



*Disclaimer: Data for this report have been gathered from a substantial number of sources, including in-person interviews and desktop research for a large number of jurisdictions. While every reasonable efforts has been made to verify the source and accuracy of the data collected, the research team cannot exclude potential errors and omissions. This report should not be considered to provide legal or investment advice. Opinions expressed in this report reflect those of the authors and not necessarily those of their respective institutions.*

# TABLE OF CONTENTS

---

FOREWORDS.....	5
RESEARCH TEAM.....	7
ACKNOWLEDGEMENTS.....	9
METHODOLOGY AND REPORT STRUCTURE.....	10
EXECUTIVE SUMMARY .....	12
<b>SECTION 1: KEY CONCEPTS.....</b>	<b>14</b>
1.1 Cryptoasset Nature and Form.....	14
A short introduction to tokens.....	14
Lack of clear terminology.....	15
Determining definitional boundaries.....	16
Risk of conflating form and nature.....	17
A multi-dimensional approach.....	18
A note on cryptoasset ownership.....	21
1.2 Token Creation, Initial Distribution, and Secondary Market Trading.....	23
Token creation .....	23
Initial token distribution (primary market).....	24
Secondary market trading.....	25
1.3 Intermediated Activities.....	26
<b>SECTION 2: COMPARATIVE ANALYSIS.....</b>	<b>30</b>
2.1 Introduction.....	30
2.2 Responsible Regulatory Authorities.....	30
Typology.....	30
Regulatory perimeter.....	32
Initial statements by regulators.....	33
2.3 Terminology, Definitions, and Classifications.....	34
What terms are regulators using?.....	34
Many definitions share similar elements.....	36
Bespoke regulatory classification frameworks.....	36
2.4 Regulatory Processes.....	39
Consultations.....	39
Information and knowledge sharing between regulators.....	40
2.5 Regulatory Responses.....	41
Scope.....	41
Typology of regulatory response.....	41
Regulated activities.....	43
Self-regulation.....	46
Authorisation of cryptoassets.....	47
Regulatory sandboxes.....	48
Enforcement actions.....	49

<b>SECTION 3: REGULATORY CHALLENGES .....</b>	<b>50</b>
<b>3.1 Mapping Cryptoasset Activities .....</b>	<b>50</b>
Data availability and quality .....	50
Infrastructure providers: miners, developers, and nodes.....	50
Airdrops and forks.....	51
Decentralised exchanges (DEXes) .....	52
Privacy coins .....	53
Stablecoins.....	53
<b>3.2 Establishing a Clear Regulatory Perimeter .....</b>	<b>54</b>
Lack of clear terminology.....	54
Regulatory arbitrage.....	54
Enhanced clarity over regulatory supervision.....	54
Limitations of technology-neutrality (substance over form) principle .....	55
<b>3.3 Identifying Potential Risks .....</b>	<b>55</b>
Consumer protection and information disclosure .....	55
Systemic risks .....	56
 <b>SECTION 4: CASE STUDIES .....</b>	 <b>57</b>
Bespoke Regulatory Regime and/or Regulation.....	57
Retrofitted Regulation .....	76
Existing Regulation.....	96
 <b>APPENDIX A: REVIEW OF REGULATORY CRYPTOASSET DEFINITIONS.....</b>	 <b>113</b>
<b>APPENDIX B: AUTHORISATION IN SELECTED JURISDICTIONS.....</b>	<b>116</b>
<b>APPENDIX C: GLOSSARY.....</b>	<b>120</b>

# FOREWORDS

---

Cambridge  
Centre  
for Alternative  
Finance



This inaugural study examining the global cryptoasset regulatory landscape goes a long way towards fulfilling the core mission of the Cambridge Centre for Alternative Finance: informing the operationalisation of technology-enabled financial innovation. Harvesting the potential benefits of innovation in financial services is highly contingent on the regulatory environment in a given jurisdiction, and few innovations in finance have emerged in recent years as controversial and presenting as many challenges to regulators and policymakers as cryptoassets.

To what extent are cryptoassets more form over function relative to traditional financial assets? This is a key question which surfaces in debates about cryptoassets amongst regulators and market participants alike. It is a critically important question because the answer defines the appropriateness of existing regulation for cryptoassets and related activities. It is a question that this study seeks to shed light on by offering analytical tools for both regulators and market participants to conceptualise cryptoassets and develop a more consistent regulatory approach across regulatory bodies. This is particularly challenging to achieve in a market that is evolving very rapidly with much of the innovation being driven by actors based outside of the traditional financial system.

Stakeholders operating in financial markets are beginning to realise that the adoption of cryptoassets in volume is likely to have profound implications for both financial market infrastructure and the relationships between market participants. The stakes are high for both market participants and regulators. For some incumbent participants it is raising existential questions and understandably provoking strong reactions aimed at preserving the status quo. Innovators see the opportunity for gain produced by disruption, with 'gain' broadly defined in terms of financial, social, or political outcomes depending on the innovator. Regulators are cognisant of these competing forces, and are also aware of that there are new risks associated with cryptoasset technological innovation that may result in unexpected consequences impacting financial stability, consumer protection, and other areas of interest to regulators.

Our hope is that this global comparative analysis of cryptoasset regulation will highlight coverage gaps in regulatory frameworks and enable individual regulators to benchmark their own regulatory approach in the context of the global cryptoasset regulatory landscape. The global scope of this project distinguishes it from many other studies of cryptoasset regulation, and this was made possible by the collective effort of more than 20 researchers and contributors based around the world, including the team of cryptoasset researchers associated with the Cambridge Centre for Alternative Finance led by Michel Rauchs and Apolline Blandin, and with the financial and research support provided by the Nomura Research Institute. A global research collaboration on that scale in itself is an achievement.

**Dr. Robert Wardrop**

Director

*Cambridge Centre for Alternative Finance*



The year 2018 was one of trial and tribulation for Japan's virtual currency market. Japan had been a front-runner in the global virtual currency market since the birth of Bitcoin, with many of these currencies seeing active use domestically and local authorities being among the first in the world to establish a regulatory framework. However, revelations of a January 2018 theft from one of Japan's leading virtual currency exchanges dramatically changed public views. Many legal and financial experts called for tighter regulation to protect users. Some even argued that virtual currencies were nothing more than speculative instruments that could never serve as a means of settlement.

We at NRI believe such a pessimistic view is unwarranted. Both the Financial Services Agency and industry group made great strides in 2018 towards establishing an appropriate regulatory framework that allows for both innovation and the protection of users. In spite of the problems associated with virtual currencies, the market itself is clearly growing more sophisticated. Meanwhile, the existing financial system still has numerous issues that have yet to be resolved, including the high cost of international remittances. We believe virtual currencies may ultimately help to address some of these shortcomings.

NRI is honored to have had the opportunity to participate in a related research project led by Cambridge University. The project involved a survey of virtual currency regulatory trends in 23 countries and sought to identify the global implications of these developments. As far as we know, it is the most comprehensive survey of its kind, and we wish to thank the Cambridge Centre for Alternative Finance (CCAF) for its leadership in bringing it to completion. We sincerely hope this report will provide valuable information to policymakers, regulatory authorities, and market participants and thereby contribute to the healthy development of the broader market for virtual currencies.

**Takashi Kawai**

General Manager, Financial Market & Innovation Research Department  
*Nomura Research Institute*

# RESEARCH TEAM

---

## Authors

**Apolline Blandin:** Apolline is a Research Manager in Cryptocurrency and Blockchain at the Cambridge Centre for Alternative Finance. Her previous research focused on financial inclusion in China.

✉ [a.blandin@jbs.cam.ac.uk](mailto:a.blandin@jbs.cam.ac.uk)

🐦 [@ApollineBlandin](https://twitter.com/ApollineBlandin)

**Ann Sofie Cloots:** Ann Sofie is a PhD candidate at the Faculty of Law, University of Cambridge, and a Research Assistant at the Cambridge Centre for Alternative Finance.

✉ [ascc2@cam.ac.uk](mailto:ascc2@cam.ac.uk)

**Hatim Hussain:** Hatim is a Research Assistant at the Cambridge Centre for Alternative Finance and is pursuing his graduation in law from Gujarat National Law University, India.

✉ [hatimhussain110@gmail.com](mailto:hatimhussain110@gmail.com)

🐦 [@hatimhussain110](https://twitter.com/hatimhussain110)

**Michel Rauchs:** Michel is the Lead in Cryptocurrency and Blockchain at the Cambridge Centre for Alternative Finance. He has co-authored five industry reports on cryptoassets and DLT.

✉ [m.rauchs@jbs.cam.ac.uk](mailto:m.rauchs@jbs.cam.ac.uk)

🐦 [@mrauchs](https://twitter.com/mrauchs)

**Rasheed Saleuddin:** Rasheed is a post-doctoral researcher at the Cambridge Centre for Endowment Asset Management. His work on the formation and regulation of modern markets, 'The Government of Markets', was recently published by Palgrave Macmillan.

✉ [r.saleuddin@jbs.cam.ac.uk](mailto:r.saleuddin@jbs.cam.ac.uk)

🐦 [@r\\_sale](https://twitter.com/r_sale)

**Jason Grant Allen:** Jason is a Humboldt Post-Doctoral Fellow at the HU Berlin and a Visiting Fellow at the UNSW Faculty of Law, where he is working on the interaction between law and technology with a focus on monetary law.

✉ [jgallen@cantab.net](mailto:jgallen@cantab.net)

**Bryan Zhang:** Bryan is the Executive Director of the Cambridge Centre for Alternative Finance. He has co-authored more than 25 reports in financial and regulatory innovation.

✉ [b.zhang@jbs.cam.ac.uk](mailto:b.zhang@jbs.cam.ac.uk)

🐦 [@BryanZhangZ](https://twitter.com/BryanZhangZ)

**Katherine Cloud:** Katherine is a Research Associate at the Cambridge Centre for Alternative Finance where her research has mainly focused on regulatory reform and financial inclusion.

✉ [k.cloud@jbs.cam.ac.uk](mailto:k.cloud@jbs.cam.ac.uk)

## Contributors

### **Julian Bajada**

Research Assistant, Cambridge Centre for Alternative Finance

### **David C. Donald**

Professor, Faculty of Law, The Chinese University of Hong Kong

### **Ivan Ermokhin**

Deputy Head, Russia-OECD Centre

### **Victor Fortun-Basauri**

LLM Candidate, University of Cambridge

### **Christian Hofmann**

Assistant Professor, Faculty of Law, National University of Singapore

### **Eva Huang**

Research Affiliate, Cambridge Centre for Alternative Finance

### **Nataliia Ivanytska**

Associate at De Gaulle Fleurance & Associés

### **Jamie Kennedy**

Policy Analyst, Commonwealth Treasury

### **Alexandra Koval**

Researcher, Russia-OECD Centre

### **Antonina Levashenko**

Head, Russia-OECD Centre

### **Lin Lin**

Assistant Professor, Faculty of Law, National University of Singapore

### **Katsutoshi Takehana**

Senior Researcher Financial Technology and Market Research Department, Nomura Research Institute

### **Marianne Verdier**

Professor of Economics, Université Panthéon Assas, Paris II

### **Nikos Yerolemou**

Research Affiliate, Cambridge Centre for Alternative Finance

# ACKNOWLEDGEMENTS

---

We would like to thank the Nomura Research Institute (NRI), and specifically Katsutoshi Takehana, for its sponsorship and relentless support.

Special thanks go to Keith Bear (CCAF), Philip Rowan (CCAF), and Emmanuel Schizas (CCAF) for providing invaluable feedback and for their thorough review of an early draft. This research study would not have been possible without the fantastic work of our designer, Louise Smith. Pawee Jenweeranon, Sunghan Ryu, Luisa Scarcella, Yuriy Slavinskiy, and Lily Zechner deserve special thanks covering their respective jurisdictions. Finally, we would like to thank the entire CCAF team – and Kate Belger in particular – for their continuous support and assistance.

We would also like to thank the following regulators for offering some of their time to give in-person interviews and to review some of the content: French DG Tresor, French ACPR, Bank of Canada, Government of Bermuda, the UK Cryptoasset Taskforce, the FSRA in Abu Dhabi, and the Government of Gibraltar.

# METHODOLOGY AND REPORT STRUCTURE

---

## Methodology

The Cambridge Centre for Alternative Finance has undertaken a detailed analysis of the regulatory landscape on cryptoasset activities in select jurisdictions. The report focuses on financial regulation and has deliberately removed tax policy from the study scope.<sup>1</sup>

The research team developed a conceptual framework that groups together cryptoasset-related activities into three broad categories to facilitate the analysis of applicable regulations and ensure a standardised data collection process: (1) asset nature and form; (2) token creation, initial distribution, and secondary market trading; and (3) intermediated activities.

The framework was then applied to 23 jurisdictions selected on the basis of two criteria: the level of domestic cryptoasset activity and the relative magnitude of the regulatory response.<sup>2</sup> Although efforts were made to eliminate biases in our sample, practical considerations and the lack of available data as a result of low to non-existent activity levels in certain regions resulted in geographic and economic concentration.

Data was collected primarily via desktop research from November 2018 to early February 2019 and included primary data sources (official documents and statements) as well as secondary data sources (articles, books, and blog posts). Whenever possible, local contributors familiar with the domestic regulatory environment were tasked with data collection of the associated jurisdiction. In some cases, desktop research was supplemented with interviews with representatives of local regulatory authorities.

The comparative analysis in Section 2 also used data drawn from two broader datasets based on information published by the US Law Library of Congress. This allowed the analysis of specific aspects to be expanded to 40 and 108 jurisdictions.<sup>3</sup>

- 
- 1 However, tax administrations may be briefly mentioned when no other authorities in a given jurisdiction have issued official statements on cryptoassets.
  - 2 The term “regulator” is used broadly throughout this report to encompass any and all authorities with jurisdiction over cryptoassets. This includes central banks, legislative bodies, securities regulators, and other agencies with financial supervisory responsibility.
  - 3 The Law Library of Congress (2018) *Regulation of Cryptocurrency Around the World*. Available at: <https://www.loc.gov/law/help/cryptocurrency/cryptocurrency-world-survey.pdf> [Last accessed: 04 February 2019] and The Law Library of Congress (2014) *Regulation of Bitcoin in Selected Jurisdictions*. Available at: <https://www.loc.gov/law/help/bitcoin-survey/regulation-of-bitcoin.pdf> [Last accessed: 04 February 2019].

## Report Structure

The report is divided into four main sections:

**Section 1** explains the main cryptoasset concepts and provides a theoretical framework to analyse key regulatory considerations. The framework is based on three interconnected components, namely the legal aspects of: (1) the nature of cryptoassets, (2) token creation, initial distribution, and secondary market trading, and (3) intermediated activities.

**Section 2** presents a comparative analysis of regulatory approaches taken by different jurisdictions globally.

**Section 3** identifies regulatory challenges and gaps that arose from the discussion in Sections 1 and 2, which should be considered by regulators.

**Section 4** offers detailed descriptions of the regulatory environments of 23 selected jurisdictions: Abu Dhabi, Australia, Bermuda, Canada, China, the European Union, Estonia, France, Germany, Gibraltar, Hong Kong, India, Israel, Japan, Malta, Mexico, Russia, Singapore, South Korea, Switzerland, Thailand, the United Kingdom (UK), and the United States of America (USA).

# EXECUTIVE SUMMARY

---

This research was conducted by the Cambridge Centre for Alternative Finance (CCAF) at the University of Cambridge Judge Business School with the support of the Nomura Research Institute (NRI). A number of external contributors have joined the CCAF research team to produce this comprehensive, systematic, and comparative analysis of the current regulatory landscape of cryptoassets and related activities. The study covers 23 jurisdictions and is based on both desktop research and in-person interviews with regulators and policymakers. The report aims to compare and contrast various regulatory approaches and practices with regards to cryptoassets in a number of jurisdictions and shed light on current regulatory challenges and opportunities.

Section 1 sets out a theoretical framework to conceptualise cryptoassets and related activities. It looks at three key aspects in a regulatory context: (1) the nature and form of cryptoassets, (2) the issuance of cryptoassets, and (3) intermediated activities in the life cycle of cryptoassets. A number of regulatory recommendations are brought forward, which include:

- Traditional assets recorded on a distributed ledger technology (DLT) infrastructure (i.e. tokenisation) should be distinguished from new and natively-digital cryptoassets with unique characteristics. The fundamentally new characteristic of a natively-digital cryptoasset is the incentive role that it may play in a particular network;
- A legal and regulatory classification of a cryptoasset should be based on an in-depth assessment of several factors (e.g. rights attached, access, economic function of the token), generally conducted on a case-by-case basis;
- The majority of cryptoasset-related activities carried out by intermediaries show strong similarities to existing financial activities found in traditional markets (e.g. exchange and trading), and therefore might be regulated as such. Only a relatively small number of cryptoasset-specific activities can be considered novel (e.g. mining).

Section 2 provides a global comparative analysis of cryptoasset regulation in 23 jurisdictions. It examines regulatory authorities regulating cryptoassets, their current definition and classification of cryptoassets and related activities, as well as regulatory processes and responses (e.g. *existing regulation*, *retrofitted regulation*, *bespoke regulation* and *bespoke regulatory regime*). Key findings of this section include:

- The scope of different regulatory authorities (“regulatory perimeter”) can and often does overlap when regulating cryptoasset activities. Our research shows that, on average, three distinct national bodies per jurisdiction have issued official statements on cryptoassets, including warnings;
- The extension of the initial study sample from 23 jurisdictions to 40 jurisdictions reveals that central banks have usually been the first type of regulatory authority to issue official statements (including warnings about cryptoassets), followed by government departments (e.g. Ministry of Finance) and financial supervisory bodies;<sup>4</sup>
- There is no standard usage of terminology across regulators and a variety of terms have been used to refer to cryptoassets in official statements. Notably, the term *virtual currency* has been used most frequently in official documents, although it has often been used interchangeably with *cryptocurrency* and *digital currency*;

---

<sup>4</sup> The expanded sample of 40 jurisdictions is based on the following report: The Law Library of Congress (2014) *Regulation of Bitcoin in Selected Jurisdictions*. Available at: <https://www.loc.gov/law/help/bitcoin-survey/regulation-of-bitcoin.pdf> [Last accessed: 04 February 2019].

