economy*, available at www.bit.ly/2ELr5SP

340. During a meeting between Kenyan ICT ministry stakeholders and members of the private sector in September 2018, task force chairman, Bitange Ndemo, was quoted as stating the following: 'We must begin to tokenize the economy by giving incentives to young people to do things which they are paid through tokens that can be converted to fiat currency.' Aru, I (2018) *Kenya's Blockchain Task Force Advises Gov't to Replace Cash With Digital Currency*, available at www.yhoo.it/2WmgyIH; Alexandre, A (2018) *Kenya: DLT and AI Task Force Chairman Calls on Government to Tokenize Economy*, available at www.bit.ly/2QZVSQo; Bitcoin Exchange Guide (2018) *Kenyan Distributed Ledgers and Artificial Intelligence Chairman Suggests Tokenizing Local Economy*, *ibid.*

341. www.kictanet.or.ke/?p=39983

342. CBK (2015) *Banking Circular No 14 of 2015: Virtual Currencies—Bitcoin*, available at www.bit.ly/2Mm9Ei1; CBK (2015) *Caution to the Public on Virtual Currencies such as Bitcoin*, available at www.bit.ly/1Ot0GE5

343. High Court of Kenya at Hairobi, Human Rights Division (2015) *Petition No. 512 of 2015, Lipisha Consortium Limited and Bitpesa Limited v. Safaricom Limited*, available at www.kenyalaw.org/caselaw/cases/view/117270/

344. CMA (2019) *CMA warns against Kenicoin initial coin offering and trading*, www.bit.ly/2W24xYH

345. SARB (2019) *Virtual Currencies/Crypto-currencies*, available at www.bit.ly/2qSFHZg

346. SARB appears to be engaging in regulatory forbearance and has stated that it is monitoring the emergence and development of virtual and crypto currencies. SARB (2019) *Virtual Currencies/Crypto-currencies*, *ibid.*

347. SARB (2014) *Position Paper on Virtual Currencies*, available at www.bit.ly/1NvvlVA

348. They can act as a 'digital representation of value that can be digitally traded and functions as a medium of exchange, a unit of account and/or a store of value…' SARB (2014) *Position Paper on Virtual Currencies*, *ibid.*

349. SARB (2019) *Virtual Currencies/Crypto-currencies*, available at www.bit.ly/2qSFHZg

350. SARB (2018) *Project Khoka: Exploring the use of distributed ledger technology for interbank payments settlement in South Africa*, available at www.bit.ly/2kSfEOK

351. SARS reasoned that since cryptocurrencies are not considered legal tender nor widely accepted for payments, accordingly they should not be treated as a currency for purposes of income tax and capital gains tax. SARS (2018) *SARS'S Stance on the Tax Treatment of Cryptocurrencies*, available at www.bit.ly/2WzkTYk

352. The IFWG consists of members from the FIC, FSCA, NT, SARS and SARB. SARB (2019) *Statement on crypto assets*, available at www.tinyurl.com/y6x26men

353. IFWG (2018) *IFWG Fintech Workshop April 19-20, 2018*, available at www.bit.ly/2XgZeB6

354. IFWG (2019) *IFWG Consultation Paper on Policy Proposals for Crypto Assets*, available at www.bit.ly/2Kgy0a1

355. 'Crypto assets are digital representations or tokens that are accessed, verified, transacted, and traded electronically by a community of users. Crypto assets are issued electronically by decentralised entities and have no legal tender status, and consequently are not considered as electronic money either. It therefore does not have statutory compensation arrangements. Crypto assets have the ability to be used for payments (exchange of such value) and for investment purposes by crypto asset users. Crypto assets have the ability to function as a medium of exchange, and/or unit of account and/or store of value within a community of crypto asset users.' IFWG (2018) *IFWG Fintech Workshop April 19-20, 2018*, *ibid.*

356. Other relevant regulators include the China Securities Regulatory Commission (handling the illegal issuance of securities), Cyberspace Administration of China (monitoring crypto-assets of online entities), Ministry of Industry and Information Technology (terminates unlawful websites), the Ministry of Public Security (prohibits and enforces criminal actions for unlawful activities).FSB (2019) *Crypto Assets Regulators Directory*, www.fsb.org/wp-content/uploads/P050419.pdf

357. PBC (2013) *Notice of the China Securities Regulatory Commission of the China Banking Regulatory Commission of the Ministry of Industry and Information Technology of the People's Bank of China on Preventing Bitcoin Risk*, available at www.bit.ly/2ZcXUjj (alternatively a reproduction of the notice can be viewed at www.cybtc.com/article-421-1.html); Blandin, A & Cloots, A S & Hussan, H et. al. (2019) *Global Cryptoasset Regulatory Landscape Study*, available at www.bit.ly/2JWDbvM

358. PBC (2017) *Announcement of the Banking Regulatory Commission, the Securities Regulatory Commission and the Insurance Regulatory Commission of the General Administration of Industry and Commerce, the Ministry of Industry and Information Technology, the Central Network of the People's Bank of China on preventing the risk of issuing and financing tokens*, available at www.pbc.gov.cn/goutongjiaoliu/113456/113469/3374222/index.html

359. In addition to the PBC, the release included the Cyberspace Administration of China (CAC), the Ministry of Industry and Information Technology (MIIT), the State Administration for Industry and Commerce (SAIC), the China Banking Regulatory Commission (CBRC), the China Securities Regulatory Commission (CSRC), and the China Insurance Regulatory Commission (CIRC).