- The first step towards regulating cryptoassets has typically been to distinguish cryptoassets which are deemed to be securities from other types of cryptoassets;
- Existing regulatory frameworks generally classify cryptoassets into payment, utility, and security tokens, although frameworks in certain jurisdictions consider an additional fourth category of *hybrid tokens* that share characteristics of multiple categories;
- An expanded sample of 108 jurisdictions reveals that countries with higher levels of domestic cryptoasset activity tend to have retrofitted regulations, whereby existing laws and regulations are amended to respond more swiftly to new-to-market activities;<sup>5</sup>
- The most sophisticated regulatory frameworks (i.e. bespoke regulatory regime or bespoke regulation) are often found in smaller countries with a relatively low level of domestic cryptoasset activity and a tendency for more flexible financial regulation;
- Regulators have to date focused mainly on addressing regulatory concerns over initial coin offering (ICOs) and cryptoasset exchange activities. These two activities are often regulated under existing securities law, supplemented with guidance from the securities regulators;
- All 23 jurisdictions from the study sample have brought at least one intermediate cryptoasset activity (e.g. exchange, storage) under the remit of their anti-money laundering and counter-terrorism financing (AML/CFT) regulations.

Section 3 highlights some of the most salient challenges and potential gaps that stem from the development and implementation of cryptoasset regulation. The section reveals four main findings:

- Regulators have primarily focused their attention on ICOs and exchanges to date. Consequently, other key activities, such as alternative token distribution mechanisms (i.e. *airdrop* and *fork*), decentralised exchanges, and the creation of cryptoassets through mining or the peer-to-peer transfer of cryptoassets, have been overlooked;
- Unclear terminology and classification, inherent limitations to regulatory principles, and regulatory arbitrage are factors that challenge regulators' ability to robustly define their regulatory perimeter and implement regulations;
- In many of the jurisdictions studied, regulators have addressed key risks related to financial integrity and systemic issues as well as investor and consumer protection. Additional risks may warrant further regulatory attention;
- Securities laws, banking and payment laws, and/or AML laws have so far received the most regulatory attention in relation to regulating cryptoasset-related activities. Regulators may need to consider how other laws might be applicable, such as tax or property law. Regulators might want to fully examine the efficacy and adequacy of existing regulations before developing new and bespoke regulations, and identify cryptoasset activities that do not require (additional) regulation.

Section 4 consists of an in-depth analysis of cryptoasset regulations in 23 jurisdictions that constitute the backbone of the comparative analysis.

The research team hopes that this report will serve as a useful empirical study to inform industry stakeholders as well as evidence-based regulation and policymaking.

<sup>5</sup> The expanded sample of 108 jurisdictions is based on the following report: The Law Library of Congress (2018) *Regulation of Cryptocurrency Around the World*. Available at: <https://www.loc.gov/law/help/cryptocurrency/cryptocurrency-world-survey.pdf> [Last accessed: 04 February 2019].

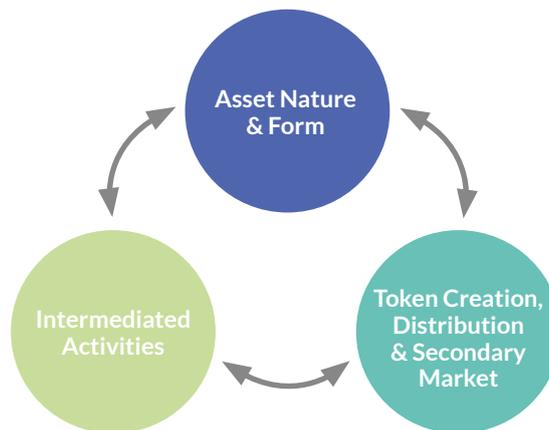
# SECTION 1: KEY CONCEPTS

This section introduces the key concepts related to cryptoassets from the perspective of three sets of regulatory and legal considerations:

1. Asset nature and form
2. Token creation, initial distribution, and secondary market trading
3. Type of intermediaries providing related services

This methodology serves as a basic framework for the legal and regulatory analysis of cryptoasset activities. These three sets of considerations are closely interlinked and impact each other, as illustrated in [Figure 1](#) below. How regulators and policymakers understand and conceptualise each dimension will affect how they view and regulate other aspects of cryptoassets and related activities. Therefore, it is of vital importance to develop a holistic and coherent understanding of cryptoassets and related market activities rooted in empirical evidence and deeper knowledge of the underlying mechanisms.

**Figure 1: A basic framework for legal and regulatory cryptoasset analysis**



## 1.1 Cryptoasset Nature and Form

### A short introduction to tokens

The hype around digital tokens suggests that asset digitisation is a relatively recent phenomenon. However, tokens have already been used for several decades in electronic recordkeeping systems. At its most basic, a digital token is simply a string of characters that constitutes a cryptographically-secure representation of a set of rights that can be used within a specific context.<sup>6</sup> Tokens do not need to be monetary in nature: for instance, web browsers commonly use so-called *security tokens* for secure online authentication.

Recently, there has been a renewed interest in tokens. The reason lies in blockchain and distributed ledger technology (DLT), which significantly changes how assets can be issued and transferred digitally. Until recently, digital tokens mostly existed in the form of ledger entries in internal database systems maintained by trusted third parties.<sup>7</sup>

<sup>6</sup> For example, a tokenised casino chip will be useful within the premises (i.e. context) of the casino that issued the chip token, but likely be worthless in a different casino.

<sup>7</sup> These parties are responsible for recording asset ownership, preventing unlawful access and transfers, and impeding the “double-spending” of assets (i.e. copy-pasting the same digital asset and spending it multiple times).

Blockchain and DLT systems are new shared accounting tools that enable distributed recordkeeping without the need to rely on a single controlling party. Such new shared infrastructures allow for the creation of *natively digital assets* (i.e. assets that only exist in digital form within the boundaries of the issuing system), as well as the *tokenisation of existing assets* (i.e. digital representation of assets, including rights, held elsewhere). Blockchains and other DLT systems allow such assets to be transferable across organisational boundaries.



### Digital tokens and token-based payment systems

Although many prominent cryptoassets are used for payments, there is an important difference in the way that the term “token” is used in computer science and in the law of payment systems. Generally, payment systems can be divided into *account-based* and *token-based systems*.

- In **account-based systems**, such as conventional bank payments, payments occur when numerical entries are made in a ledger. The tally of each user’s ledger changes more or less dynamically as value passes between users. Traditionally, the only way to maintain such a ledger was via some central bookkeeping entity, such as a bank.
- In a **token-based payment system**, such as cash, payments occur when physical tokens pass directly between users of the system, and the property law regime underlying the payments system treats physical possession as evidence of ownership. There is no need for a central bookkeeper, because each user’s balance is evident in the number of tokens held.

Many argue that cryptoassets mimic a token-based payment system because they lack a trusted intermediary; indeed some open, public, and permissionless DLT systems enable new forms of payment which display hybrid features. However, the legal presupposition of token-based payment systems has traditionally been a physical token. A change in the physical possession of cash, for example, is *prima facie* evidence of a change of ownership. In the case of cryptoassets, there is no “token” that actually moves like a coin or banknote; instead, information is changed in a digital ledger via a new accounting entry. Although there have been calls to do so, the law of token-based systems cannot straightforwardly be carried over directly to the digital realm: this would require a fundamental rethink of the law of negotiable instruments, particularly the notion of “possession” in digital environments. It is therefore perhaps better to remain circumspect about the notion of “electronic cash” while the legal treatment of cryptoassets develops.

## Lack of clear terminology

A major impediment to the analysis and the formulation of clear policies for the emerging cryptoasset and blockchain industry is the lack of clear and common terminology. A variety of terms are used, often interchangeably and without a clear definition. Even the term *cryptoasset* lacks a specific definition; it is widely employed as an umbrella term to refer to digital tokens that are issued and transferred on DLT systems.<sup>8</sup> However, there is no clear agreement on the definitional boundaries to date.

The terms *cryptoasset* and *token* can have different meanings depending on the context in which they are used. Regulators therefore face several challenges: first, to understand the nuances of the different terms, second, to identify the terminology most suitable for their regulatory objectives, and finally to define the terminology clearly and ensure it is used consistently in official statements.

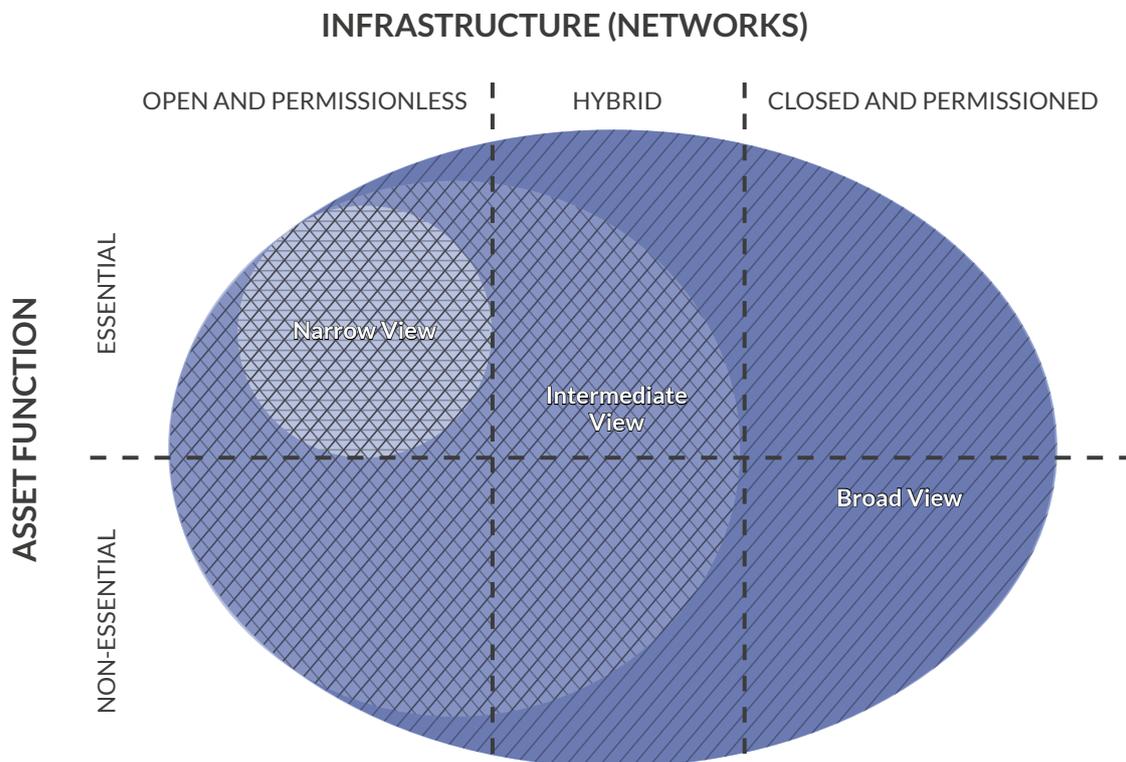
<sup>8</sup> DLT systems are systems of electronic records that enable independent entities to establish a consensus around a shared ‘ledger’ - without relying on a central coordinator to provide the authoritative version of the records. For a primer on DLT systems, see Rauchs, M et al. (2018) *Distributed Ledger Technology Systems: A Conceptual Framework*. Cambridge Centre for Alternative Finance. Available at: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3230013](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3230013) [Last accessed: 14 January 2019].

## Determining definitional boundaries

There have been attempts by regulators, industry participants, and academics to define the boundaries of the term *cryptoassets*. These attempts can generally be divided into three major views:

- **Broad:** encompasses all types of digital tokens issued and transferred via both *open* and *permissionless*<sup>9</sup> as well as *closed enterprise*<sup>10</sup> DLT systems;
- **Intermediate:** includes all types of digital tokens issued and transferred via permissionless DLT systems with open access and public transaction history. The tokens do not necessarily need to perform an essential function for the underlying network to operate properly;
- **Narrow:** exclusively refers to digital tokens issued and transferred via open, permissionless DLT systems that play an essential role in the functioning of the underlying distributed ledger or application. There is no formal issuer; instead, a network of nodes creates new units according to a transparent and pre-defined schedule specified by an intangible software protocol.<sup>11</sup> The token is inextricably linked to the underlying network by acting as an indispensable economic coordination mechanism without which the network would cease to function.

**Figure 2: Determining the boundaries of the term “cryptoassets”**



<sup>9</sup> Public (or open, permissionless) DLT systems are complex socio-economic consensus systems that rely on potentially costly Sybil prevention mechanisms (e.g. Proof-of-Work and Proof-of-Stake) and economic incentive design in order to reach agreement over the state of the system. Access is unrestricted and open to anyone.

<sup>10</sup> Private (or closed, permissioned) DLT systems are multi-party consensus systems that rely on access control and contractual agreements between known, vetted participants in order to achieve distributed consensus. A gatekeeper is responsible for member onboarding.

<sup>11</sup> The software protocol is intangible in the sense that its rules to create new token units are enforced by network participants (nodes) running compatible client implementations that implement protocol rules. As a result, cryptoassets, as defined by the “narrow” view, are not a liability of someone else and thus do not represent a claim on a particular party.

The classification illustrated by [Figure 2](#) highlights the remarkable differences in the way industry and academia is interpreting the same term. The “broad” view considers any digital token issued and transferred via any type of DLT system to be a cryptoasset. The “intermediate” view limits the scope to both open and permissionless as well as hybrid DLT systems, whereas the “narrow” view further restricts the scope exclusively to open and permissionless infrastructure. Moreover, the latter excludes tokens that are not an essential component of the underlying network’s socio-economic incentive design.

### Risk of conflating form and nature

Tokens issued on blockchains can represent traditional types of agreements (e.g. a share of common stock) held in a new form. This new infrastructure, which includes an integrated value transfer mechanism, enables new forms of asset creation, distribution, and transfer. However, the nature and subsequent legal obligations of the underlying asset does not change automatically. From a regulator’s perspective, therefore, a distinction could be made between traditional assets held in these new formats and new, previously nonexistent asset types that exhibit distinct characteristics represented in a new form.

The fundamentally new characteristic of natively-digital cryptoassets lies in the incentive role that the token plays in a particular network: namely, if the token were to be stripped away, would the network still function properly?<sup>12</sup> Such tokens may require distinct regulation compared to traditional assets. [Table 1](#) provides a comparison between different asset types and the form they can take to establish what is substantively new.

**Table 1: Comparing asset types and the form they can take**

		ASSET NATURE			
		Conventional		New	
		Financial: Stocks, bonds, money, derivatives, depository receipts, private equity, private debt, etc.	Non-financial: Real estate, commodities, etc.	Cryptoassets (“narrow” view): Cryptocurrencies and utility tokens	Other: <sup>13</sup> Documents, media files, domain names, digital collectibles, etc.
FORM	Physical	Paper certificate or register: directly held by owner or custodian	Depends on asset nature: often physical possession and/or paper certificate or register	N/A	N/A
		<i>Gateways required to bridge the physical and the digital world (hybrid or exogenous)</i>		<i>No gateways required: purely endogenous</i>	<i>Gateways may be required</i>
	Electronic	Ownership registries: dematerialised asset held by CSD or custodian	N/A	Depository receipt: claim on custodial service provider	Internal enterprise registry system
	DLT-based token	a) Direct issuance <sup>14</sup> : natively digital b) Tokenised <sup>15</sup>	Tokenised: cannot be natively digital	Primary issuance: endogenous to DLT system	Depends on the application type and underlying platform

<sup>12</sup> This approach corresponds to the “narrow” view that exclusively focuses on tokens that are vital for the game-theoretical incentive systems that drive open cryptoasset networks.

<sup>13</sup> This category includes tokens that are not a security token, nor a utility or payment token (see p. 20). It consists of natively digital files that are made transferable and can thus carry monetary value. These files may reside in a closed environment maintained by a single entity or live on a shared network: the system boundaries determine the transferability of the assets in question. Unlike cryptoassets, they do not perform an essential role in the functioning of the underlying system.

<sup>14</sup> The token itself is the financial asset.

<sup>15</sup> The token is a digital representation of an existing financial asset held in custody. It is similar to a depository receipt in the sense that tokens represent ownership in the underlying item that exists “off-chain” (i.e. outside of the DLT system).

## A multi-dimensional approach

As Section 2 will show, some regulatory authorities worldwide have adopted a token classification dividing cryptoassets into three broad categories, typically:

- *Payment/exchange tokens* or *cryptocurrencies*: a means of value exchange;
- *Utility tokens*: granting access to a digital platform or service;
- *Security tokens*: an investment instrument.

The three-category classification has been a helpful first step to guide regulatory responses to cryptoassets. This basic framework nevertheless needs to be refined to capture the complexities of a quickly evolving landscape.

First, this classification may not cover all cryptoassets.<sup>16</sup> Tokens that cannot be classified under either of these three categories thus far remain largely off regulators' radars.

Second, some tokens could fall under more than one of these categories. For such so-called *hybrid tokens*, it may be unclear whether the legal obligations associated with each category are cumulative or hierarchical. For example, for a security token that is also a payment token, regulators and courts could adopt different positions, such as:

- **Cumulative:** the hybrid token has to comply with both securities laws and payment services laws;
- **Hierarchical:**
  - **Securities feature prevails:** The hybrid token has to comply with the more stringent securities law requirements only (securities features supercede other features); or
  - **Predominant feature prevails:** The hybrid token has to comply with either securities law or payment services laws depending on which is the predominant feature (is the token mainly a payment or an investment instrument?).

A number of regulators have elaborated which of these positions they favour, although most regulatory guidance is limited to listing the three categories without clarifying the legal obligations on hybrid tokens.

Third, tokens classified within these three categories may have very different functions. Natively digital tokens that play a crucial role in open network security are fundamentally different from digital tokens that are, in essence, simply a blockchain-based security, depository receipt, or voucher. Securities tokens may already be subject to existing securities laws and enforcement mechanisms and consequently no additional regulation may be needed for those tokens; although new types of intermediaries dealing with these tokens may call for bespoke regulation. Some payment tokens may already be covered by banking or payment services laws, although others may require a bespoke regulatory response. Little attention has gone so far to assess which existing regulations may be applicable to utility tokens, however, and which tailored regulatory response may be desirable.

In short, regulatory guidance and legislative initiatives on cryptoassets seem to be converging towards the three-category classification (payment, utility, and security tokens). This broad categorisation may become more refined over time, as legislators, regulators and courts encounter an increasingly diverse set of cryptoassets.

<sup>16</sup> See footnote 13 on page 19.

The following subsections attempt to identify how the regulatory categorisation of cryptoassets could be refined to capture the complexity of cryptoasset activities more fully. This could be done by:

1. Considering the different types of actors and intermediaries involved in cryptoasset activities; and
2. Distinguishing between:
  - a. Activities at different levels of DLT infrastructure (protocol/network/data – individual contract layer);
  - b. Types of DLT protocols (private/public); and
  - c. Token features (across the three categories or within one category).

This will help separate activities, tokens, and intermediaries that are truly novel from those already covered by existing regulations, or requiring only minor amendments.

**Table 2** below lists a set of key dimensions that can be used as a tool to assess the nature of a particular digital asset. The list of considerations can help regulators and other stakeholders distinguish between “form” and “nature” and identify which cryptoassets are merely a blockchain-based variant of a known instrument<sup>17</sup> as opposed to cryptoassets that have unique properties that require a bespoke regulatory solution.

**Table 2: A multi-dimensional approach for assessing token nature**

Dimension	Description	Examples
Counterparty	Verify the nature of the token issuer and potential legal liabilities that may arise.	Company; Consortium; Network protocol; Public sector institution; Individual, etc.
Reference type <sup>18</sup>	Determines what data the blockchain records are pointing to. This has a material impact on effective enforcement of ownership transfers.	<ol style="list-style-type: none"> <li>1. Endogenous: cryptocurrencies (BTC, ETH)</li> <li>2. Hybrid: Royal Mint Gold (RMG) - tradable token redeemable for physical gold held in custody</li> <li>3. Exogenous: “accounting token” used exclusively for recordkeeping purposes</li> </ol>
Technical function	Indicates the role that the token plays in the DLT system.	Economic coordination mechanism essential for the functioning of the network, regulate record production.
Economic function	Indicates the underlying economic role of the token in the network.	Payment method (e.g. transaction fee); Financial agreement, etc.
Rights attached	Specifies the type of rights (relative and absolute) that the token confers to the holder. Also covers whether these rights can be unilaterally modified by the issuer (including circumstances and conditions) and how they are effectively enforced.	Platform/application access; Profit-sharing; Ownership; Voting; Block creation; “Work”; Voucher; Claim; No rights, etc.
Underlying infrastructure <sup>19</sup>	Analyses the nature and power dynamics of the underlying platform upon which the tokens are issued, distributed, and transferred. Includes an assessment of the layer hierarchy and whether assets can easily be moved to an alternative platform.	Permissioned, closed, and private DLT system; Consortium-run DLT system; Permissionless, open, and public DLT system; Closed internal database system, etc.
Access	Specifies who can acquire, hold, use, and sell the token. Also indicates the access and exit points of the tokens (e.g. directly via blockchain, third-party access, closed trading venue).	<ul style="list-style-type: none"> <li>• Unrestricted: anyone can participate</li> <li>• Restricted: only accredited investors have access to security tokens.</li> </ul>
Redress	Determines whether issuers and users have some sort of recourse at their disposal in the case of theft, loss of funds, smart contract bug/vulnerability, and similar events. Also specifies the nature and required measures of the recovery process.	None; Insurance; Legal; Equitable

**Note:** This is not an exhaustive list. Other dimensions, criteria, and factors may be taken into account as well.

<sup>17</sup> Some projects spent considerable efforts on rebranding their token offering as “utility tokens” in order to avoid complying with securities regulation. However, recent enforcement actions by securities regulators have shown that the use of different terminology does not exempt issuers from complying with existing securities regulation. This phenomenon is also known as the “Duck test”: if it looks like a duck, swims like a duck, and quacks like a duck, then it probably is a duck.

<sup>18</sup> See 4.2.2 Exogenous and Endogenous References (pp. 48-51) in Rauchs, M. et al. (2018) *Distributed Ledger Technology Systems: A Conceptual Framework*. Cambridge Centre for Alternative Finance. Available at: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3230013](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3230013) [Last accessed: 15 January 2019].

<sup>19</sup> Idem: see 4.1.2 Layer Hierarchy (pp. 41-43).

The mere fact that assets are issued in token form on a DLT system should not inform the decision. A legal categorisation may be applied only after an in-depth factual assessment of the above factors has been conducted on a case-by-case basis.



### Regulatory Considerations I:

Based on the discussion above, there are a number of key steps to consider before regulating cryptoasset and related activities:

- Recognise that ‘cryptoasset’ is not a homogenous concept but an umbrella term to describe an array of tokens that exhibit a wide range of characteristics;
- Gather empirical evidence to inform regulatory approaches;
- Create a typology based upon the nature and form of these tokens;
- Use an evidence-based approach to develop a nuanced understanding of the types of tokens and their functions, underlying infrastructure and other key attributes;
- Identify crystallised and potential harms to both the financial markets, investors, and consumers;
- Engage with relevant stakeholders to understand their activities and business models;
- Consider statutory mandates and legal frameworks to establish a clear regulatory perimeter.

## A note on cryptoasset ownership

The move from paper-based securities to electronic registries maintained by central securities depositories since the 1970s has led to a substantial shift from direct to indirect holding of assets, with significant implications for property law.<sup>20</sup> The meaning of “ownership” differs fundamentally across major jurisdictions, and even more so with regards to how property law treats immaterial digital objects. The recent emergence of natively digital assets requires a reexamination of the concepts of *custody* and *ownership*.

Cryptoassets have no physical manifestation: they exist exclusively as digital book entries in a virtual, shared ledger.<sup>21</sup> “Moving” cryptoasset units (e.g. to transfer ownership) requires an authorisation in the form of a cryptographically-signed message by the initiator. The signature, produced by a *private key*, represents the user’s permission for the DLT system to request a ledger entry reflecting the change in ownership.<sup>22</sup> A valid signature provides the cryptographic assurance to the DLT system and its participants that the transaction initiator has the authorisation to enact a corresponding ledger entry. If accepted, the ledger is updated such that a particular cryptoasset is associated with the (typically pseudonymous) public key of a particular user.

In this context, the private key can be compared to a password that unlocks the user account, whereas the associated public key (and the derived address) resemble a user account number. This would suggest that proving ownership and exercising ownership rights of cryptoassets is dependent on knowing (and securely storing) the private key corresponding to the address in which the funds are locked. As a

<sup>20</sup> See e.g. Micheler, E. (2007) *Property in Securities. A Comparative Study*. Cambridge University Press.

<sup>21</sup> While it is possible to create physical representations of cryptoassets (e.g. see Casascius coins, OpenDIME), the unit itself still remains purely digital in the form of a ledger entry.

<sup>22</sup> Public-key cryptography, pioneered in 1976 by American cryptographers Whitfield Diffie and Martin Hellman, is an authentication and asymmetric encryption system that uses a pair of mathematically-related keys (public and private). The public key, which as the name suggests can be widely shared, is used to encrypt a message before sending it. Only the corresponding private key, which should be kept secret, can subsequently decrypt the message encrypted with the public key.

result, cryptoassets are sometimes likened to digital bearer assets where ownership is determined by “possession” – i.e. in this case knowing a private key.

However, a valid signature does not automatically provide proof that the owner of the corresponding private key has produced the signature. Instead, it provides a guarantee that a holder of the private key has initiated the transaction. The use of a private key underpins the presumption that a transaction was authorised. In the context of cryptoassets, the notion of *custody* thus no longer refers to the direct holding of assets but to the secure storage of cryptographic keys. Despite this functional equivalence, it is far from straightforward that (exclusive) knowledge of a private key is equivalent for all purposes to legal possession.<sup>23</sup>



### Property law and cryptoassets

Various legal systems are currently struggling with the property status of cryptoassets.<sup>24</sup> The question is whether the transfer process set out above should be recognised by the legal system as the transfer of “ownership” or “possession” of the cryptoasset. However, more fundamentally, it is necessary to ask what the asset is in the first place — and the answer may not be necessarily straightforward. The qualification of a cryptoasset as *property* (i.e. as an object of property rights including the right of ownership) thus constitutes a fundamental legal rather than “regulatory” consideration.

Legal systems take divergent approaches to the concept of incorporeal property. Nevertheless, it is possible to establish a few programmatic points. While no legal system has a dedicated regime for purely virtual objects, many have traditionally recognised incorporeal objects of property rights, most commonly *reified rights* (i.e. rights treated as things).

Three broad approaches can be observed in the world’s major legal systems: the common law jurisdictions use the category of *choses in action* to reify rights such that they can be owned and transferred like other types of personal property. Most civil jurisdictions treat certain rights as incorporeal things, too, although a few stipulate that only *corporeal* objects qualify as “things” that can be owned. The latter subset of civil jurisdictions, which includes German and Japanese law, presents the most fundamental problems, as the recognition of any non-physical object as an object of property rights has to get around this dogmatic axiom.<sup>25</sup> However, even this third group has found ways to accommodate immaterial objects (such as company shares held in electronic form) into their property laws, and there is no reason to think that cryptoassets cannot be accommodated.

<sup>23</sup> Further, legal possession is differently defined in every legal system, traditionally being a *terminus technicus* in civilian jurisdictions and barely defined at all in the common law systems.

<sup>24</sup> For a legal analysis of cryptoassets under different property regimes, see Chapters 6-7 in Fox, D. & Green, S. (eds.) (2019) *Cryptocurrencies in Public and Private Law*.

<sup>25</sup> A translation of the judgment of the Tokyo District Court in August 2015, which turned on the question whether a bitcoin could be the object of ownership, has just been made available. See Gullifer QC, L. (2019) *English translation of the Mt Gox judgment on the legal status of bitcoin prepared by the Digital Assets Project*. Available at: <https://www.law.ox.ac.uk/business-law-blog/blog/2019/02/english-translation-mt-gox-judgment-legal-status-bitcoin-prepared> [Last accessed: 04 February 2019].

Potential difficulties in all three legal systems remain extant, not least because paper instruments have traditionally been used to “embody” the rights in question. Further, while the traditional category of reified rights might be stretched to accommodate cryptoassets that represent rights in exogenous assets, this is not an option for those that appear to be natively “digital commodities”. It would appear that some legislative attention is needed for a rational and consistent treatment of virtual objects in the future (as, for example, a recent Swiss Federal Council report on DLT acknowledged).<sup>26</sup> Generally, until a closer examination of their property status by lawyers, courts and legislatures, cryptoassets will remain in a grey area within property law.<sup>27</sup>

## 1.2 Token Creation, Initial Distribution, and Secondary Market Trading

This subsection covers different methods of how cryptoassets are created, distributed, and subsequently traded and transferred.



### A note on token issuance

Token *issuance* refers to the combination of the token creation (e.g. through mining or pre-mining) and distribution process (e.g. through a public token sale). These two stages in the issuance of tokens are often intrinsically linked and performed by the same actor, i.e. the *issuer*.

### Token creation

Cryptoassets can, in theory, be created by any individual or entity that has been granted access to the *data layer*<sup>28</sup> (i.e. where the applications run) of a given DLT system. Such access could be granted to registered corporations, public-sector institutions, and enterprise consortia among others, but also to any individual in an open-source community. Where digital tokens are created by an informal group (e.g. an open source community of developers) or an association without legal personality, this may raise additional legal challenges for regulators, such as identifying who can be held liable for a breach of securities laws (e.g. the prospectus or other disclosure obligations) or who is the data controller for data privacy purposes.

It is important to assess whether the token created constitutes a claim on the creator (i.e. a liability for the creator) or not. In the case of tokenised assets, a custodian needs to take full control over real-world assets before corresponding tokens can be created.

There are three major mechanisms to create cryptoassets:

- **Pre-mine:** an entity creates all token units in one batch as a one-time event;
- **Continuous mining:** special nodes called *record producers* (also often referred to as “miners”, “stakers”, “bakers”, etc.) create new units on a continuous and regular basis according to a transparent, pre-specified procedure specified by the protocol that governs the network or application ruleset;
- **Hybrid:** some entity pre-mines a specific proportion of the total final token supply; the remaining token units are then “minted” through continuous mining after network or application launch.

<sup>26</sup> Federal Council Report (2018) *Legal framework for distributed ledger technology and blockchain in Switzerland*. Available at: <https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-73398.html> [Last accessed: 04 February 2019].

<sup>27</sup> See generally Allen, J.G. (2019) Property in Digital Coins. *European Property Law Journal*. 4(1) (forthcoming).

<sup>28</sup> For a description of the three core layers of a given DLT system, see pp. 33-37 in Rauchs, M. et al. (2018) *Distributed Ledger Technology Systems: A Conceptual Framework*. Cambridge Centre for Alternative Finance. Available at: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3230013](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3230013) [Last accessed: 15 January 2019]. More information on the data layer is available at pp. 66-69.

## Initial token distribution (primary market)

Once tokens have been created, there are various means for distributing the tokens to potential holders (Table 3). It should be noted that issuers can also use a combination of the models below, often in the specified order in accordance with the development stage of the associated network, application, or service.

**Table 3: Overview of initial token distribution models**

Model	Description	Access restrictions	Development stage
<b>Pre-token sale</b>	Private round offering of pre-mined token units, often at substantial discounts. The network/application may not be operational yet. <sup>29</sup> Examples include Telegram and Kin.	Generally restricted to accredited investors.	Network or application is generally not operational yet; tokens are often non-transferable and have lock-up periods. <sup>30</sup>
<b>Token sale/ Initial Coin Offering (ICO)</b>	Public (or private) offering of pre-mined token units. The network/application may not be operational yet. Examples include Tezos and Bancor.	Can be open to the public or restricted to certain investor types.	Network/application generally not operational yet; tokens may be transferable. <sup>31</sup>
<b>Mining</b>	Newly minted units are distributed ad-hoc to agents (e.g. miners, stakers, bakers) that satisfy the necessary conditions specified by the protocol (e.g. find a valid proof-of-work). <sup>32</sup> Examples include Bitcoin and Litecoin.	Dependent on network/application settings and permission levels. <sup>33</sup>	Network/application is live and operational.
<b>Airdrop</b>	New token units are distributed to holders of an existing other token, generally under specific conditions. Examples include Stellar Lumen and Decred.	Prospective holders need to be in possession of the other token before the airdrop.	Network/application may be operational.
<b>Fork</b>	A new token is created as a result of an incompatible rule change in the underlying DLT system that causes the network to split. Existing token holders receive the new token on a 1-1 basis. Examples include Ethereum Classic (2016) and Bitcoin Cash (2017).	Prospective holders need to be in possession of the other token before the fork.	Network/application is operational.

An interesting observation is that the network, application, or service associated with the token does not necessarily need to be operational at the time of the initial distribution. In this case, the token constitutes a “proof of contribution” that records the investor’s endowment. Upon system or application launch, the tokens may be redeemable for new tokens issued on the now-operational new network.

*Pre-operational* tokens (i.e. tokens associated with networks, applications, or services that are not operational yet) may be transferable via the underlying infrastructure upon which they have been issued (e.g. Ethereum for ERC20 tokens) or via private over-the-counter (OTC) desks. However, token issuers may also encode transferability restrictions and lock-up periods directly into the token to prevent it from being traded prior to launch.

<sup>29</sup> If the network or application is not operational yet at the moment of the token sale, the distributed tokens generally represent a claim on the future delivery of operational tokens that can be used on the network/application once it goes live.

<sup>30</sup> The distributed token itself may not even be issued on a DLT, but only in the context of the issuer’s internal database system as a record of the holder’s contribution. Once the network/application is operational, the holder can claim the actual token.

<sup>31</sup> The distributed token is issued on a DLT system and distributed to participating investors’ accounts in return for their contribution. The token can be transferred assuming no directly encoded restrictions, but has effectively no operational use. If the associated network or application will be launched on a different DLT system, the token effectively acts as a voucher that can be redeemed for the actual token once the system goes live.

<sup>32</sup> For further information on mining, see p.68 in Rauchs, M.; Blandin, A.; Klein, K.; Pieters, G.; Recanatini, M., & Zhang, B. (2018) *2nd Global Cryptoasset Benchmarking Study*. Cambridge Centre for Alternative Finance. Available at: <https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/2nd-global-cryptoasset-benchmark-study/> [Last accessed: 18 January 2019].

<sup>33</sup> Open, public, and permissionless DLT systems allow anyone - in theory - to participate in mining (i.e. the record creation process). In practice, however, there can be substantial barriers to entry that may discourage new entrants (e.g. high capital requirements, high operational costs etc.).

## Secondary market trading

Once created and distributed, tokens can be traded, exchanged, and transferred in multiple ways on secondary markets, which can take different forms, including but not limited to:

- **Underlying DLT systems:** each DLT system has an integrated value transfer mechanism that allows the direct transfer of funds from one peer to another as well as the exchange of one token for another as long as both tokens reside on the same network;<sup>34</sup>
- **Exchange platforms:** marketplaces that provide (primarily off-chain) transfer and exchange services, often without requiring corresponding on-chain transfers. Transfers are usually recorded in the exchange service provider’s internal database system.<sup>35</sup> Prospective buyers and sellers can also directly exchange and transfer tokens (or, in many cases, rather *claims* on tokens) with each other OTC.