360. Mullany, G (2013) *China Restricts Banks' Use of Bitcoin*, available at www.nyti.ms/2ENIZXB; Hill, K (2013) *Bitcoin in China: The Fall-out From Chinese Government Banning Real World Use*, available at www.bit.ly/2wwtFYp

361. PBC (2018) *Continued efforts to prevent ICO and virtual currency trading risks*, available at www.bit.ly/2MAEvYa and www.bit.ly/31emMsL

362. Huang, E (2018) *China is now policing crypto-currency by targeting WeChat accounts*, available at www.bit.ly/2EKX2L3; CAC (2018) *Interim Provisions on the Development Management of Public Information Services for Instant Messaging Tools*, available at www.cac.gov.cn/2014-08/07/c_1111983456.htmT; The shutdown was also implemented via notices in Beijing's Chaoyang district. Huang, Z (2018) *China shuts down blockchain news accounts, bans hotels in Beijing from hosting crypto-currency events*, available at www.bit.ly/2QGqd6Q

363. Linver, H (2019) *Paying the Price: WeChat Merchants Banned From Crypto Payments*, available at www.bit.ly/2W40SsA; CAC (2019) *Interim Provisions on the Development Management of Public Information Services for Instant Messaging Tools*, available at www.cac.gov.cn/2014-08/07/c_1111983456.htm

364. Bitcoin Exchange Guide (2018) *China's DCEP Cryptocurrency: Digital Currency Electronic Payment?*, available at www.bit.ly/2wB73pr; TrustNotes (2018) *China Working on a Digital Currency Electronic Payment, DCEP*, available at www.bit.ly/2JSiou6;

365. Li, C (2019) *China, a Major Bitcoin Source, Considers Moving Against It*, available at www.nyti.ms/2I94GCc; Chen, J & Ren, X (2018) *PBOC gets tougher on bitcoin*, available at www.bit.ly/2MmBKcP; Russel, J (2019) *China is reportedly moving to clamp down on bitcoin miners*, available at www.tcrn.ch/2VZTTg8; Huang, Z (2019) *China, home to world's biggest cryptocurrency mining farms, now wants to ban them completely*, available at www.bit.ly/2YYseyW

366. Zhao, W (2019) *China's Economic Planning Body Labels Bitcoin Mining an 'Undesirable' Industry*, available at www.nyti.ms/2I94GCc; Barber, G (2019) *China Says Bitcoin is Wasteful. Now it Wants to Ban Mining*, available at www.bit.ly/2v3HBII; Huang, Z (2019), *ibid.*

367. CAC (2019) *Administrative Provisions on Blockchain Information Service*, available at www.bit.ly/2KkDVet; Library of Congress (2019) *China: Rules on Blockchain-Based Information Services Issued Requiring Authentication of Users' Real Identities*, available at www.bit.ly/2JPMX3u

368. FSB (2019) *Crypto Assets Regulators Directory*, www.fsb.org/wp-content/uploads/P050419.pdf

369. Government of India, Ministry of Finance (2017) Government constitutes an Inter- Disciplinary Committee chaired by Special Secretary (Economic Affairs) to examine the existing framework with regard to Virtual Currencies., available at http://pib.nic.in/newsite/PrintRelease.aspx?relid=160923

370. Nupur, A (2018) *At last, India's ready to clarify its stance on cryptocurrencies*, available at www.bit.ly/2Bm7tmZ; Linver, H (2019) *India's Complex Relationship with Crypto*, available at www.bit.ly/2MuDSQ2

371. Garg, Subhash Chandra (SecretaryDEA) (2017) *Cryptocurrencies like bitcoins are neither currency nor coin. Not legal tender in India at all.*, available at www.bit.ly/2W2CxPy; see also Gola, Y (2019) *India's Central Bank Targets Blockchain Payments While Hating Bitcoin*, available at www.bit.ly/2QAUDr9

372. RBI (2013) *RBI cautions users of Virtual Currencies against Risks*, available at www.bit.ly/2MjZCh6; RBI (2017) *RBI cautions users of Virtual Currencies*, www.bit.ly/2Q3n6rH; RBI (2017) *Reserve Bank cautions regarding risk of virtual currencies including Bitcoins*, www.bit.ly/2EM986u

373. Writ Petition 1071/2017 filed by Vijay Pal Dalmia, Advocate. *See* Vaish Associates Advocates (2017) *Supreme Court Issues Notice to RBI, Union of India and Other Government Ministries and Institutions in Petition Seeking Ban on All Cryptocurrencies Like Bitcoin in India*, available at www.bit.ly/2XhL1DU

374. Jaitley, A (2018) *Union Budget 2018: Full text of Arun Jaitley's budget speech*, available at www.bit.ly/2nGAdyX

375. The prohibition included services related to 'maintaining accounts, registering, trading, settling, clearing, giving loans against virtual tokens, accepting them as collateral, opening accounts of exchanges dealing with them and transfer/receipt of money in accounts relating to purchase/ sale of VCs.' See RBI (2017) *RBI/2017-18/154 DBR.No.BP.BC.104 /08.13.102/2017-18 Prohibition on dealing in Virtual Currencies (VCs)*, available at www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11243

376. Trivedi, U & Satija, R (2018) *Cryptocurrency Virtually Outlawed in India as Top Court Backs Ban*, available at www.bloom.bg/2Nl0ajk

377. Coindelta Exchange—Bitfair Technologies Pvt. Ltd., Gurgaon; Koinex Exchange—Discidium Internet Labs Pvt. Ltd., Mumbai; Throughbit Exchange—Throughbit Technologies Pvt. Ltd., Bangalore; CoinDCX—Neblio Technologies Pvt. Ltd., Mumbai

378. CCN (2018) *India's Bitcoin Banking Blockade in Supreme Court*, available at www.bit.ly/2Mj4DXj

379. Anupam, S (2019) *Supreme Court Gives Centre 4 Weeks To Bring In Cryptocurrency Policy*, available at www.bit.ly/2Xn4oMr; Avan-Nomayo, O (2019) *India's Supreme Court Issues Ultimatum for Clear-Cut Bitcoin Regulations*, available at www.bit.ly/2ELytOd

380. While crypto-currencies may not have been viewed favorably by Jaitley in is budget speech, DLT and blockchain development was still of interest. He stated that '[t]he Government will explore use of block chain technology proactively for ushering in digital economy.' LiveMint (2018) *Union Budget 2018: Full text of Arun Jaitley's budget speech*, available at www.bit.ly/2nGAdyX

381. The Institute for Development and Research in Banking Technology (IDRBT) was established by the RBI. See IDRBT (2017) *Applications of Blockchain Technology to Banking and Financial Sector in India*, available at www.bit.ly/2Qxs5yH