Table 4 presents a variety of secondary market transfer methods, analysed in terms of the *locus of execution* (i.e. on which system the transfer is executed: on-chain vs. off-chain), the *ability to transfer* (i.e. whether there are restrictions on token transfer), and the *applicable trust model* (i.e. whether a third-party intermediary is required to perform a transaction).

**Table 4: Overview of secondary market trading options**

		LOCUS OF EXECUTION	
		On-chain Direct transfer of funds via the underlying DLT system	Off-chain Transfer of funds outside of the DLT system (e.g. exchange platform, OTC trading desks)
ABILITY TO TRANSFER	Unrestricted	Token has no embedded restrictions and can be transferred directly via the DLT system. 	No restrictions on off-chain token transfer. 
	Restricted	Transfer (and potentially access) constraints are natively encoded into the token by the issuer to prevent unauthorised on-chain transfers. 	Token can only be transferred under specific conditions (e.g. via a regulated token exchange). 
APPLICABLE TRUST MODEL	Trust-minimised No third party required	Direct P2P transfer via the underlying DLT system (e.g. on-chain bitcoin transaction).	Token can be transferred without the use of intermediaries (e.g. via layer-2 solutions such as the Lightning Network).
	Trusted Third party involved	Transaction needs to be authorised (i.e. co-signed) by a third party before it can be broadcast.	Third-party authorisation required (internal recordkeeping via database entries).

It should be noted that the ability to transfer cryptoassets is dependent on the asset’s nature and characteristics,<sup>36</sup> potential restrictions that may be natively encoded into the asset by the issuer,<sup>37</sup>

34 There are cryptographic techniques (e.g. “atomic swaps”) that enable the trust-minimised transfer of tokens between different systems. However, these mechanisms are still in early development stages and currently impractical for widespread use.

35 These off-chain token transfers, effectively corresponding to internal recordkeeping performed by custodial service providers, are more likely to fall within the scope of existing regulatory framework.

36 Cryptoassets of non-functional networks may not have been issued yet; instead, holders have a claim on the future cryptoasset in the form of a database entry in the issuer’s internal systems. As a result, there are no “tokens” that can be traded beforehand.

37 For instance, whitelisted addresses (i.e. addresses that are allowed to hold and transfer said cryptoasset) hard-coded directly into the cryptoasset smart contract.

and the underlying platform upon which the asset has been issued.<sup>38</sup> This also has implications for the applicable trust model.



### Regulatory Considerations II:

Our analysis has revealed a number of considerations regarding the regulation of cryptoasset creation and distribution:

- Understand the mechanisms through which cryptoassets are issued;
- Identify channels and models for initial token distribution (e.g. ICO);
- Refer to applicable directives, regulations and requirements insofar as applicable;
- Create a bespoke regulatory framework if necessary;
- Consider regulations in relation to the issuer including firm and individual authorisation, AML, KYC and CFT, prospectus, disclosure requirements, advertising, etc.;
- Consider regulations in relation to the advisers and promoters including general solicitation, advertising, individual and firm permissions, etc.;
- Consider regulations in relation to the retail and institutional investors including permissions, KYC, AML and CFT, territoriality, suitability, etc.;
- Examine third-party and transferability risks.

## 1.3 Intermediated Activities

While *disintermediation* (i.e. eradicating the need for any form of trusted intermediary) arguably lies at the core of cryptoasset ideology, the ecosystem has seen the rapid emergence of a variety of intermediaries. These may operate without being registered or approved by traditional regulators; in many cases because there is no legal requirement for them to do so. Nevertheless, existing regulation can sometimes be directly applied to new intermediaries that perform tasks similar to traditional financial activities. Conversely, some cryptoasset services are not commercial in nature (e.g. on-chain applications, open-source toolkits) and could, therefore, not fall under existing regulations.

**Table 5** summarises the major activity types and indicates whether an activity resembles existing traditional activities or not. Many of the aforementioned activities are described in greater detail in the *2nd Global Cryptoasset Benchmarking Study* published by CCAF in December 2018.<sup>39</sup>

<sup>38</sup> Cryptoassets issued on the same platform (e.g. Ethereum) are generally interoperable and can thus be relatively easily exchanged directly via the platform's native secondary market (assuming that no restrictions apply).

<sup>39</sup> Rauchs, M.; Blandin, A.; Klein, K.; Pieters, G.; Recanatini, M., & Zhang, B. (2018) *2nd Global Cryptoasset Benchmarking Study*. Cambridge Centre for Alternative Finance. Available at: <https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/2nd-global-cryptoasset-benchmark-study/> [Last accessed: 18 January 2019].

Table 5: Major intermediated activity types

Main Activity Type	Description	Activity Breakdown	Example
Token Creation and Distribution	Entities involved in the creation and initial distribution of (a) cryptoassets and blockchain-based tokens, and/or (b) financial instruments that derive their value from an underlying cryptoasset.	<ul style="list-style-type: none"> <li>Token creation, distribution, and related services</li> </ul>	ICOBx
		<ul style="list-style-type: none"> <li>Derivatives issuance: futures, swaps</li> <li>Underwriting services</li> </ul>	BitMEX, Cboe, CME Group, Grayscale Investment
Storage	Software program handling key management.	<ul style="list-style-type: none"> <li>Custodial wallet services</li> </ul>	Coinbase, Xapo
		<ul style="list-style-type: none"> <li>Non-custodial wallet services</li> </ul>	BitGo, Blockchain
Exchange	On-off ramps for buying and selling tokens.	<ul style="list-style-type: none"> <li>Centralised exchange services (order-book, trading platforms, brokerage services, ATMs, etc.)</li> </ul>	Bitstamp, Kraken, Coinbase
		<ul style="list-style-type: none"> <li>P2P exchange services</li> <li>Decentralised exchange services</li> </ul>	LocalBitcoin Paradex, IDEX
Payments	Gateways facilitating the use of tokens for payments.	<ul style="list-style-type: none"> <li>Consumer payments (merchant processing, spending)</li> </ul>	BitPay, BitRefill, Purse
		<ul style="list-style-type: none"> <li>Cross-border payments (remittances, B2B)</li> <li>Bill payment services</li> <li>Other (micropayments, M2M, etc.)</li> </ul>	BitPesa Bitwage
Mining	Agents performing specific operations for processing blockchain transactions.	<ul style="list-style-type: none"> <li>Hardware manufacturing</li> <li>Hardware distribution</li> <li>Remote hosting services</li> </ul>	Bitmain, Canaan Bitmain Warranty BitFury
		<ul style="list-style-type: none"> <li>Proprietary hashing</li> <li>Cloud mining services</li> <li>Mining pools</li> </ul>	NiceHash Antpool
Investing	Entities (retail and institutional) engaged in (or facilitating) the purchase, trading, and sale of tokens.	<ul style="list-style-type: none"> <li>Asset management</li> <li>Collective investment schemes</li> <li>ETFs</li> <li>Investment advisory</li> <li>Investment promotion ("influencers")</li> <li>Investment brokerage services</li> </ul>	Family offices, cryptoasset hedge funds, venture capital funds, retail investors, HNWI, asset managers, advisors.
		<ul style="list-style-type: none"> <li>ICO rating services</li> <li>Security audits</li> <li>Accounting &amp; Legal</li> <li>Compliance (KYC, AML, CFT)</li> <li>Data services</li> </ul>	ICOBench ZeppelinOS MME Coinfirm
Other	Entities providing peripheral services that are complementary to the cryptoasset ecosystem.	<ul style="list-style-type: none"> <li>Software development (protocol, middleware application)</li> </ul>	CryptoCompare Blockstream, ConsenSys
		<ul style="list-style-type: none"> <li>Blockchain analytics</li> </ul>	Chainalysis

**Traditional activity type:** activity that is not specific to cryptoassets and can also be found in other industries.

**New activity type:** activity that is specifically enabled by the properties of cryptoassets and the underlying infrastructure; does not have a direct resemblance to traditional activities in other industries.

**Mixed activity type:** activity that shares characteristics of both traditional and new activities.

The majority of cryptoasset-related activities carried out by intermediaries show strong similarities to existing traditional activities found in other markets. Examples include exchange and trading platforms, financial services and products (e.g. derivatives, ETFs), asset managers, custodians, data service providers, and payment service providers, among others.

Some activities (other than those of traditional intermediaries) have been adapted to better match the new characteristics of specific cryptoassets. Yet, only a relatively small number of activities specific to the intermediating of cryptoassets can be considered completely novel, namely that they are uniquely enabled through cryptoassets. These include cryptoasset mining activities (hashing services, pool operators) as well as peripheral services that are specifically tailored to cryptoassets (e.g. blockchain analytics and forensics).

The unique properties of cryptoassets also enable new types of ownership and custody, such as non-custodial wallet services where the provider cannot unilaterally move funds without user approval, and trust-minimised exchange services such as decentralised exchanges (“DEXes”) that do not require a central operator.

## Cryptoasset storage and custody

Holding any asset entails an element of risk, and the storage of cryptoassets is no exception, although the exact threats are somewhat different from traditional assets. Keys can be stolen by attackers, or hacked from wallets or exchanges, if not properly secured. Similarly, keys can get lost, which prevents holders from accessing their asset indefinitely. Inheritance proceedings could also be complicated if a cryptoasset holder passes away without sharing the private key to the assets.

One challenge is that secure key storage and management is a cumbersome and complex task which still requires a high level of technical proficiency.<sup>40</sup> Consequently, it is often outsourced to third-party custodial storage services. This re-introduces a layer of intermediation to the way that cryptoassets are held, which *prima facie* presents a site for both financial stability and consumer protection risks.

Early interactions of exchanges and wallets have often overly exposed cryptoasset holders to such risks. However, the industry and regulators are adopting better - if not best - practices for custodial and non-custodial cryptoasset storage. Advanced cryptographic techniques such as *Shamir's secret*<sup>41</sup> and *multi-signature*<sup>42</sup> enable the creation of new forms of custody where multiple parties are required to authorise a transaction. For instance, an account may be configured in such a way that authorising an outgoing transaction requires the signature of  $m$  out of  $n$  participants. Both the account holder and the storage service provider could hold a certain number of keys so that neither party can initiate a transaction without the other party approving. Similarly, the account holder may control a sufficient number of keys to unilaterally move funds, with back-up keys securely stored by a service provider that cannot unilaterally enact payments.

As a result, the distinction between self-custody and third-party custody becomes increasingly blurred as new models emerge. Different conceptualisations of “custody” will determine legal characterisation in turn: most bitcoin users would consider control of the private key corresponding to the address in which the funds are stored to equate to legal “ownership”, whereas some lawyers would rather take the view

<sup>40</sup> For further information on key storage, see p.52 of Rauchs, M., Blandin, A., Klein, K.; Pieters, G., Recanatini, M., & Zhang, B. (2018) *2nd Global Cryptoasset Benchmarking Study*. Cambridge Centre for Alternative Finance. Available at: <https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/2nd-global-cryptoasset-benchmark-study/> [Accessed: 18 January 2019].

<sup>41</sup> Shamir's Secret Sharing (SSS) is a cryptographic technique that divides a secret (e.g. password, private key) into  $n$  parts. Only  $k$  parts are needed to reconstruct the secret, with  $k < n$ . An agent with less than  $k$  parts will be unable to reconstruct the secret.

<sup>42</sup> Multi-signature (also called “multisig”) is a cryptographic technique that enables the creation of transactions that require a minimum threshold of private keys ( $m$  out of  $n$ , with  $m < n$ ) to sign off. For example, a company may not want to give a single employee the power to unilaterally sign off on blockchain-based transaction. The company may therefore provide  $n$  of its employees with a different private key each, and require that any cryptoasset transaction needs to be signed off by at least  $m$  of the employees holding a key.

that bitcoin registration is not constitutive of “ownership” in the same way as registration (for example in a public register) of a more conventional financial asset,<sup>43</sup> or would at least maintain that legal ownership and control of the private key might diverge.



### Regulatory Considerations III:

The risks to stakeholders involved in the intermediated holding of cryptoassets depend in part on previously identified characteristics such as (1) token nature and form (Section 1.1), and (2) token creation and distribution (Section 1.2). Some cryptoasset intermediating activities are remarkably similar to those involving traditional financial assets. In principle, such cryptoasset intermediaries can be brought under existing regulations, sometimes with minor changes or simply with guidance from the on-the-ground authority. On the other hand, some activities have entirely new characteristics, bringing about new challenges and thus requiring enhanced knowledge from the regulators (e.g. cybersecurity risks are exacerbated in the context of cryptoassets because of the irreversible nature of on-chain payments).<sup>44</sup>

In order to determine how to regulate cryptoasset intermediation, it is worth considering the actual cryptoasset intermediaries and activities that they undertake, classified by token typology as well as purpose and nature of activities. Regulators will then move to identifying the risks and opportunities involved in some activities and act based on their mandate and objectives.

Below are some of the options available to regulators:

- If feasible, apply existing regulations to traditional activities;
- If required, develop a bespoke regulatory framework for new and mixed activities;
- Make minor adjustments to existing laws;
- Supplement existing laws with regulatory guidance;
- Consult widely to assess the potential impact of regulations;
- Implement regulations with a built-in review mechanism;
- Leave some activities unregulated while issuing caveat emptor and other warnings to consumers and investors.

<sup>43</sup> Anderson, R., Ahmed, M., & Shumailov, I. (2018) Making bitcoin legal. *Security Protocol Workshop*. Available at: <https://www.cl.cam.ac.uk/~rja14/Papers/making-bitcoin-legal.pdf> [Last accessed: 10 January 2019].

<sup>44</sup> Recently, the sudden passing of a Canadian exchange platform CEO resulted in the permanent loss of approximately \$145 million worth of cryptoassets in customer funds, because the deceased was the only person to know the passwords required to access the company wallets. See Alexander, D. (2019) Crypto CEO Dies Holding Only Passwords That Can Unlock Millions in Customer Coins. *Bloomberg*. Available at: <https://www.bloomberg.com/news/articles/2019-02-04/crypto-exchange-founder-dies-leaves-behind-200-million-problem> [Last accessed: 07 March 2019].

# SECTION 2: COMPARATIVE ANALYSIS

---

The following subsections compare the approaches taken by key jurisdictions globally with regards to cryptoassets, drawing on both qualitative and quantitative data. Figures are primarily based on a dataset of 23 jurisdictions covered in Section 4, unless explicitly stated otherwise. The section concludes with an overview of expected regulatory developments.

## 2.1 Introduction

Cryptoasset-related products and services are becoming increasingly sophisticated as they rapidly evolve and scale. These innovations may increase access to finance, lower transaction costs, as well as improve market efficiency and customer experience. However, these activities also engender risks. Regulators in both developed and developing economies are getting to grips with the regulatory challenges raised by these activities, including the need to balance the benefits of innovation with other regulatory objectives such as financial stability and integrity, and consumer and investor protection.<sup>45</sup>

According to survey data from the *2nd Global Blockchain Benchmarking Study*, ICOs and cryptoasset exchange services cause the greatest concern for central banks and regulators.<sup>46</sup> Yet many of those surveyed were also concerned about the risks from custodial wallet service providers and both centralised and decentralised exchanges, signalling these activities out for increased regulatory scrutiny in the future.

Regulators have often acted on their concerns; a number of regulatory agencies have issued warnings to investors and consumers,<sup>47</sup> conducted enforcement actions, developed guidance or enacted laws to provide regulatory clarity and mitigate against risks. However, regulatory responses in the cryptoasset landscape have been far from homogenous across jurisdictions. The following subsections provide a comparative analysis of the diverse regulatory approaches taken.

## 2.2 Responsible Regulatory Authorities

### Typology

---

Different types of authorities have played an active role in cryptoasset regulation. **Table 6** provides a schematic overview of the major types of authorities. The table highlights that a wide range of authorities may have (sometimes overlapping) mandates over cryptoasset activities within a given jurisdiction.

---

<sup>45</sup> For further discussion on this, see UNSGSA FinTech Working Group and CCAF (2019) *Early Lessons on Regulatory Innovations to Enable Inclusive FinTech: Innovation Offices, Regulatory Sandboxes, and RegTech*. Available at: <https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/early-lessons-on-regulatory-innovation-to-enable-inclusive-fintech/> [Last accessed: 01 March 2019].

<sup>46</sup> Cambridge Centre for Alternative Finance (2019) *2nd Global Blockchain Benchmarking Study*. The data is based on a survey sample of 18 central banks and 11 regulators.

<sup>47</sup> A warning from a regulator often indicates that the regulatory authority does not consider cryptoasset activities as falling under its mandate.

**Table 6: Authorities involved in the legal and regulatory framework**

			General objective(s) <sup>48</sup>
Supranational (e.g. EU, UAE)			Regulatory harmonisation, information sharing, best practices development
Intergovernmental (e.g. FATF)			Regulatory harmonisation, information sharing, best practices development
Judiciary			Adjudication in both public (regulatory, criminal, etc) and private (contract, trust, etc) litigation, interpretation of applicable legislation
Legislature			Legislation
Executive	Government department	Tax administration	Policy planning and administration of tax laws
		Ministries	Consumer protection, market development, financial inclusion
	Independent regulatory authority	Financial supervisory body	Market integrity, transparency, consumer and investor protection, market development
		Central bank	Financial and monetary stability
		AML regulator	Financial integrity, transparency

**Note:** The exact division between judicial, legislative, and executive powers varies from one jurisdiction to another. Branches may overlap to a certain extent.

### Supranational and intergovernmental level

Cryptoasset related policy making and regulations at the domestic level can be shaped by supranational legal instruments or intergovernmental policy standards. One of the main objectives of supranational or intergovernmental authorities is to promote *regulatory harmonisation*, which consists of creating common standards across jurisdictions. In some cases, legislative instruments issued by supranational bodies must be incorporated into domestic laws and regulation. EU member states, for example, must transpose the provisions, including those that apply to specific cryptoasset activities, from the 5th Anti-Money Laundering Directive (5AMLD) into their domestic laws by January 2020.<sup>49</sup>

There are also recent examples of non-legally binding guidance, such as the 2019 cryptoasset guidance published by the European Securities and Markets Authority (ESMA)<sup>50</sup> and the report published by the European Banking Authority (EBA),<sup>51</sup> which both emphasise the need to ensure a level playing field among EU member states before calling on EU institutions to assess the desirability of EU-wide regulation on the topic.

Where there is no formal authority at the supranational level, there may still be pressure to coordinate regulation across jurisdictions from intergovernmental agencies. These agencies promote regulatory harmonisation across jurisdictions but do not enforce it. They can serve as data and expertise clearinghouses for regulators, but also often issue guidance that can shape domestic regulatory

<sup>48</sup> The list of objectives presented in this table is not exhaustive, and only intends to name a few that are relevant to the cryptoasset regulatory context. Furthermore, many authorities have additional regulatory objectives that may be equally, or even more, important.

<sup>49</sup> EU (2018) 5th AMLD 2018/843 Art. 1(2). Available at: [https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL%3APE\\_72\\_2017\\_INIT&from=LT](https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL%3APE_72_2017_INIT&from=LT) [Last accessed: 21 December 2018].

<sup>50</sup> ESMA (2019) *Advice - Initial Coin Offerings and Crypto-Assets*. Available at <https://www.esma.europa.eu/document/advice-initial-coin-offerings-and-crypto-assets> [Last accessed: 10 January 2019].

<sup>51</sup> EBA (2019) *Report with Advice to the European Commission on cryptoassets*. Available at <https://eba.europa.eu/-/eba-reports-on-crypto-assets> [Last accessed: 14 January 2019].

responses. For example, a number of national regulators made explicit reference to the Financial Action Task Force's (FATF) latest AML Recommendations, which include cryptoassets.<sup>52</sup>

### National level

At the domestic level, responses to global cryptoasset activities have come from a wide range of public authorities. These authorities represent all three branches of the state (i.e. legislature, executive, and judiciary). All jurisdictions examined in this report have had national regulators issue guidance or publish warnings on cryptoassets and related activities.<sup>53</sup> This is often in the absence of any legislative actions (e.g. the USA or Switzerland). A more limited number of jurisdictions regulators have adopted or enacted laws on cryptoassets or a particular subset of cryptoasset activities (e.g. Malta and Bermuda).

In a number of jurisdictions, courts have been asked to rule on legal aspects of cryptoassets. In these instances, they have had to interpret and apply existing laws to cryptoasset activities, as well as rule on the legality of regulators' enforcement actions in the field (see call-out box "The German Case"). In addition to a number of legal proceedings against ICO organisers under securities laws, courts have had to adjudicate a variety of other legal issues, including whether banks have the right to deny bank accounts to cryptoasset companies (e.g. a case before the Israeli Supreme Court).<sup>54</sup>



#### The German Case: Court vs. Regulator

On September 25, 2018 the *Kammergericht Berlin* (the highest court for the federal city-state of Berlin) recently overruled the *Bundesanstalt für Finanzdienstleistungsaufsicht's* (BaFin, the federal German financial regulator) position on cryptoassets in a criminal trial concerning an unauthorised Bitcoin exchange. In its judgment, the court held that bitcoins were not financial instruments nor units of account, as they lacked the defining characteristics of such (e.g. issuance by a known entity and statutory validity as legal tender).<sup>55</sup> Trading in bitcoins therefore did not require authorisation from the BaFin. The court made some direct statements criticising BaFin for overstepping the bounds of its competence by adopting such a broad interpretation. Given that the case was decided in the court's criminal jurisdiction, the BaFin is not bound by the *Kammergericht's* judgment and it is currently uncertain how bitcoins will ultimately be characterised in German law.

## Regulatory perimeter

Sample data shows that, on average, there are three distinct national bodies per jurisdiction that have issued official statements, including warnings, on cryptoassets. However, significant differences can be observed between jurisdictions; while in some countries a single regulatory authority has issued statements, this number rises to six in other countries.<sup>56</sup>

<sup>52</sup> FATF (2018) *International Standards for Combating Money Laundering and the Financing of Terrorism & Proliferation*. Available at: <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf> [Last accessed: 26 February 2018].

<sup>53</sup> Regulatory guidance and warnings have very different. While the former may create binding obligations and have force of law, the latter never does.

<sup>54</sup> Levush, R. (2018) Israel: Supreme Court Grants Temporary Injunction Ordering Israeli Bank to Provide Banking Services to Bitcoin-Related Account. *The Law Library of Congress: Global Legal Monitor*. Available at: <https://www.loc.gov/law/foreign-news/article/israel-supreme-court-grants-temporary-injunction-ordering-israeli-bank-to-provide-banking-services-to-bitcoin-related-account/> [Last accessed: 07 February 2019].

<sup>55</sup> Kammergericht Berlin (2018) *Handel mit Bitcoin ist nicht strafbar, da Bitcoin kein Finanzinstrument im Sinne des KWG*. Available at: <https://www.online-und-recht.de/urteile/Handel-mit-Bitcon-ist-nicht-strafbar-da-Bitcoin-kein-Finanzinstrument-im-Sinne-des-KWG-Kammergericht-Berlin-20180925/> [Last accessed: 07 January 2019].

<sup>56</sup> These figures are limited to the federal level: including initiatives and statements from regional and local regulatory bodies would likely significantly increase the range.

The reason principally lies in the fact that cryptoasset activities can fall within the regulatory perimeter of several regulators, such as in Australia where four regulators have mandates to ensure financial market stability.<sup>57</sup> Even when regulators have different statutory objectives, their regulatory powers over such activities can overlap. In such instances, regulators may choose to cooperate with each other. While cooperation may be informal or ad-hoc, regulators facing new markets or new powers might formalise their collaborative efforts through working groups, consultations or taskforces. The UK, for example, has established the “UK Cryptoasset Taskforce” to coordinate the efforts of the financial regulator (the Financial Conduct Authority - FCA), the central bank (the Bank of England - BoE), and the Ministry of Finance (Her Majesty’s Treasury). The expected benefits of coordination include information sharing, learning and the pooling of resources, in addition to potentially providing a higher degree of legal certainty for the industry and consumers.

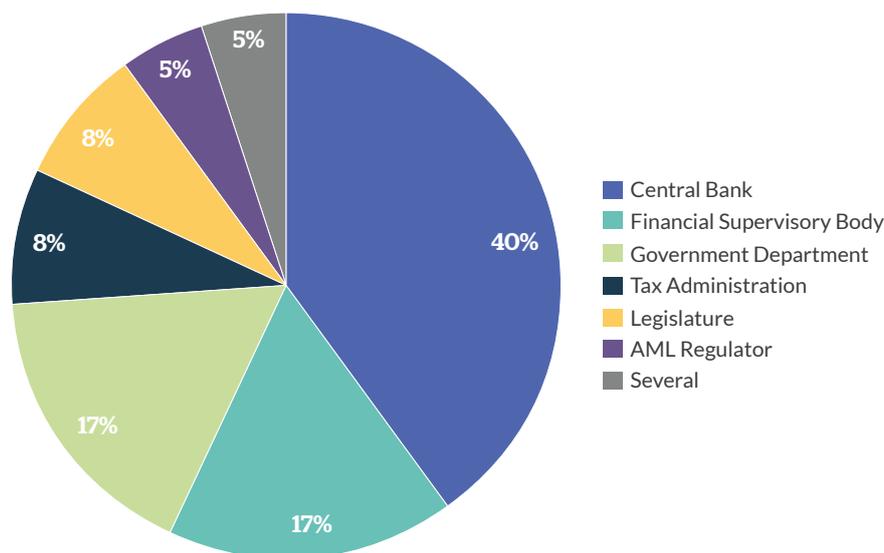
On the other hand, an overlap can cause confusion for industry and consumers if different regulators claim the activity falls under their regulatory remit (e.g. USA), without each regulator’s remit being clearly delineated for a particular activity or cryptoasset.

### Initial statements by regulators

While multiple authorities can be active in regulating and supervising cryptoasset-related activities within a single jurisdiction, it appears that certain types of authorities are first movers.

An analysis of 40 jurisdictions suggests that central banks have generally been the first type of authority to issue a warning or statement on cryptoassets (40% of covered jurisdictions), followed by government departments such as the Ministry of Finance (17%), and financial supervisory bodies (17%, see [Figure 3](#)). This observation is perhaps unsurprising given that the first generation of cryptoassets was often designed and marketed as non-sovereign digital “currencies”, prompting central banks to clarify legal tender laws.

**Figure 3: Breakdown of classification of regulatory authorities that first issued an official statement on cryptoassets in their respective jurisdiction**

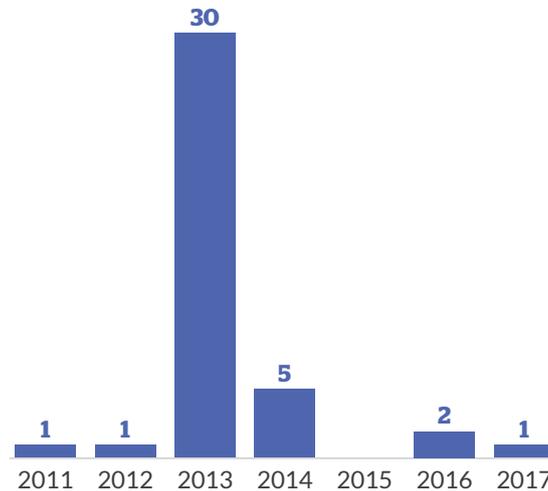


**Note:** This chart is based on the expanded sample of 40 jurisdictions.

<sup>57</sup> The four regulators are; Australian Securities and Investment Commission, Australian Prudential Regulatory Authority, Reserve Bank of Australia and Department of the Treasury.

The first official report mentioning cryptoassets by a regulatory authority was published in 2011 by the French AML regulator Tracfin,<sup>58</sup> followed by the European Central Bank in 2012 (Figure 4).<sup>59</sup> By 2014, 93% of analysed jurisdictions had their first official statement published. Interestingly, the vast majority (75%) of initial statements were issued in 2013, the same year the market experienced the largest bubble since the inception of Bitcoin in 2009.

**Figure 4: Timeline of first official statement issuance**



**Note:** This chart is based on the expanded sample of 40 jurisdictions.

Skyrocketing prices catapulted cryptoassets into the mainstream media and introduced them for the first time to a wider audience. It is argued that this development was one of the main drivers for regulators to take action. Unsurprisingly, the nature and content of initial official statements primarily consisted of warnings to consumers and investors over the risks associated with cryptoassets, and Bitcoin more specifically. Interestingly, the three jurisdictions that were among the last to issue an initial official statement (i.e. 2016 and later) are also among the first to have developed a bespoke regulatory framework (see subsection 2.5).<sup>60</sup>

## 2.3 Terminology, Definitions, and Classifications

### What terms are regulators using?

Regulators have been using a variety of terms to refer to cryptoassets in official statements. An analysis of major regulatory statements and publications identified the use of at least ten different terms between 2013 and 2019.

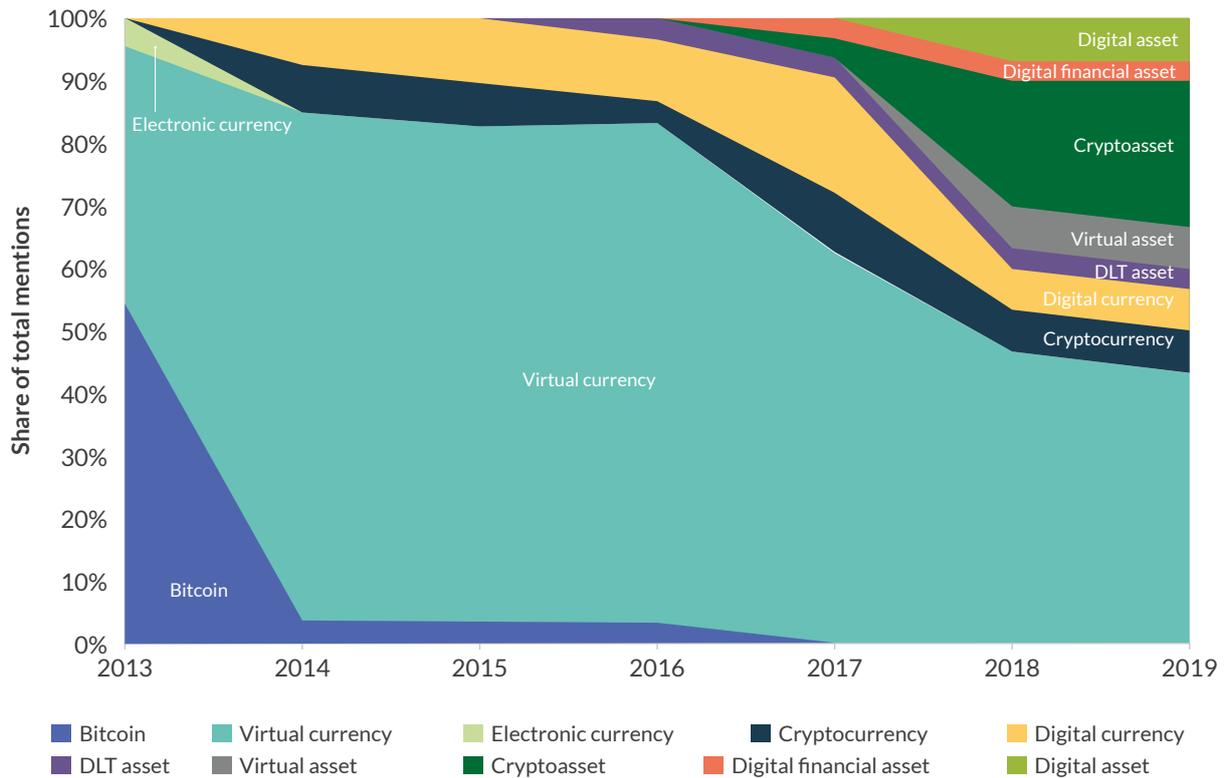
Figure 5 below suggests that *virtual currency* has been the most popular term overall, although its use has been decreasing since 2016. It is worth noting that the terms *cryptocurrency*, *virtual currency* and *digital currency* have often been used interchangeably, with several official documents containing all three.

<sup>58</sup> TracFin (2011) *Rapport d'activité 2011*. Available at: [https://www.economie.gouv.fr/files/files/directions\\_services/tracfin/Publications/rapports\\_activite/RAVFTracfin\\_09082012.pdf](https://www.economie.gouv.fr/files/files/directions_services/tracfin/Publications/rapports_activite/RAVFTracfin_09082012.pdf) [Last accessed: 04 February 2019].

<sup>59</sup> European Central Bank (2012) *Virtual Currency Schemes*. Available at: <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf> [Last accessed: 04 February 2019].

<sup>60</sup> According to our research, these three jurisdictions are Abu Dhabi, Bermuda, and Gibraltar.

Figure 5: Evolution of the terminology used by regulators (2013-2019)



**Note:** This chart is based on terminology used by regulators from the 23 selected jurisdictions, as well as selected international organisations (e.g. FATF, FSB).<sup>61</sup>

Expectedly, the first official statements issued by regulators mostly focused on Bitcoin, exploring both the functioning of the open DLT system and the potential risks associated with it. As a result, *Bitcoin* was often used as an umbrella term to refer to all cryptocurrencies prior to 2014. Over the course of 2014, *cryptocurrency* and *digital currency* became more popular, although they still only accounted for a minor share compared to the use of *virtual currency*.

During 2017 and 2018, new terms such as *virtual asset*, *digital asset*, and *cryptoasset* emerged more frequently in official documents. Some regulators have recently started to use *cryptocurrencies* more narrowly as solely a synonym for payment or exchange tokens (see [Table 7](#)) in order to distinguish them from other token types, such as utility or security tokens.

A general move to using the more generic term *virtual currency* after the FATF published its first report on virtual currencies and AML/CFT risks in June 2014 has been observed.<sup>62</sup> In the aftermath of the FATF 2014 report, many regulators drew on the definition and terminology provided by the intergovernmental body in their official communications.<sup>63</sup> A similar trend can be observed among EU member states that adopted terms and definitions used in warnings issued by other European regulatory authorities.

<sup>61</sup> Data tracking the evolution of terminology used by regulators over time has been collected manually by the research team through the analysis of official documents and publications. This analysis requires a certain level of interpretation and judgment calls for a variety of reasons: misunderstandings may arise from errors in translation, the use of diverging terminology among regulators from the same jurisdiction, the interchangeable use of specific terms by the same regulator across different statements and/or within the same statement. It was not always possible to cross-reference and verify data from all websites and repositories associated with a given jurisdiction.

<sup>62</sup> FATF (2014) *Virtual Currencies. Key Definitions and Potential AML/CFT risks*. Available at: <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf> [Last accessed: 16 January 2019].

<sup>63</sup> Among the 23 selected jurisdictions, 19 are members of the FATF. A list of FATF members is available at: <http://www.fatf-gafi.org/about/membersandobservers/> [Last accessed: 16 January 2019].

The growing diversity in terminology could be interpreted as regulators gaining a better understanding of the nuances of, and differences between, various types of tokens. The shift in terminology also represents regulators' continuous efforts to differentiate cryptoassets from fiat currencies (i.e. domestic legal tender).

**Figure 6: Current terminology used by selected jurisdictions<sup>64</sup>**



**Note:** Data as of early February 2019.

## Many definitions share similar elements

An analysis of definitions reveals that many share a common set of elements and characteristics. For instance, definitions often cover the *form* of the asset (“digital representation of value”/“electronically”), its associated *properties* (“transferable”/“tradeable”/“storable”) and its primary *functions* (“means of payment”/“store of value”/“unit of account”).