382. RBI (2019) *Draft Enabling Framework for Regulatory Sandbox*, available at www.bit.ly/2HMarUY

[383] FATF is an intergovernmental organization which combats AML/CFT on a global scale. For more information, see FATF (2019) *Who we are*, available at www.fatf-gafi.org/about/

[384] Johnson, K (2018) *Global watchdog to put Pakistan back on terrorist financing watchlist: sources*, available at www.reut.rs/2osjxLI; The Economic Times (2019) *FATF team not happy with Pakistan's efforts to combat terror financing: Report*, available at www.bit.ly/2YT4sU2; Khan, A U (2018) *FATF Grey List: Time for Pakistan to Take Bold Steps*, available at http://issi.org.pk/wp-content/uploads/2018/07/IB_Asad_July_11_2018.pdf

[385] Dawn.com (2019) *FATF 'grey list': Pakistan gets time, but not out of the woods yet*, available at www.dawn.com/news/1465397

[386] Ansari, I (2019) *Govt introduces regulations for cryptocurrencies*, available at www.tinyurl.com/y525vh2j

[387] SBP (2018) *ERD/M&PRD/PR/01/2018-31 Caution Regarding Risks of Virtual Currencies*, available at www.bit.ly/2W5lj4i

[388] The SBP specifically enumerated Bitcoin, Litecoin, Pakcoin, OneCoin, Dascoin, Pay Diamand and implied application to other altcoins of its ilk.

[389] 'All banks, development financial institutions, microfinance banks and payment system operators, payment service providers are advised to refrain from processing, using, trading, holding, transferring value, promoting and investing in virtual currencies/tokens.' SBP (2018) *BPRD Circular No. 03 of 2018, Prohibition of Dealing in Virtual Currencies/Tokens*, available at www.sbp.org.pk/bprd/2018/C3.htm

[390] SBP (2019) *Regulations for Electronic Money Institutions (EMIs)*, available at www.bit.ly/2HO0OFt

[391] EMIs are intended to provide low cost alternatives to banking, with prudent compliance measures, and can provide wallets, prepaid cards and contactless payment instruments which can issue e-money to make digital payments.

[392] Ansari, I (2019), *ibid.*

[393] Customer due diligence requirements for payment instruments include collecting the name, father or spouse's name, Computerized National Identity Card (CNIC), mobile number, residential address, a live photo (under certain circumstances) and potentially other requirements. *See* SBP (2019) *Regulations for Electronic Money Institutions (EMIs)*, *ibid.*

[394] Kiani, K (2019) *State Bank eyes issuance of digital currency by 2025*, www.bit.ly/2OFvL04; Zmudzinski, A (2019) *Pakistan's Central Bank Aims to Issue Its Own Digital Currency by 2025*, available at www.tinyurl.com/y5xf4gzf

[395] .Trotman, A (2013) *Bitcoins banned in Thailand*, available at www.bit.ly/2Wz1ZR5; Bitcoin Co. Ltd. (2013) *Trading suspended due to Bank of Thailand advisement*, available at www.bit.ly/2MmHROu; Reuters (2018) *Thai central bank bans banks from cryptocurrencies*, www.reut.rs/2Z2gzOB; The initial 2013 suspension was lifted after the Bank of Thailand stated that digital currency is not under the purview of Thai law. See Leesa-Nguansuk, L & Sangwongwanich, P (2014) *Bitcoins back in the Thai marketplace*, available at www.bit.ly/2QL1r5D

[396] Kietduriyakul, K & Charoenkitraj, N & Phongsathaporn, K (2018) *A Complete Guide to Regulations on Cryptocurrencies and ICOs in Thailand*, available at www.bit.ly/2EMiOOi; and Kitiyansub, S (2018) *Regulation of digital assets takes effect in Thailand*, available at www.bit.ly/2W5eakC (Thai), www.bit.ly/2W2E4p3 (English)

[397] Royal Decree (2018) *Digital Asset Business*, available at www.bit.ly/2If3jyb

[398] A crypto-currency is defined by the Royal Decree as 'an electronic data unit created on an electronic system or network for the purpose of being used as a medium of exchange for the acquisition of goods, services or any other rights, or the exchange between digital assets, and shall include any other electronic data units as specified in the notification of the SEC.' Blandin, A & Cloots, A S & Hussan, H et. al. (2019) *ibid.*

[399] A digital token is defined by the Royal Decree as 'an electronic data unit created on an electronic system or network for the purpose of: (1) specifying the right of a person to participate in an investment in any project or business; (2) specifying the right of a person to acquire specific goods, specific service, or any specific other right under an agreement between the issuer and the holder, and shall include any other electronic data units of right as specified in the notification of the SEC.' Blandin, A & Cloots, A S & Hussan, H et. al. (2019) *ibid.*

[400] Kietduriyakul, K & Charoenkitraj, N & Phongsathaporn, K (2018), *ibid.*

[401] TSEC (2019) *SEC updates list of cryptocurrencies eligible for investment in ICOs and base trading pairs*, available at www.sec.or.th/EN/Pages/News_Detail.aspx?SECID=7346

[402] Prior to any offering, issuers must be a Thailand based and registered company with at least THB 5 million in working capital (~USD 160,000 as of June 2019); have filed a registration statement and prospectus with the TSEC; paid the application fee; and have satisfied reporting and other application requirements.

[403] Retail investors are limited to an investment of THB 300,000 per person per offering.

[404] A complete list of rules and regulations of digital asset business operators may be found on the TSEC website. See TSEC (2019) *Regulations: Digital Asset Business Operators*, available at www.bit.ly/2JPWyr4; *See also* TSEC (2019) *Digital Asset Information: Exchange, Broker, Dealer, ICO Portal, ICO Issuer*, available at www.bit.ly/2XjablD

[405] www.cointelegraph.com/news/thailand-approves-fully-legal-bitcoin-exchange

[406] Thailand had made illegal the buying and selling of Bitcoin and the use of Bitcoin to make payments for goods and services, including sending or receiving Bitcoins with another party outside of Thailand. *See* Bitcoin Co. Ltd. (2013) *Trading suspended due to Bank of Thailand advisement*, available at www.tinyurl.com/n37yj8b

[407] Helms, K (2018) *Thai Government Cannot Stop Crypto Use—Regulatory Framework Expected in a Month*, available at www.tinyurl.com/ybd7k9tu

[408] Reuters (2018) *Thai central bank bans banks from cryptocurrencies*, available at www.tinyurl.com/yxsvwqpr

[409] Alois, JD (2019) *Project Inthanon: Bank of Thailand Pushes Forward with Central Bank Digital Currency*, available at www.bit.ly/2Xlrkv0; Wipro (2019) *Wipro, R3 build blockchain-based solution prototype to power digital currency in Thailand*, available at www.bit.ly/2IgjM6n

[410] Helms, K (2019) *Thailand Issues 4 Crypto Licenses, Rejects 2 Exchanges*, available at www.bit.ly/2YYxGkv

[411] Helms, K (2019) *Thailand Approves Country's First ICO Portal*, available at www.bit.ly/2EXFgDA; Gola, Y (2019) *Thailand SEC Approves First-Ever Foreign ICO Screening Portal*, available at www.bit.ly/2HwXKxJ

[412] SBV, (2014) *Press release on bitcoins and other virtual currencies*, www.bit.ly/2I28O4H; The Hindu (2014) *Vietnam bans bitcoin*, available at www.bit.ly/2I9r4Jj.

[413] Bank of Vietnam (2017) *Information regarding the use of virtual currency (also known as crypto-currency) as a means of payment*, available at www.bit.ly/2Vz6xT5; Vietnam Plus (2017) *SBV says bitcoin prohibited in Vietnam*, available at www.bit.ly/2W8lStX; Akolkar, B (2017) *Vietnam's Central Bank Bans Bitcoin as Payment Method*, available at www.bit.ly/2JPyJ2u

[414] Bank of Vietnam (2017), *ibid.*; Vietnam Plus (2017), *ibid.*; Akolkar, B (2017), *ibid.*

[415] Das, S (2018) *Vietnam Investigates Alleged $660 Million ICO Fraud of Pincoin, Ifan*, available at www.bit.ly/2Z4qa7R

[416] Meyer, D (2018) *Vietnam Is Outraged Over a $658 Million Cryptocurrency Scam*, available at www.bit.ly/2Mit9Yx; Das, S (2018) *Vietnam Investigates Alleged $660 Million ICO Fraud of Pincoin, Ifan*, *ibid.*

[417] SSC (2018) *Notification to the operations on investment and business in the field of financial technology*, available at www.bit.ly/2YVXgGE

[418] Socialist Republic of Viet Nam (2018), *Directive No 10/CT-TTg*, available at www.bit.ly/2WNHj83

[419] Das, S (2018) *Vietnam's Securities Watchdog Bans Industry from Cryptocurrency Activity: Report*, available at www.bit.ly/2YYaAuf

[420] SSC (2018) *The SSC would like to inform the management of the issuance, trading and brokerage activities related to crypto-currency*, available at www.bit.ly/2Iomxmz

[421] Viet Nam News (2018) *Central bank agrees to suspend import of crypto-currency mining machines*, available at www.bit.ly/2JSfZj9; Memoria, F (2018) *Vietnam To Ban Bitcoin Miner Imports, Increase Scrutiny*, available at www.bit.ly/2KpYF4D; Das, S (2018) *Vietnam's Central Bank Approves Call to Suspend Import of Cryptocurrency Miners*, available at www.bit.ly/2XdSofL; Viet Nam News (2018) *Securities watchdog tightens crypto-currency management*, available at www.bit.ly/2Z1pIH8

[422] SBV (2018) *Workshop on International Experience in Fintech Regulatory Sandbox*, available at www.bit.ly/2w6K7hA

[423] KRONN Ventures AG (2019) *KRONN Ventures AG to Establish Vietnam's First Authorized Cryptocurrency Exchange and Lead Cryptocurrency Production*, available at www.tinyurl.com/y6zbbbox; Memoria, F (2019) *Vietnam to Soon Have a Fully-Authorized Cryptocurrency Exchange*, available at www.tinyurl.com/y2qlq9lx

[424] Gola, Y (2019) *Vietnam to Get Its First Ever Cryptocurrency Exchange—But Is It Legal?*, available at www.tinyurl.com/y65dkkc5

[425] Fischler, N (2018) *Vietnam has a crypto-currency dilemma*, available at www.bit.ly/2QzfQ4u

[426] Legance (2018) *Virtual currencies in Italy—an overview*, www.tinyurl.com/y5h5xwgu

[427] The AGID can be found online at www.agid.gov.it

[428] Giannelli, A & Ciani, M (2018) *Virtual Currencies in Italy, an overview*, available at www.bit.ly/2JQ3Qv2 and Vena, M (2018) *New Proposal For Crypto Regulation in Italy: Analysis, Opinions, Context*, available at www.bit.ly/2I0YskJ; Papa, A & Quattrocchi, D & Toriello, E (2017) *IV Anti-Money Laundering Directive: the issuance of the Italian Legislative Decree implementing the Directive*, available at www.tinyurl.com/y2gcwblb; Legance (2018), *ibid.*

[429] Giannelli, A & Ciani, M (2018), *ibid.*; Papa, A & Quattrocchi, D & Toriello, E (2017), *ibid.*; Legance (2018), *ibid.*

[430] Giannelli, A & Ciani, M (2018), *ibid.*; Papa, A & Quattrocchi, D & Toriello, E (2017), *ibid.*; Legance (2018), *ibid.*

[431] *ibid.*

[432] *ibid.*

[433] BOI (2015) *Unità di informazione finanziaria per l'italia: utilizzo anomalo di valute virtuali*, available at www.bit.ly/1udi2Ru; Wong, J I (2015) *Italian Central Bank: No AML Requirement for Bitcoin Exchanges*, available at www.tinyurl.com/y2ylojcq

[434] BOI (2015) *Unità di informazione finanziaria per l'italia: utilizzo anomalo di valute virtuali*, *ibid.* and BOI (2015) *Comunicazione del 30 gennaio 2015—Valute virtuali*, available at www.tinyurl.com/y535pgjw

[435] The Mediterranean Seven are Malta, France, Spain, Portugal, Cyprus, Greece and Italy.