Regulatory definitions often definitively state that cryptoassets are not recognised as legal tender and thus do not constitute currency strictly so called. Only three definitions explicitly mention the use of DLT or blockchain technology as an important characteristic, which confirms the technology-neutral approach adopted by most regulatory authorities (see Appendix I).<sup>65</sup>

## Bespoke regulatory classification frameworks

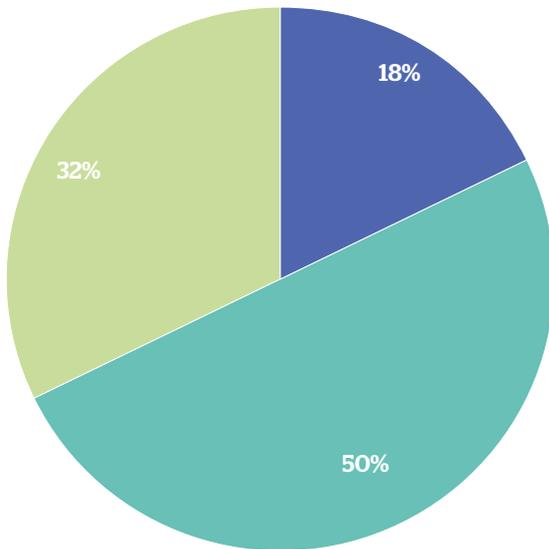
**Figure 7** shows that a prevalent regulatory approach to date is to draw a clear distinction between cryptoassets that qualify as securities and those that do not (82% of selected jurisdictions). The criteria used by these jurisdictions to determine whether a cryptoasset qualifies as a security differ from one jurisdiction to another: the majority of jurisdictions (80%) are operating on a case-by-case basis that involves assessing the characteristic of each asset individually, whereas 20% make use of a financial instrument test (e.g. the “Howey Test” in the USA).

<sup>64</sup> The terms are those used by regulators in their legal documentation.

<sup>65</sup> The three jurisdictions are Gibraltar, Malta, and the UK.

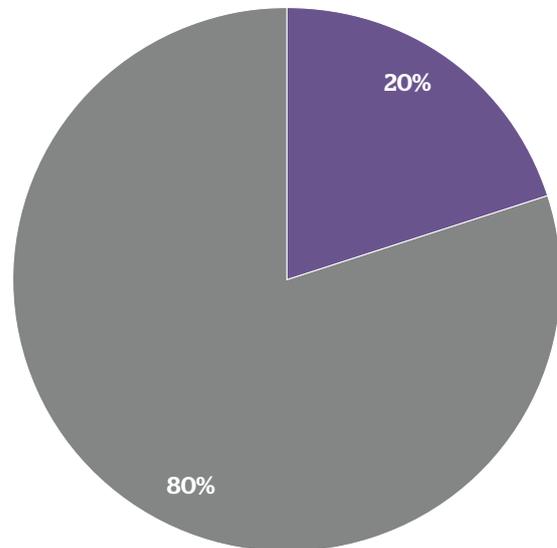
**Figure 7: Regulatory approaches to cryptoasset classification**

Do jurisdictions distinguish between security tokens and other cryptoassets?



■ No distinction and no explicit classification  
 ■ Distinction but no explicit classification  
 ■ Distinction and explicit classification

How are security tokens distinguished from other cryptoassets?



■ Financial instrument test  
 ■ Case-by-case examination

*Share of Jurisdictions*

Only four of the 23 selected jurisdictions do not explicitly distinguish between security tokens and other cryptoassets, primarily due to two opposing logics: either the distribution of cryptoassets is prohibited (e.g. China's ban on ICOs), or the absence of a token classification framework is expected to help jurisdictions stay flexible and keep abreast with the emergence of new types of cryptoassets (e.g. Bermuda and Thailand).

Of the analysed jurisdictions, 32% have created a clear classification framework for cryptoassets. In general, existing frameworks tend to divide cryptoassets into three main categories:

- **Payment tokens:** primarily used as a digital means of payment or exchange;
- **Utility tokens:** grant holders access to - and use of - a digital resource (e.g. network, application); and
- **Security tokens:** represent an investment similar in nature to traditional securities.

Some frameworks exhibit an additional fourth category of hybrid tokens, which denotes cryptoassets that share characteristics from two or more categories. While the terminology may vary across jurisdictions (e.g. exchange token and payment token both referring to tokens that are primarily used as a means of payment and exchange), the definitions of these categories are relatively similar ([Table 7](#)).

Table 7: Overview of major regulatory cryptoasset classification frameworks

	<i>Used as a digital means of payment or exchange</i>	<i>Exhibits an investment purpose</i>	<i>Grants holders access to a digital resource</i>	
 UK	Exchange token	Security token	Utility token	2019
 Malta	Virtual financial asset	Financial instrument	Virtual token	
 Abu Dhabi	Crypto Asset	Security token	Utility token	
 Israel	Currency token	Security/investment token	Utility token	
 Germany	Payment token	Equity token	Utility token	
 ESMA	Payment-type Cryptoasset	Investment-type Cryptoasset	Utility-type Cryptoasset	2017
	 EBA	Payment/exchange/currency token	Investment token	
 Switzerland	Payment token / cryptocurrency	Asset token	Utility token	

## 2.4 Regulatory Processes

Many regulators have set up internal team(s), collaborative working group(s) or taskforce(s) to assess and monitor emerging cryptoasset-related activities. In fact, 81% of jurisdictions covered in this study have staff within their regulators devoted to cryptoasset regulations. This can be in the context of an Innovation Office or as part of a taskforce specifically set up for cryptoasset activities.<sup>66</sup> Only 5% of regulators do not seem to have a dedicated team working on cryptoasset regulations (no data was available for 14% of analysed jurisdictions). There are, however, significant disparities between jurisdictions and authorities in terms of team size and scope.

### Consultations

The development of a regulatory response - and more specifically the set-up of a regulatory framework - generally involves private and/or public consultation(s). Private consultation with industry participants and other regulators may precede a public consultation, as it enables the drafting of regulatory proposals that will be made available during a public consultation.

The objective of a public consultation is generally threefold: (1) to clarify the regulator's expectations and perimeter, (2) to solicit feedback and input from concerned stakeholders and test regulatory proposals, and (3) to adapt and refine the regulatory response in light of the feedback received from stakeholders.

Across the examined jurisdictions, 63% have conducted one or more public consultations, whereas only 5% have not. No information was available for the remaining 32% of jurisdictions in the dataset. Relevant stakeholders generally include both domestic and foreign cryptoasset service providers, advisors, law firms, professional services firms, industry associations, SROs, consumer organisations, think tanks, and academics.

Additional data from CCAF's *2nd Global Cryptoasset Benchmarking Study*<sup>67</sup> gives an indication of the level of interaction and engagement between public authorities and the industry: 76% of surveyed service providers (including exchanges, wallets, and payment services from 47 countries worldwide) confirmed some collaboration with public institutions on regulatory matters.



#### Abu Dhabi's consultation process

Abu Dhabi's *Spot Crypto Asset Framework* was issued following a two-step public consultation. Firstly, a consultation period was held with leading international actors from the cryptoasset industry. This helped to draft the first proposal to amend the Abu Dhabi Global Market (ADGM) regulations and Financial Services Regulatory Authority (FSRA) rulebooks, such as definitions, fees, the creation of a new business category, and AML/CFT requirements. In a second step, the FSRA invited all cryptoasset-related businesses in the ADGM to provide feedback or comments on the proposed amendments.<sup>68</sup>

The FSRA emphasised the importance of collaboration with industry, foreign regulators and international organisations in drafting the new regulation. In particular, the consultation with international cryptoasset players not operating in Abu Dhabi allowed the FSRA to obtain a wide range of opinions. Throughout the consultation, the FSRA identified demand for greater regulation from within the industry, which supported its decision to regulate cryptoassets.

<sup>66</sup> Innovation Offices engage with, and provide regulatory clarification to, financial services providers that seek to offer innovative products and services.

<sup>67</sup> Rauchs, M.; Blandin, A.; Klein, K.; Pieters, G.; Recanatini, M., & Zhang, B. (2018) *2nd Global Cryptoasset Benchmarking Study*. Cambridge Centre for Alternative Finance. Available at: <https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/2nd-global-cryptoasset-benchmark-study/> [Last accessed: 18 January 2019].

<sup>68</sup> ADGM (2018) *Introduction of Crypto Asset Regulatory Framework in ADGM*. Available at: <https://www.adgm.com/media/277391/01-consultation-paper-no-2-of-2018.pdf> [Last accessed: 02 January 2019].

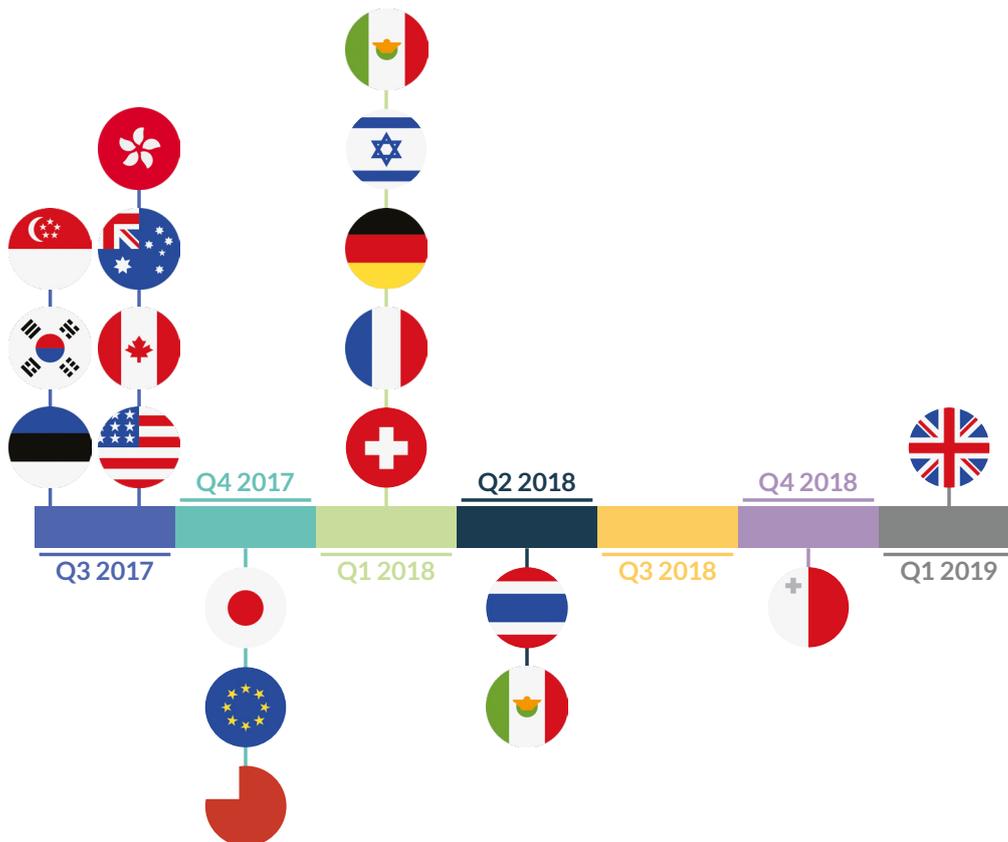
## Information and knowledge sharing between regulators

Regulatory collaboration and information exchange frequently occurs among regulators from different jurisdictions. This is primarily within the ambit of an intergovernmental or international body, such as the International Organisation of Securities Commissions (IOSCO) and the FATF, or through bilateral cooperation.

Several regulators interviewed for this report indicated that collaboration with industry actors and other regulators helped them bridge the knowledge gap about the underlying technology, and draw on other regulators' best practices.

Without necessarily entering into a formal cooperation agreement, studying the regulatory responses from other authorities can assist regulators in developing their own regulatory position on cryptoassets. For instance, the timing of regulatory statements on cryptoassets issued in selected jurisdictions suggests that some jurisdictions may have modeled their approach on prior statements made by other regulators. For example, the release of the US SEC's investigation report on The Decentralised Autonomous Organisation (TheDAO) in July 2017 influenced the approach of other jurisdictions (e.g. Israel)<sup>69</sup> towards cryptoassets that bear security-like features, either by adopting a similar or an opposite attitude (Figure 8).<sup>70</sup> This is corroborated by regulators during in-person interviews or in official communication statements.

**Figure 8: Timeline of cryptoasset guidance**



<sup>69</sup> Israel Security Authority (2018) *The Committee to Examine the Regulation of Decentralized Cryptographic Currency Issuance to the Public Interim Report*. Available at: <http://www.isa.gov.il/sites/ISAEng/1489/1513/Documents/DOH17718.pdf> [Last accessed: 20 December 2018].

<sup>70</sup> SEC (2017) *Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO*. Available at: <https://www.sec.gov/news/press-release/2017-131> [Last accessed: 31 January 2019].

The Swiss Financial Market Supervisory Authority (FINMA) has been similarly influential in the emergence of token classification frameworks. FINMA was the first regulatory body to put forth a classification of cryptoassets in November 2017, which has since been considered by regulators from other jurisdictions, albeit using a slightly different terminology, as outlined in subsection 2.3.<sup>71</sup>

## 2.5 Regulatory Responses

### Scope

Regulatory responses have thus far predominantly focused on the creation and distribution of pre-mined cryptoassets (e.g. ICOs), as well as cryptoasset exchange and trading intermediaries. Authorities' responses have ranged from public warnings, to regulatory guidance, selected enforcement actions against non-compliant actors, outright bans, and legislative initiatives on cryptoassets in offshore financial services hubs.

The sections below assess legislative responses and regulatory guidance on the legal framework applicable to cryptoasset activities (collectively referred to as "regulatory responses"). Enforcement actions are discussed in the last section.

### Typology of regulatory response

This study distinguishes between four types of regulatory responses:

- **Existing regulation:** application of existing laws or regulations to cryptoasset activities. Clarification on the applicability of existing legal instruments typically comes from regulatory guidance.<sup>72</sup> Much of the regulatory guidance has been on the applicability/relevance of securities laws and, to a lesser extent, of other laws such as banking regulations and payment provider laws.<sup>73</sup>
  - Example: Australia's *Information sheet (INFO 225) on ICOs and crypto-currency*.<sup>74</sup>
- **Retrofitted regulation:** amendment of existing laws or regulations to include one or more cryptoasset activities. A retrofitted regulation expands the scope of an existing law or regulation to cover certain cryptoasset activities explicitly.
  - Example: Estonia's amendment of the *Money Laundering Act and Terrorism Financing Prevention Act* to cover cryptoasset exchanges and wallets.<sup>75</sup>
- **Bespoke regulation:** new law or regulation enacted or issued specifically to regulate cryptoasset activities. A bespoke regulation (typically a law) establishes a separate legal framework applicable only to cryptoasset activities.
  - Example: Malta's *Virtual Financial Assets Act*.

71 FINMA (2018) *Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs)*. Available at: <https://www.finma.ch/en/~media/finma/dokumente/dokumentencenter/myfinma/1bewilligung/fintech/wegleitung-ico.pdf?la=en> [Last accessed: 08 January 2019].

72 Guidance from regulators on the applicability of existing laws and regulations to a particular cryptoasset activity remains subject to judicial review.

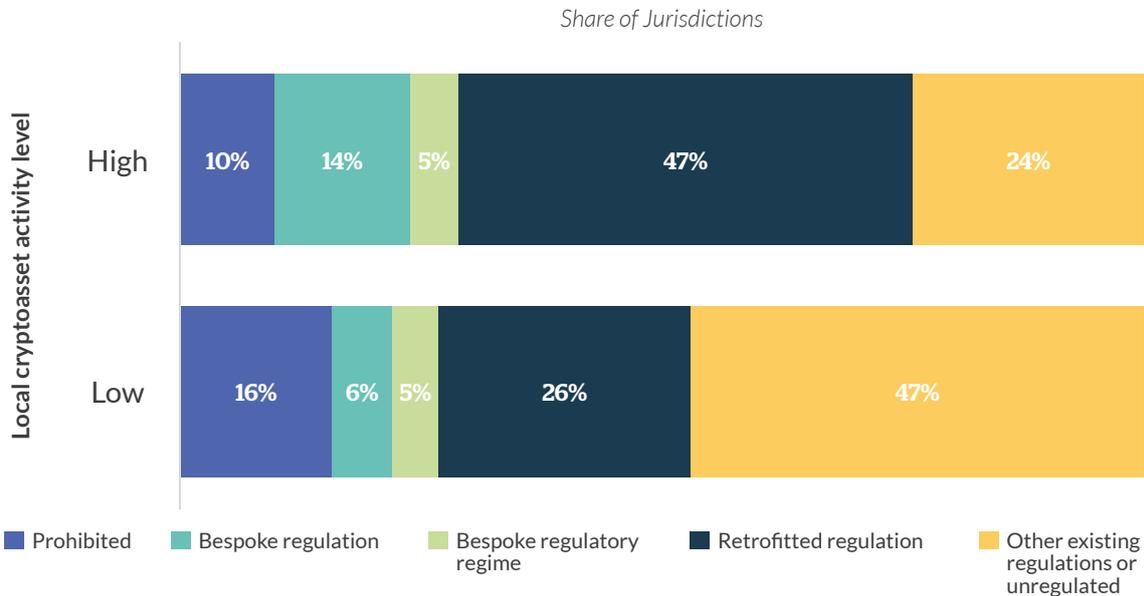
73 A distinction between applicable securities laws and various other laws (including banking laws) is also made in the regulatory comparison table in Appendix II.

74 Australian Securities and Investment Commission (2018) *Information Sheet (INFO 225) on ICOs and crypto-currency*. Available at: <https://asic.gov.au/regulatory-resources/digital-transformation/initial-coin-offerings-and-crypto-currency/> [Last accessed: 02 January 2019]

75 Riigi Teataja (2017) *Money Laundering and Terrorism Financing Prevention Act*. Available at: <https://www.riigiteataja.ee/en/eli/517112017003/consolide> [Last accessed: 14 December 2018].