[436] Khan, M (2018) *Mediterranean EU countries make push on blockchain technology*, available at https://on.ft.com/2EQaixQ; Bank of Italy (2015) *Comunicazione del 30 gennaio 2015—Valute virtuali*, available at www.bit.ly/2S4Hxlk

[437] Senate of the Republic of Italy (2019) *Article 8.0.3*, available at www.bit.ly/2CEHV3U; See also Legge, 11/02/2019 n° 12, G.U. 12/02/2019 which is a conversion of Law Decree No. 135/2018, commonly referred to as Decreto semplificazioni.' Altalex (2019) Decreto semplificazioni: la legge di conversione in Gazzetta Legge, 11/02/2019 n° 12, G.U. 12/02/2019, available at www.bit.ly/314IWgX; and Maruffi, F (2019), *ibid.*

[438] DLTs are defined as: 'technologies and IT protocols using a shared, distributed, replicable and simultaneously accessible ledger, decentralized and encrypted, which enable the registration, validation, updating and storage of data, whether encrypted or not, which cannot be modified or forged.' Translation from Maruffi, F (2019), *ibid.*

[439] Smart contracts are defined as 'a computer program based on DLTs which execution is legally binding upon two or more parties with reference to the effects previously agreed by the same parties.' Maruffi, F (2019), *ibid.*

[440] Maruffi, F (2019), *ibid.*

[441] Pedersoli, G & Sassella, M & Tanno, A (2019) *Italy affirms legal effectiveness of Distributed Ledger Technologies (DLTs) and Smart Contracts*, available at www.bit.ly/2EKpX1W; and Maruffi, F (2019), *ibid.*

[442] Ernst & Young Global Limited (2019) *Italian Tax Authorities clarify VAT treatment of Bitcoin transactions*, available at https://go.ey.com/2WabAcN

[443] Giannelli, A & Ciani, M (2018), *ibid.*; Tortora, A (2016) *Bitcoin moneta virtuale, l'Agenzia delle Entrate chiarisce il trattamento fiscale*, available at www.bit.ly/30ZRSEi

[444] Higgins, S (2016) *Italy Wants to Tax Speculative Bitcoin Use*, available at www.bit.ly/30Zs8YO

[445] 'If you wish to offer services in the field of FinTech in Liechtenstein, this is the place to find initial information about the regulatory framework.' FMA (2019) *FinTech in Liechtenstein*, available at www.bit.ly/2Q7UbCV

[446] Government Principality of Liechtenstein (2019) *Report and Motion on the Blockchain Act adopted*, available at www.regierung.li/en/press-releases/222668 ; Government Principality of Liechtenstein (2019) *Bericht und antrag der regierung an den landtag des fürstentums liechtenstein betreffend die schaffung eines gesetzes über token und vt-dienstleister (token- und vt-dienstleister-gesetz; tvtg) und die abänderung weiterer gesetze*, available at www.bit.ly/30Xoyyj

[447] www.fma-li.li/files/fma/fma-fact-sheet-crowdfunding.pdf

[448] FMA (2018) *Fact Sheet on Initial Coin Offerings*, available at www.bit.ly/2KmEh29

[449] FMA (2018) *Fact Sheet on Virtual Currencies*, available at www.bit.ly/2YZwBck

[450] FMA (2018) *Business models*, available at www.bit.ly/2WCZIEO

[451] Definition provided from English translation which is not the official language of the principality. Principality of Liechtenstein (2008) *Law of 11 December 2008 on Professional Due Diligence for the Prevention of Money Laundering, Organised Crime and Financing of Terrorism (Due Diligence Act; SPG)*, available at www.bit.ly/2YVDoDG; *See also* Principality of Liechtenstein (2008) *Gesetz vom 11. Dezember 2008 über berufliche Sorgfaltspflichten zur Bekämpfung von Geldwäscherei, organisierter Kriminalität und Terrorismusfinanzierung (Sorgfaltspflichtgesetz; SPG)*, available at www.bit.ly/2W3AcEd

[452] BCB (2014) *Nr. 25,306 of Policy Statement 25,306, of February 19, 2014; Policy Statement on the risks related to the acquisition of the so-called 'virtual currencies' or 'encrypted currencies' and to the transactions carried out with these currencies*, available at www.bit.ly/2WRNAzG; BCB (2017) *Communique 31,379 of November 16, 2017; Warns about the risks derived from storing and negotiating virtual currencies*, available at www.bit.ly/2KwqBn9

[453] BCB (2014) *Nr. 25,306 of Policy Statement 25,306, of February 19, 2014*, *ibid.*; BCB (2017) *Communique 31,379 of November 16*, 2017, *ibid.*

[454] RFB (2014) *Informação Cosit nº 4, de 7 de abril de 2017: Informações relativas a moedas virtuais e atividade da RFB*, available at www.bit.ly/2JLvYj2

[455] RFB (2014) *Informação Cosit nº 3, de 7 de abril de 2017: Nota explicativa sobre moedas virtuais*, available at www.bit.ly/2YTJynN

[456] CVM (2018) *Ofício Circular nº 1/2018/CVM/SIN*, available at www.bit.ly/2DnmTqm

[457] CVM (2018) *Orientações para administradores de fundos de investimento*, available at www.bit.ly/2xBv5kr

[458] Alexandre, A (2019) *Brazil Establishes Committee for Cryptocurrency Regulation*, available at www.bit.ly/2IbFyIv; Camara Dos Deputados (2019) *Ato Da Presidencia (regarding draft law No. 20303/2015)*, available at www.bit.ly/2Z40PuB; See also Revoredo, T (2018) *Legal 'Status' of Cryptocurrencies in Brazil*, available at www.bit.ly/2QNcprj

[459] Panorama Crypto (2019) *What do we think of the new Brazil's bitcoin and cryptocurrencies bill?*, available at www.bit.ly/2XlblNz

[460] 'Offers of virtual assets that meet the definition of securities and are not compliant with regulation will be considered as illicit and, as such, subject to applicable sanctions and penalties. The CVM informs that, up to date, no ICO has been registered or exempted from registration in Brazil.' CVM (2017) *CVM Statement on Initial Coin Offering (ICO)*, available at www.bit.ly/2YZfHdQ

[461] RFB (2018) *Consulta Pública RFB Nº 06/2018*, available at www.bit.ly/2EGQ3m9

[462] RFB (2019) *Instrução normativa rfb nº 1888, de 03 de maio de 2019*, available at www.bit.ly/2WsUZSN; Tauil, Checquer, Mayer, Brown (2019) *Brazilian IRS Normative Ruling No. 1,888/2019: Regulates the Declaration of Transactions with Cryptocurrencies*, www.bit.ly/2HQdKKI

[463] "The following are required to provide information to the Brazilian IRS regarding cryptocurrency transactions: (i) the so-called Digital Currency Exchangers ('DCE'), domiciled in Brazil, and (ii) individuals and legal entities, resident and domiciled in Brazil, engaging in transactions with DCEs domiciled overseas or without the intermediation of a DCE if the monthly value of the transactions exceeds thirty thousand reais (BRL 30,000.00). The information to be provided to the Brazilian IRS includes the type of operation and the amount of the cryptocurrency used, to ten decimal places; the transaction value in BRL; the address of the remittance and receipt wallet; and, if the DCE is domiciled overseas, the DCE's name.' Summarization of main obligations—*see* Tauil, Checquer, Mayer, Brown (2019), *ibid.*

[464] CVM (2017) *CVM Statement on Initial Coin Offering (ICO)*, *ibid.*

[465] Nobium Foundation (2017) *Niobium Coin White Paper*, available at www.bit.ly/2HJFXDe

[466] CVM (2017) *Memorandum nº 19/2017-CVM/SRE*, available at www.bit.ly/2wtldJq; CVM (2018) *Memorandum nº 7/2018-CVM/SRE/GER-3*, available at www.bit.ly/2wtldJq

[467] Nobium Foundation (2017) Niobium Coin White Paper, *ibid.*

[468] 'Pier enables the data exchange between the BCB and other regulators, such as the Superintendence of Private Insurance (Susep), the Securities and Exchange Commission of Brazil (CVM), and the National Pension Funds Authority (Previc). Initially connected regulators will use Pier for sharing data regarding the authorization processes for financial institutions, including information on administrative sanctioning processes, the conduct of financial institutions' officers, and the corporate control of entities regulated by the BCB.' BCB (2018) *The new Central Bank of Brazil blockchain platform will strengthen supervisory information exchange between Brazilian regulatory authorities*, available at www.bit.ly/2Wn72js; Brown, J (2019) *Cryptocurrency* and Brazil, available at www.bit.ly/2Wfibms

[469] Gogo, J (2018) *Brazilian Banks Ordered to Reopen Cryptocurrency Exchange's Frozen Accounts*, www.bit.ly/2HQbMKA; There is no requirement that these accounts be kept open and active permanently. Garden of Crypto (2019) *A Brazilian Court Has Ruled in Favor of Cryptocurrency Exchanges*, www.bit.ly/2WBsVjn

[470] Santander Brasil, Banco Inter, Itaú Unibanco, Bradesco, Sicredi and Banco do Brasil

[471] Additionally, the court described the failure of the banks to send written notice of the closure as 'abusive conduct that is prohibited by consumer protection rules.' Trapp, A (2018) *Brazilian Banks Investigated for Unfair Crypto Restrictions*, available at www.bit.ly/2JRZ2oU; Reuters (2018) *Brazil antitrust watchdog probes banks in cryptocurrency trade*, available at www.reut.rs/2QHDZFW; *See also* Brown, J (2019), *ibid.*

[472] Memoria, F (2018) *Brazilian Cryptocurrency Exchange Wins Injunction Against Bank Who Closed Its Account*, available at www.bit.ly/2Xl35x1; Bitcoin Exchange Guide (2018) *Walltime Crypto Exchange Gets $200,000 in Funds Unfrozen After Winning Lawsuit Against Bank*, www.bit.ly/2HQdLhN

[473] President of the Republic (2018) *Law to Regulate Financial Technology Institutions*, available at both www.tinyurl.com/y8rwaopp or www.tinyurl.com/yb4e5k9c (PDF)

[474] As contained in Article 30 of the Fintech Law, virtual assets are defined as 'the representation of value electronically registered and used among the public as a payment instrument in any type of legal transaction and which can only be transferred through electronic means.' English translation used from Blandin, A & Cloots, A S & Hussan, H et. al. (2019) *ibid.*

[475] General rules were issued by the CNBV in September 2018. CNBV (2018), *ibid.*; FSB (2019) *Crypto Assets Regulators Directory*, *ibid.* These rules set forth 'enabling legislation for effective enforcement of the Fintech Law…' Blandin, A & Cloots, A S & Hussan, H et. al. (2019) *ibid.*

[476] General rules were issued by the CNBV in September 2018. CNBV (2018) *Disposiciones de carácter general aplicables a las Instituciones de Tecnología Financiera*, available at www.tinyurl.com/y67aucmz; FSB (2019) *Crypto Assets Regulators Directory*, *ibid.*

[477] CNBV (2018) *Disposiciones de carácter general aplicables a las Instituciones de Tecnología Financiera*, available at www.tinyurl.com/y67aucmz

[478] BdeM issued press releases on March 10, 2014 and in August 2017. providing a general warning of dangers and risks of dealing with Bitcoin, virtual currencies and ICOs. *See* BdeM (2014) *Advertencias sobre el uso de activos virtuales como sucedáneos de los medios de pago en moneda de curso legal*, available at www.bit.ly/2EMsSXA and BdeM & CNBV & SHCP (2017) *Comunicado conjunto SHCP- BANXICO-CNBV. Las autoridades financieras advierten de los riesgos asociados al uso de activos virtuales*, available at www.bit.ly/2JQgOsB

[479] BdeM (2014) *Advertencias sobre el uso de activos virtuales como sucedáneos de los medios de pago en moneda de curso legal*, available at www.bit.ly/2EMsSXA