- **Bespoke regulatory regime:** a distinct regulatory framework applied to a set of activities (typically fintech activities), of which cryptoasset activities are but one aspect. Bespoke regulatory regimes are typically legislative instruments.
  - Example: Mexico's *Law to Regulate Financial Technology Institutions*.<sup>76</sup>

**Figure 9: Regulatory response by level of cryptoasset activity in selected jurisdictions<sup>77</sup>**



**Note:** This chart is based on an expanded sample of 108 jurisdictions.<sup>78</sup>

Actual regulatory responses generally display a combination of these types. Based on an expanded sample of 108 jurisdictions, **Figure 9** shows that the retrofitted regulation approach has prevailed in countries with a higher level of cryptoasset activities (47%). This approach offers a relatively quick solution to bring regulatory clarity in comparison with the lengthy development of a bespoke regulatory framework. A retrofitted approach does not, however, exclude the application of existing regulation as well (e.g. securities law). In contrast, jurisdictions with a lower level of cryptoasset activity have predominantly opted to rely on existing regulations or leave such activities unregulated (47%).

Analysing cryptoasset activity levels as a function of the regulatory response reveals an interesting observation: jurisdictions with the most advanced regulatory framework (i.e. bespoke regulatory regime or specific new regulation) are often smaller countries with a low level of cryptoasset activities. These jurisdictions also correspond to countries with historically less rigid attitude towards business regulations. Their apparent incentive to create a “friendly” regime to attract cryptoasset activity may be at odds with the regulatory objectives of larger jurisdictions with higher endemic cryptoasset activity, and thus potentially create risks for the latter because of the cross-border nature of cryptoasset activities.

Most regulators in the examined jurisdictions have adopted an *activity-based approach* rather than an *entity-based approach*. An *activity-based approach* means that regulation is applicable to a specific type of cryptoasset activity, as opposed to a particular type of company or entity (i.e. *entity-based approach*). The rationale of this approach is that risks associated with cryptoasset activities are correlated with the

<sup>76</sup> President of the Republic (2018) *Law to Regulate Financial Technology Institutions*, *Diario Oficial de la Federación*. Available at: [http://www.dof.gob.mx/nota\\_detalle.php?codigo=5515623&fecha=09/03/2018](http://www.dof.gob.mx/nota_detalle.php?codigo=5515623&fecha=09/03/2018) [Last accessed: 11 December 2018].

<sup>77</sup> These regulatory responses only apply to secondary market activities.

<sup>78</sup> The classification between “high” and “low” level of cryptoasset activities is based on the number of cryptoasset firms operating in the country, the number of ICOs launched, and the level of mining activities recorded in the country.

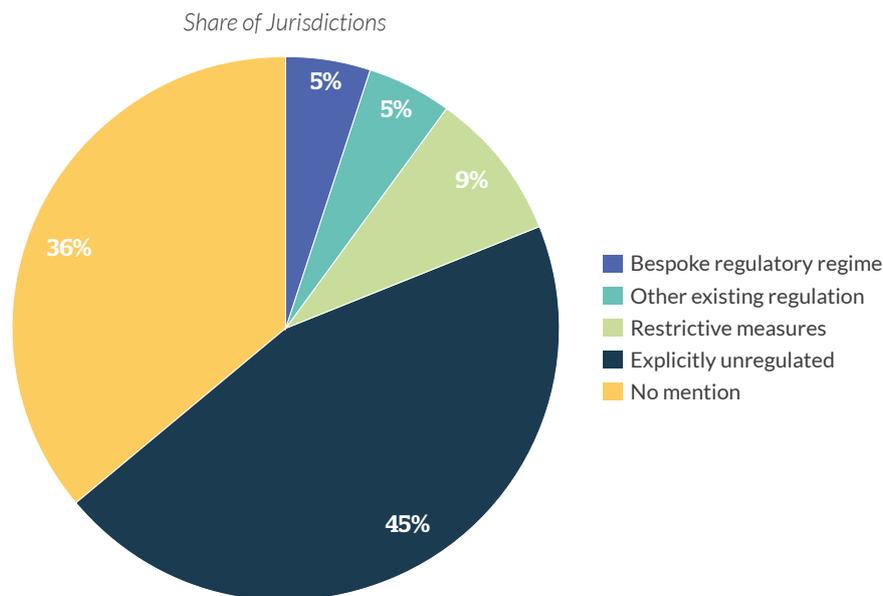
nature of the activities rather than the underlying entity conducting these activities. Additionally, by taking an activity-based approach regulators can set out in their perimeter exactly which activities they are responsible for regulating. This approach may enable firms to clearly understand if their business activities will fall under the regulatory perimeter and what type of authorisation may be required.

The activity-based approach observed across most jurisdictions may, however, be combined with an entity-based approach, especially when regulating systemic risk. This is particularly the case when regulators have issued restrictions to prevent existing regulated entities (e.g. commercial banks) to deal with cryptoassets, as demonstrated by the Reserve Bank of India's 2018 ban.

## Regulated activities

**Figure 10** reveals that token creation activities are largely unregulated across selected jurisdictions. Of the analysed jurisdictions 45% have explicitly indicated that mining activities fall outside the scope of their regulatory perimeter, whereas 36% do not mention mining activities at all in their guidance/regulations. The cross-border nature of mining activities, the limited level of mining activity in many jurisdictions, and a lack of interest on the part of the regulators - either explicitly (after some study) or implicitly - may be some of the explanatory factors for the absence of precise reference to mining activities in regulators' guidance/regulations.

**Figure 10: Relevant regulations for the creation of digital tokens**



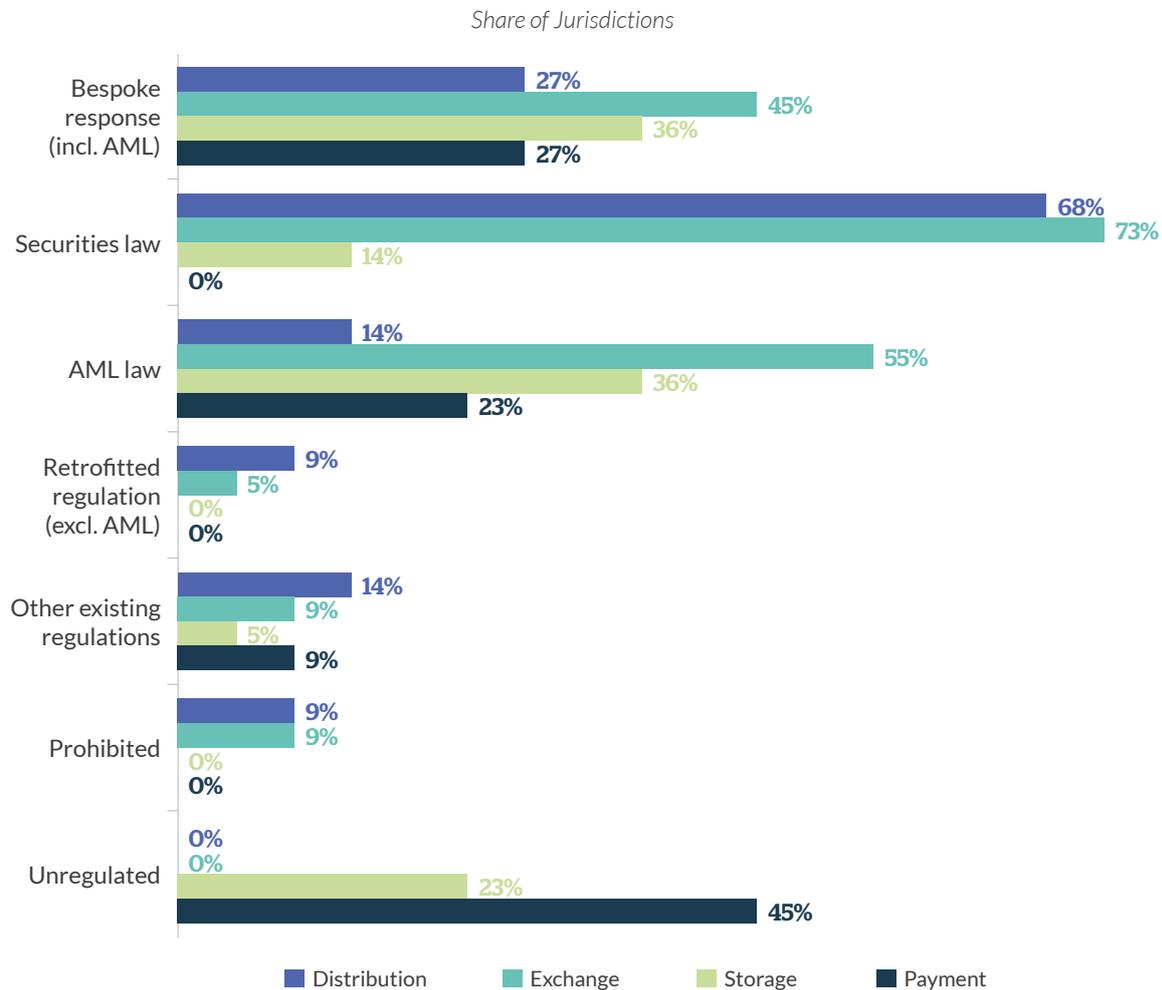
Only 5% of jurisdictions have developed a bespoke regulatory framework, such as Russia's draft bill on digital assets, or issued guidance indicating that these activities may have to comply with existing regulations (5%). For instance, BaFin in Germany considers that mining pools that offer shares in proceeds from mined cryptoassets in exchange for computing power should obtain a written authorisation to operate. Some jurisdictions have imposed restrictive measures on mining activities (9%). Unsurprisingly, these jurisdictions are also countries with a high level of mining activities (e.g. China).

**Figure 11** shows that distribution and exchange activities are regulated to a certain extent in all selected jurisdictions - regardless of the regulatory approach adopted. It should be noted that all regulators within selected jurisdictions make mention of a single distribution mechanism: token sales (including pre-token sales), better known as "initial coin offerings" or "ICOs". None of the examined official statements and regulatory documentation mentions other distribution mechanisms, such as airdrop and fork.<sup>79</sup>

<sup>79</sup> However, in a recent report, the People's Bank of China indicated planning to expand their ICO ban to airdrops. People's Bank of China (2018) *China Financial Stability Report 2018*. Available at: <http://www.pbc.gov.cn/goutongjiaoliu/113456/113469/3656006/2018110214365877856.pdf> [Last accessed: 07 February 2019].

While distribution and exchange activities are regulated in all analysed jurisdictions, 45% and 23% of jurisdictions do not regulate payment or storage activities, respectively.

**Figure 11: Relevant regulations for intermediated activities<sup>80</sup>**



As discussed above, most regulators have clearly established the distinction between cryptoassets bearing the features of a security and the other types of cryptoassets (Figure 7). If a cryptoasset qualifies as a security, distribution and secondary trading market activities automatically fall under the scope of securities law, whereas this is not necessarily the case for cryptoasset storage or payment services. Hence a large share of jurisdictions primarily regulates the distribution (68%) and the exchange of security-like tokens (73%) under securities law. The applicability of securities law triggers a variety of regulatory requirements and obligations.

For cryptoassets that do not qualify as securities, some jurisdictions have developed a bespoke regulatory response. The introduction of a bespoke regulatory regime or regulation systematically entail an amendment of AML regulations to force compliance with AML obligations. As Figure 11 highlights, bespoke responses usually cover all four intermediated activities in relatively similar proportions: 45% and 36% of jurisdictions have developed a bespoke response to regulate exchange and storage activities, respectively. Payment and distribution activities are subject to bespoke regulation in 27% of cases.

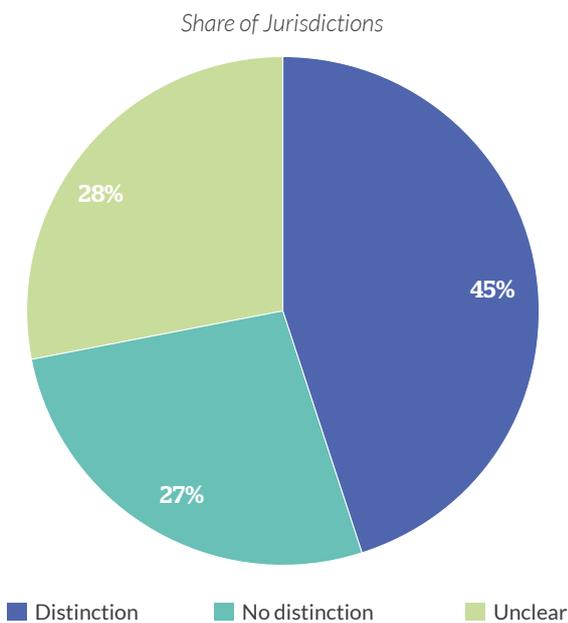
Regulators have repeatedly pointed out the risk of money laundering associated with exchange and custodial wallet services and consequently expanded the scope of their AML regulation to include these two activities. In jurisdictions where no bespoke regulatory framework has been enacted, storage

<sup>80</sup> "Bespoke response" includes the introduction of a "bespoke regulatory framework" or of a "bespoke regulation".

activities are indeed more likely to be regulated under AML law (36%) than cryptoasset distribution activities (14%) and the offering of payment services (27%), but less than exchange activities (55%).

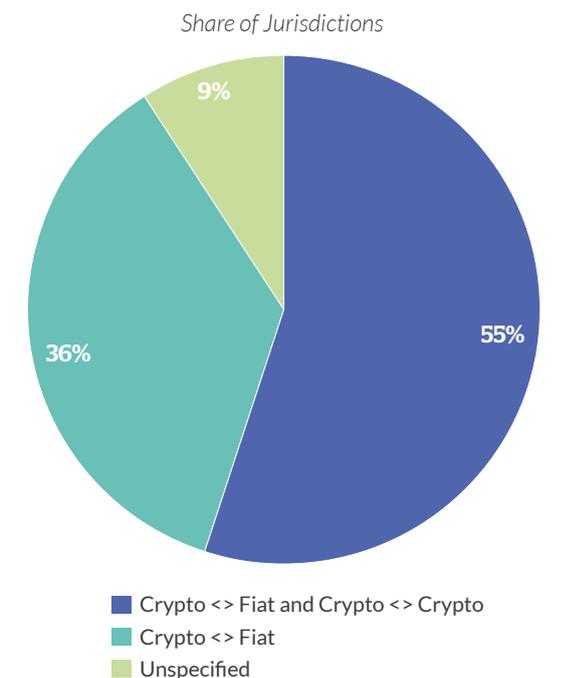
Finally, **Figure 11** also reveals that 9% of analysed jurisdictions prohibited the distribution and the exchange of cryptoassets. In the case of distribution, prohibition applies to all ICO initiatives regardless of the nature of the distributed token, whereas prohibition of cryptoasset exchange services may disregard some local regulatory particularities. For instance, the Reserve Bank of India (RBI) prohibits the dealing in cryptoassets by regulated financial entities, but cryptoasset trading through other channels is still permitted. Similarly, the ban issued by Chinese regulatory authorities only applies to cryptoasset-to-fiat exchange activities but not to cryptoasset-to-cryptoasset exchange activities.

**Figure 12: Distinction between custodial and non-custodial wallet service providers**



Furthermore, given the different interventions custodial and non-custodial services providers can carry out (e.g. authorisation to move customer funds, ability to freeze customer accounts), some regulators have decided – or expressed an intent – to regulate storage service providers that hold customers’ private keys (custodial) differently from those who do not (non-custodial). **Figure 12** shows that 45% of jurisdictions differentiate between custodial and non-custodial storage service providers, which implies that the former would be subject to additional requirements. In contrast, 27% of covered jurisdictions do not draw such a distinction. Although regulators primarily referred to storage activities when distinguishing between custodian and non-custodian, the distinction is also relevant to entities offering exchange services that take custody of user funds.

**Figure 13: Nature of regulated exchange activities**



Regulators may regulate entities offering both cryptoasset-to-fiat and cryptoasset-to-cryptoasset exchange services differently from entities only engaged in the exchange of cryptoasset against a fiat currency. Across our study sample, it appears that more than half of relevant regulations apply to entities providing both cryptoasset-to-fiat and cryptoasset-to-cryptoasset exchange services (**Figure 13**). 36% of the remaining jurisdictions consider only cryptoasset-to-fiat exchanges to fall under their regulatory perimeter.

Interestingly, three jurisdictions that adopted a regulatory framework for cryptoasset exchange activities, either by means of retrofitted regulation, bespoke regulatory regime, or bespoke regulation, have established a list of accepted cryptoassets to be traded or exchanged on the platform.<sup>81</sup> While two of those jurisdictions do not publicly disclose the list of accepted cryptoassets, the Thai SEC has announced that only Bitcoin (BTC), Bitcoin Cash (BCH), Ethereum Classic (ETC), Ethereum (ETH), Litecoin (LTC), Ripple (XRP), and Stellar (XLM) will be authorised. The list, disclosed in May 2018, is subject to change as the regulator examines the inclusion of other cryptoassets.<sup>82</sup>

Similarly, in Abu Dhabi, the Financial Services Regulatory Authority (FSRA), which does not publicly disclose the list of authorised cryptoassets, has indicated that a cryptoasset is assessed based on several factors – such as market capitalisation, cybersecurity, and market demand – in order to prevent additional risks associated with immature and illiquid cryptoassets.<sup>83</sup>

In Japan, the Financial Services Agency (FSA) does not restrict the cryptoassets that can be traded. However, to add a new cryptoasset to its platform, a licensed exchange needs to get the approval from Japan's self-regulatory organisation, the Japan Virtual Currency Exchange Association (JVCEA).

## Self-regulation

Self-regulatory initiatives emanating from the industry may play an important role in shaping regulatory regimes. The logic of industry self-regulation is that the players often have better expertise and information than regulators, as well as an incentive to design an efficient and trusted system. A risk associated with these regimes is that members begin implementing or lobbying for rules that protect their interest rather than consumers. Hence the existence of a formally authoritative hybrid, “enforced self-regulation”, in which self-regulation occurs under the aegis of an official mandate delivered by regulators. In such cases, industry performs many of the day to day functions of self-regulation, but a regulatory agency retains powers to alter the regime, or provide additional enforcement.