[480] Morales, Y (2017) *Carstens rechaza el bitcoin como moneda virtual; no tiene respaldo del banco central*, available at www.bit.ly/2Mkm21V; Althauser, J (2017) *Banco de Mexico Governor: Bitcoin is Commodity Rather than Currency*, available at www.bit.ly/2etDGQQ

[481] FCAC (2019) *Digital currency*, available at www.bit.ly/2g3n5Ao

[482] CRA (2019) *Guide for cryptocurrency users and tax professionals*, available at www.bit.ly/2Wa6w8s

[483] Bill C-21 states it is to be in force 'on a day to be fixed by order of the Governor in Council' which has not occurred nor been announced. Druzeta, C & Grant, S & Peters, M (2019) *Blockchain & Cryptocurrency Regulation 2019 (Canada)*, available at www.bit.ly/2IiLek1; Blandin, A & Cloots, A S & Hussan, H et. al. (2019), *ibid.*

[484] Druzeta, C & Grant, S & Peters, M (2019) *Blockchain & Cryptocurrency Regulation 2019 (Canada)*, *ibid.*

[485] CSA (2017) *CSA Staff Notice 46-307 Cryptocurrency Offerings*, available at www.bit.ly/318myU1

[486] CSA (2018) *CSA Staff Notice 46-308 Securities Law Implications for Offerings of Tokens*, available at www.bit.ly/318myU1

[487] See also the initial news release of the Ontario Securities Commission (OSC) warning that coins, tokens and their offerings may be subject to Ontario securities law. OSC (2017) *OSC Highlights Potential Securities Law Requirements for Businesses Using Distributed Ledger Technologies*, available at www.bit.ly/2WoZ2n1

[488] SA (2017) *CSA Staff Notice 46-307 Cryptocurrency Offerings*, *ibid.*; CSA (2018) *CSA Staff Notice 46-308 Securities Law Implications for Offerings of Tokens*, *ibid.*; Klayman, J A & Kovnats, M & Johnston, D et. al. (2017) *Canada Confirms Tokens May Be Securities and Pacific Coin Is the Test*, available at www.bit.ly/2JZXHfY

[489] IIROC (2018), *Joint CSA/IIROC Consultation Paper 21-402 Proposed Framework for CryptoAsset Trading Platforms*, available at: www.bit.ly/2CmxGlt

[490] The mission of the Régie de l'énergie is to 'foster the conciliation of the public interest, consumer protection and the fair treatment of the electricity carrier and distributors' Régie de l'énergie (2019) *FAQ—Frequently Asked Questions*, available at www.bit.ly/2ESrXFk

[491] Hydro Quebec (2019) *The Régie de l'énergie hands down its decision in the blockchain file*, available at www.bit.ly/2vtGpys; Régie de l'énergie decision available at www.bit.ly/2WryYHR and www.bit.ly/2WryYHR

[492] CSA (2018) *CSA Regulatory Sandbox*, available at www.bit.ly/2wLA0Qz

[493] CSA (2019) *Decisions*, available at www.bit.ly/2LBUf8P

[494] For more information about and the status of Project Jasper, see Bank of Canada (2017) *Project Jasper: Are Distributed Wholesale Payment Systems Feasible Yet?*, available at www.bit.ly/2tycS5M; Bank of Canada (2019) *Fintech Experiments and Projects*, available at www.bit.ly/2QLuVQN; Payments Canada, Bank of Canada, R3 (2017) *Project Jasper White Paper*, available at www.bit.ly/2rLu9qO

[495] FINCEN (2019) *Mission*, available at www.fincen.gov/about/mission

[496] FSB (2019) *Crypto Assets Regulators Directory*, *ibid.*

[497] CFTC (2019) *Mission & Responsibilities*, available at www.bit.ly/2QPE0Yx

[498] IRS (2019) *About IRS*, available at www.irs.gov/about-irs

[499] Kohen, M & Wales, S (2019) *State Regulations on Virtual Currency and Blockchain Technologies*, available at www.bit.ly/2QT6vow

[500] FINCEN (2013) *Application of FINCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies" (FIN-2013-G001)*, available at ?

[501] The IRS defines 'virtual currency' as 'a digital representation of value that functions as a medium of exchange, a unit of account, and/or a store of value. In some environments, it operates like "real" currency—i.e., the coin and paper money of the United States or of any other country that is designated as legal tender, circulates, and is customarily used and accepted as a medium of exchange in the country of issuance—but it does not have legal tender status in any jurisdiction.' IRS (2014) *Notice 2014-21*, available at www.irs.gov/pub/irs-drop/n-14-21.pdf; CFTC (2018) *Request for Input on Crypto-Asset Mechanics and Markets, FR Doc No: 2018-27167*, available at www.bit.ly/2KvaTsK; FINCEN (2013) *Application of FINCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, FIN-2013-G001 (March 18, 2013)*, available at www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf

[502] 'The CFTC's jurisdiction is implicated when a virtual currency is used in a derivatives contract, or if there is fraud or manipulation involving a virtual currency traded in interstate commerce.' CFTC (2017) *CFTC Backgrounder on Self-Certified Contracts for Bitcoin Products*, available at www.bit.ly/2Z9DyHO

[503] 'The SEC provided a caveat that the framework 'is not a rule, regulation, or statement of the Commission. The Commission has neither approved nor disapproved its content. This framework, like other Staff guidance, is not binding on the Divisions or the Commission.' US SEC (2019) *Framework for "Investment Contract" Analysis of Digital Assets*, www.bit.ly/2HXfEdZ; SEC (2019) *Statement on "Framework for 'Investment Contract' Analysis of Digital Assets"*, available at www.bit.ly/2YNZ996

[504] *SEC v. W.J.Howey Co.*, 328 U.S. 293 (1946) ("*Howey*"). *See also United Housing Found., Inc. v. Forman*, 421 U.S. 837 (1975) ("*Forman*"); *Tcherepnin v. Knight*, 389 U.S. 332 (1967) ("*Tcherepnin*"); *SEC v. C. M. Joiner Leasing Corp.*, 320 U.S. 344 (1943) ("*Joiner*")

[505] While the *Howey* test applied to the 'MUN Token' may not have qualified it as a security (but as a 'utility token'), it was ultimately deemed a security based upon the 'manner of sale' which promoted expectations of profits of the MUN Token.' Munchee, Inc., Securities Act of 1933 Release No. 10455 (Dec. 11, 2017), available at www.sec.gov/litigation/admin/2017/33-10445.pdf; Token giveaways, whether pursuant to bounties, air-drops or other form without monetary consideration, could still constitute the sale of securities since the test analysis focuses on the perceived benefit of value by the token recipient. Tomahawk Exploration LLC and David Thompson Laurance, Securities Act of 1933 Release No. 10530 (Aug. 14, 2018); see also Securities Exchange Act of 1934 Release No. 83839 (Aug. 14, 2018), available at www.sec.gov/litigation/admin/2018/33-10530.pdf;.For a comprehensive analysis of security tokens including these and other SEC Orders, see Klayman, J A (2019) *Blockchain & Cryptocurrency Regulation 2019, Mutually assured disruption: The rise of the security token*, available at www.bit.ly/2IiLek1

[506] US SEC (2018) *Division of Enforcement Annual Report 2018*, available at www.bit.ly/2zrMHAh

[507] Some of the conditions included a requirement that proceeds of token sales have limited internal uses, tokens are immediately usable, pricing remains fixed at the stated USD 1 price, redeemable only for air charter services, no representation will be made about profit potential of token purchases. US SEC (2019) *TurnKey Jet, Inc., Securities Act of 1933 Section 2(a)(1) and Section 5 Securities Exchange Act of 1934 Section 3(a)(10) and Section 12(g)*, available at www.bit.ly/2WO0E97

[508] US SEC (2018) *Digital Asset Transactions: When Howey Met Gary (Plastic)*, available at www.bit.ly/2l8t5dB; *See also* Mendelson, M (2019) From Initial Coin Offerings to Security Tokens: A U.S. Federal Securities Law Analysis, available at www.stanford.io/2K0QZWY

[509] US SEC (2017) *SEC Issues Investigative Report Concluding DAO Tokens, a Digital Asset, Were Securities*, available at www.sec.gov/news/press-release/2017-131

[510] IRS (2014) Notice 2014-21, *ibid.*

[511] Department of Banking and Securities (2019) *Money Transmitter Act Guidance for Virtual Currency Business*, available at www.bit.ly/2Xryvlj

[512] Texas Department of Banking (2019) *Supervisory Memorandum 1037, Regulatory Treatment of Virtual Currencies Under the Texas Money Services Act*, available at www.bit.ly/2Z86U9j

[513] New York State Dept. of Financial Services (2015) *Title 23, Chapter 1, Part 200 Virtual Currencies*, available at www.dfs.ny.gov/docs/legal/regulations/adoptions/dfsp200t.pdf

[514] State of Washington (2019) *SB5031, Uniform Money Services Act—Virtual Currency—Online Currency Exchangers*, available at www.legiscan.com/WA/text/SB5031/2017

[515] DeWaal, G (2019) *New York State Department of Financial Services Revokes Crypto Exchange's Safe Harbor to Operate Without BitLicense*, available at www.bit.ly/2QOdij2; Rasmussen, M & Shipchandler, S & Love, E (2019) *NYDFS Rejects Cryptocurrency Exchange License Applications, Citing Compliance Program Flaws*, available at www.bit.ly/2QOdij2; Brennan, S (2018) *Contortions for Compliance: Life Under New York's BitLicense*, available at www.bit.ly/2QODES2; Wieczner, J (2018) *Inside New York's BitLicense Bottleneck: An 'Absolute Failure?'*, available at www.bit.ly/2HY86GB

[516] New York State, Department of Financial Services (2019) *DFS Advances New York's Thriving Virtual Currency Market, Grant Virtual Currency and Money Transmitter Licenses to Tagomi Trading, LLC*, available at https://on.ny.gov/2FD15c6

[517] State of Colorado (2019) *SB 023, The Colorado Digital Token Act*, available at www.legiscan.com/CO/bill/SB023/2019

[518] State of Montana (2019) *House Bill No. 584, An Act Relating to Cryptocurrency; Amending Transactions from Certain Securities Law*, available at www.legiscan.com/MT/bill/HB584/2019

[519] Department of Banking and Securities (2019), *ibid.*

[520] State of South Dakota (2019) *HB1196, An Act to provide a definition of blockchain technology for certain purposes*, available at www.legiscan.com/SD/bill/HB1196/2019

[521] Texas Department of Banking (2019), *ibid.*

[522] Virtual currency is defined as 'broadly construed to include digital units of exchange that (i) have a centralized repository or administrator; (ii) are decentralized and have no centralized repository or administrator; or (iii) may be created or obtained by computing or manufacturing effort.' State of West Virginia (2019) *HB2813, An Act to amend and reenact §11-15A-1 of the Code of West Virginia, 1931, as amended; and to amend said code by adding thereto a new section, designated §11-15A-6b, all relating generally to collection of use tax*, available at www.legiscan.com/WV/bill/HB2813/2019

[523] State of Wyoming (2019) *SF0125, An Act relating to property; classifying digital assets within existing laws; specifying that digital assets are property within the Uniform Commercial Code; authorizing security interests in digital assets*, available at www.legiscan.com/WY/bill/SF0125/2019

[524] State of Wyoming (2019) *HB0185, An Act relating to corporate shares and distributions; authorizing corporations to issue certificate tokens in lieu of stock certificates as specified; making conforming amendments; and providing for an effective date*, available at www.legiscan.com/WY/bill/HB0185/2019

[525] State of Wyoming (2019) *HB0057, An Act relating to trade and commerce; making legislative findings; creating the financial technology sandbox for the testing of financial products and services in Wyoming*, available at www.legiscan.com/WY/bill/HB0057/2019

[526] Perlman, L (2018) *A Model Crypto-Asset Regulatory Framework*, available at www.ssrn.com/abstract=3370679

SIPA

Where the World Connects

SIPA.COLUMBIA.EDU