The study has identified only two enforced self-regulatory bodies that participate in the regulation of cryptoasset activities. In Japan, the JVCEA was approved by the Japanese financial regulator as a self-regulatory body to oversee cryptoasset activities in October 2018.<sup>84</sup> This official status grants the newly certified self-regulatory body a wide array of responsibilities, from setting industry standards to conducting on-site inspections and collecting data from its members. In Canada, the Investment Industry Regulatory Organisation of Canada (IIROC), the national self-regulatory organisation, has included the “preparation of regulation for blockchain applications and digital assets” in its 2019 priorities.<sup>85</sup>

Industry groups not explicitly tasked by governmental organisations may still contribute to regulate cryptoasset activities by, for example, developing industry standards and best practices in collaboration with regulators. One example of this approach is the Virtual Commodities Association Working Group in the USA.

Study data did not contain any instances of consumer groups participating in regulatory conversations, as they do in other financial markets, although it would not be a surprise to see them do so in the near future, given many high-profile losses in the cryptoasset space.

<sup>81</sup> The three jurisdictions are Abu Dhabi, Mexico, and Thailand.

<sup>82</sup> See Thailand in Section 4.

<sup>83</sup> See p.9 in ADGM (2018) *Guidance – Regulation of Crypto Asset Activities in ADGM*. Available at: <https://www.adgm.com/doing-business/adgm-legal-framework/guidance-and-policy-statements/adgm-wide-guidance/> [Last accessed: 02 January 2019].

<sup>84</sup> Financial Services Agency (2018) 認定資金決済事業者協会の認定について. Available at: [https://www.fsa.go.jp/news/30/virtual\\_currency/20181024-1.html](https://www.fsa.go.jp/news/30/virtual_currency/20181024-1.html) [Last accessed: 04 February 2019].

<sup>85</sup> Investment Industry Regulatory Organisation of Canada (2018) *IIROC Priorities for 2019*. Available at: [http://www.iiroc.ca/Documents/2018/84e09271-5a9a-4761-b0b6-5876d7dbfcbd\\_en.pdf](http://www.iiroc.ca/Documents/2018/84e09271-5a9a-4761-b0b6-5876d7dbfcbd_en.pdf) [Last accessed: 04 February 2019].

## Authorisation of cryptoassets

The authorisation landscape for cryptoasset activities is ever-changing, hence this study's approach is to distinguish between three approaches to authorisation:<sup>86</sup>

- **Bespoke authorisation:** an authorisation specific to cryptoasset activities created under a bespoke regulation or bespoke regulatory regime;
- **Retrofitted authorisation:** authorisation is mandatory only for selected activities (e.g. exchange, custodial wallet service providers) under retrofitted regulation;
- **Existing authorisation:** an authorisation for entities dealing with cryptoassets qualifying as a financial instrument (i.e. security) or payment instrument that is mandatory under existing laws (e.g. securities law or payment services law).

The relevant authorisation requirements are determined by the applicable regulation, which depends on the nature of the cryptoasset and the type of activities conducted by the company. Entities dealing with security-like cryptoassets are often subject to existing authorisation regimes under securities law, particularly when involved in issuance and/or exchange activities. The table on authorisation requirements (see [Appendix II](#) for a full list of requirements in the 23 analysed jurisdictions) demonstrates that bespoke and retrofitted authorisation regimes are primarily concerned with exchange and storage activities.

Some cryptoasset activities do not require any form of authorisation. Indeed, as previously shown by [Figure 10](#), only 10% of jurisdictions have brought mining activities under existing regulation or created a bespoke regulatory framework, and therefore require an authorisation. For instance, in Russia, the draft *Federal Law on Digital Financial Assets*, in its present form, will trigger specific licensing requirements and obligations for miners.

Requirements and obligations vary between different types of authorisation, as well as from one jurisdiction to another. Authorisation requirements often entail capital requirement, AML/CFT obligations, client disclosure rules, and cybersecurity measures, among others. While some jurisdictions have adopted a traditional approach, others are experimenting with alternative approaches (see, for instance, the call-out box on France's optional licensing regime).

In federal jurisdictions, such as the USA, authorisation regimes also differ across states, further fragmenting the regulatory landscape and creating new opportunities for regulatory arbitrage. For instance, in August 2015, the State of New York was the first to set up an operating license for cryptoasset activities.<sup>87</sup> Elsewhere, in the State of Wyoming, the Wyoming Blockchain Coalition has been actively engaged in developing a sound regulatory framework for cryptoasset activities to engender regulatory certainty. In early 2019, Wyoming introduced a bill to foster custody advancement for digital assets and to give *virtual currencies* (i.e. *cryptoassets* according to our narrow view) the same legal status as fiat currencies.<sup>88</sup>

<sup>86</sup> An authorisation regime includes licensing and/or registration process.

<sup>87</sup> New York State Department of Financial Services (2015) *23 NYCRR Part 200 Virtual Currencies*. Available at: <https://www.dfs.ny.gov/legal/regulations/adoptions/dfsp200t.pdf> [Last accessed: 31 January 2019].

<sup>88</sup> Wyoming State (2019) *SF0125 - Digital Assets-existing Law*. Available at: <https://wyoleg.gov/Legislation/2019/SF0125> [Last accessed: 01 February 2019].



### France's upcoming opt-in authorisation regime

French regulators have set forth an innovative licensing regime to regulate activities around cryptoassets. Under the bill Action Plan for Business Growth and Transformation (PACTE, in French), two licensing regimes would be created: one for the distribution of cryptoassets through an ICO, and one for cryptoasset service providers.<sup>89</sup> The innovation lies in the optional nature of the licensing regimes, whereby actors will not be forced to apply for a license and will be allowed to operate lawfully without a license. Only voluntary licensing applications will be examined. French regulators expect that this approach, which they refer to as the “whitelist approach” (as opposed to a blacklisting process), will incentivise viable and trustworthy undertakings to seek regulators’ approval and apply for a license.

## Regulatory sandboxes

Global interest in regulatory sandboxes is growing. As stated in the report *Early Lessons on Regulatory Innovation to Enable Inclusive FinTech: Innovation Offices, Regulatory Sandboxes and RegTech*, regulatory sandboxes are now live or planned in over 50 jurisdictions globally.<sup>90</sup> While regulatory sandboxes tend to be directed towards encouraging and supporting FinTech start-ups more generally, they could be – and are being – utilised to test cryptoasset products and services. The most common approach taken by regulators is to accept applications from firms looking to test DLT-based offerings or developing services for cryptosassets into their regulatory sandbox.

For example, since the UK FCA’s regulatory sandbox first started accepting applications in 2015, it has seen over 30% of companies accepted into the different cohorts use DLT or provide cryptoasset-related services.<sup>91</sup> By allowing firms to test DLT and cryptoassets products and services in a controlled environment, the FCA was able to work with these firms to understand their business model as well as their potential market impacts. Ultimately, the sandbox provided policymakers with hands-on experience and empirical evidence to inform the resulting cryptoasset guidance. Another example is the Abu Dhabi Global Market, which has been working with cryptoasset firms in their sandbox to consolidate their understanding of cryptoasset products and ensure their Spot Cryptoasset Framework is useful to firms.

Some regulators have gone even further and developed a regulatory sandbox entirely dedicated to cryptoassets and DLT. One such example is the Bank of Lithuania’s LBChain, which has allowed the Bank of Lithuania to gain knowledge and a deeper understanding of the technology, while creating collaboration and experience-sharing opportunities for the firms accepted in the sandbox.<sup>92</sup>

<sup>89</sup> The law is expected to be passed by mid-2019.

<sup>90</sup> UNSGSA FinTech Working Group and CCAF (2019) *Early Lessons on Regulatory Innovations To Enable Inclusive FinTech: Innovation Offices, Regulatory Sandboxes and RegTech*. Available at: <https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/early-lessons-on-regulatory-innovation-to-enable-inclusive-fintech/#.XK9x0maZNBw> [Last accessed: 01 March 2019].

<sup>91</sup> Financial Conduct Authority (2018) *Regulatory Sandbox*. Available at: <https://www.fca.org.uk/firms/regulatory-sandbox> [Last accessed: 09 February 2019].

<sup>92</sup> Bank of Lithuania (2018) *Blockchain sandbox project LBChain moving to next stage*. Available at: <https://www.lb.lt/en/news/blockchain-sandbox-project-lbchain-moving-to-the-next-stage> [Last accessed: 09 February 2019].

## Enforcement actions

A number of enforcement actions have been observed, in particular within jurisdictions with the highest levels of cryptoasset activities, such as the USA, Japan, South Korea, Switzerland and Israel. Most enforcement actions have focused on ICOs.<sup>93</sup> The US SEC has been particularly active in enforcing securities regulation on ICOs of tokens deemed securities. Regulators in a number of jurisdictions have closely watched regulatory enforcement in the USA.<sup>94</sup> In addition to post-ICO proceedings, pre-ICO regulatory warnings and orders have been used to ensure compliance, such as a strong warning to cryptoasset exchanges and ICO issuers by the Monetary Authority in Singapore.<sup>95</sup>

Cryptoasset exchange is the second type of activity that has come under regulatory scrutiny. In Japan, the FSA ordered cryptoasset exchanges to review their systemic risk management policies after a hack led to a substantial loss of cryptoassets at one of the exchanges.<sup>96</sup> In South Korea, the Korea Communication Commission (KCC) fined local cryptoasset exchanges for insufficiently protecting users' personal data.<sup>97</sup>

In addition to enforcement actions by regulators, lawsuits by consumers (cryptoasset users) may compel greater regulatory compliance, which in turn might lead to higher legal and regulatory certainty. Courts may be asked to clarify whether a particular token is a security, for instance. One example is the class action against Ripple Labs in the USA, alleging that the XRP token was a security when offered to the public.<sup>98</sup>

At times legal proceedings have also facilitated cryptoasset activities. In Israel, for example, the Supreme Court issued a preliminary injunction against a bank that refused an account from being used by a company trading in bitcoins.<sup>99</sup>

<sup>93</sup> For Hong Kong, see, e.g., Securities and Futures Commission (2018) SFC's regulatory action halts ICO to Hong Kong public. Available at: <https://www.sfc.hk/edistributionWeb/gateway/EN/news-and-announcements/news/doc?refNo=18PR29> [Last accessed: 20 February 2019]. For Switzerland, see, e.g. FINMA (2018) FINMA launches proceedings against ICO issuer. Available at <https://www.finma.ch/en/news/2018/07/20180726-mm-envion/> [Last accessed: 20 February 2019].

<sup>94</sup> The FCA's CEO has been quoted as suggesting European regulators could learn from the SEC's strong enforcement of ICOs. Law360 (2018) FCA's Bailey Sees US Crackdown On ICO Market As Model. Available at: <https://www.law360.com/articles/1110091/fca-s-bailey-sees-us-crackdown-on-ico-market-as-model> [Last accessed: 20 February 2019].

<sup>95</sup> Monetary Authority of Singapore (2018) MAS warns Digital Token Exchanges and ICO Issuer. Available at: <http://www.mas.gov.sg/News-and-Publications/Media-Releases/2018/MAS-warns-Digital-Token-Exchanges-and-ICO-Issuer.aspx> [Last accessed: 20 February 2019].

<sup>96</sup> Reuters (2018) Japan's FSA orders all cryptocurrency exchanges to report on system risk management. Available at: <https://uk.reuters.com/article/us-japan-cryptocurrency-briefing/japans-fsa-orders-all-cryptocurrency-exchanges-to-report-on-system-risk-management-idUKKBN1FM08L> [Last accessed: 20 February 2019].

<sup>97</sup> Korea Communication Commission (2018) 가상통화 거래사이트, 개인정보 보호조치 매우 미흡. Available at: <https://kcc.go.kr/user.do?boardId=1113&page=A05030000&dc=K00000001&boardSeq=45407&mode=view> [Last accessed: 20 February 2019].

<sup>98</sup> Vladi Zanicov et al. v. Ripple Labs et al. (N.D.Cal.). Coindesk (2018) Combined Class-Action Lawsuit Against Ripple Moves to Federal Court. Available at: <https://www.coindesk.com/combined-class-action-lawsuit-against-ripple-moves-to-federal-court> [Last accessed: 20 February 2019].

<sup>99</sup> CA 6389/17 (2018) Bits of Gold Ltd. v. Bank Leumi Lelsrael Ltd.

# SECTION 3: REGULATORY CHALLENGES

---

Jurisdictions around the world have encountered a number of challenges when addressing regulatory issues surrounding cryptoassets. Section 1 highlighted some of the key issues that arise as a result of the conceptualisation and classification of cryptoassets and related activities. The comparative analysis in Section 2 helped identify potential gaps in the development and implementation of cryptoasset regulations.

This section brings together key takeaways from previous sections and provide regulators and policymakers with additional considerations for regulating cryptoasset-related activities. Regulatory challenges have been identified at each stage of the decision-making process (i.e. assessing the scope of activities, determining the regulatory perimeter, identifying potential risks and harms, and gauging the suitability of existing regulations).

## 3.1 Mapping Cryptoasset Activities

Regulators have increasingly sophisticated knowledge of the complexities and intricacies of cryptoassets and the underlying DLT. However, some technical features of cryptoassets have not yet received much regulatory attention, and some industry actors have been largely overlooked.

### Data availability and quality

---

Data on cryptoasset activities, especially with regards to token creation, distribution, and secondary trading is often incomplete, unreliable, or unavailable. Information is disparately located between many distinct, disconnected services and often hard to verify. Frequent changes to projects are often not reflected in publicly available data sources, which may lead to an inaccurate view of a given project's status. The quality of exchange trading data varies significantly from one platform to another, making it difficult to get a reliable macro-view of monetary flows in and out of the ecosystem.

Improving data collection on cryptoasset activities, both at the domestic and international level, is crucial for regulators to understand the risks and opportunities that can significantly impact their regulatory objectives. Broader and more detailed empirical datasets can be sourced directly from market participants (e.g. through registration and authorisation processes), industry associations, academia, or other regulatory bodies. There are a number of market efforts to create a curated, trusted information source through the transparent aggregation of diverse data sources (e.g. data services firm Messari building the “EDGAR database for cryptoassets”).<sup>100</sup>

### Infrastructure providers: miners, developers, and nodes

---

Some cryptoasset infrastructure providers, maintainers, and operators (e.g. developers, miners, and node operators) have received little to no attention in regulatory frameworks thus far, or have not been clearly exempted from existing regulations. Regulators may use terms such as “issuing virtual currency”, without clarifying whether this excludes infrastructure-related activities.

---

<sup>100</sup> Selkis, R. (2017) Introducing Messari: An Open-Source EDGAR Database for Cryptoassets. *Medium*. Available at <https://medium.com/tbis-weekly-bits/introducing-messari-an-open-source-edgar-database-for-cryptoassets-46fec1b402f6> [Last accessed: 06 March 2019].

One example is mining activities, which few regulatory frameworks mention. An exception is Russia's draft *Federal Law on Digital Financial Assets*, whereby miners are required to obtain a license based on their level of activity (dependent on energy consumption).

Likewise, the role of developers has been largely ignored to date. Some blockchain protocols and systems have become highly centralised, i.e. a small number of core developers may hold the power to change the system's ruleset, and subsequently key properties.<sup>101</sup> There have been suggestions to consider expanding fiduciary duties to protocol developers with highly centralised governance rights, although these proposed measures have been met with resistance.<sup>102</sup> Others have argued that the *comply-or-explain* approach typically used for corporate governance could be applied to cryptoasset companies to increase transparency of governance and protect cryptoasset users.<sup>103</sup>

Finally, some have argued that node operators may be liable for unlawful uses of a DLT system. Under the EU's General Data Protection Regulation (GDPR), node operators could face liability as so-called "data controllers" because they actively run the software and have a say in protocol upgrades.<sup>104</sup> However, the EU Blockchain Observatory suggested otherwise, recommending that developers — as well as node operators on public, permissionless blockchains — should probably not be held liable under the GDPR.<sup>105</sup>

Liability of infrastructure providers and operators may need to be assessed differently depending on the layer of the DLT system on which they operate and the role they fulfill. For example, regulators may decide to treat developers of a particular DLT-based *application* differently from developers of the underlying DLT *protocol*. Likewise, those involved in issuing a particular cryptoasset contract may be treated differently by regulators than those producing records (e.g. mining blocks). Those involved in developing public, permissionless protocols could be subjected to different liability standards than those developing private, permissioned protocols. Regulators will eventually need to decide which of these activities should comply with existing regulations, be subjected to bespoke regulation, or remain unregulated.

## Airdrops and forks

ICOs have been on most regulators' radar, whereas other mechanisms of token distribution, such as airdrops and forks, have received very little or no attention; with the exception of the People's Bank of China, which announced the possibility to extend its ICO ban to airdrops labelled as "disguised ICOs".<sup>106</sup>

A set of questions would need to be answered by regulators in order to understand where and what regulatory intervention is needed for these other distinct distribution mechanisms. One unanswered question is who, if anyone, should be considered responsible for the token issuance in case of a fork. In the event of a fork, network participants and service providers (e.g. miners, node operators, developers, exchanges, wallets, etc.) ultimately decide which side of the fork to support. For instance, in the case of

<sup>101</sup> For further discussion on protocol governance, see 5.1.2 Alteration Component (pp. 55-57) in Rauchs, M. et al. (2018) *Distributed Ledger Technology Systems: A Conceptual Framework*. Cambridge Centre for Alternative Finance. Available at: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3230013](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3230013) [Last accessed: 15 January 2019].

<sup>102</sup> Walch, A. (2019) In Code(rs) We Trust: Software Developers as Fiduciaries in Public Blockchains. *Regulating Blockchain. Techno-Social and Legal Challenges*. Available at: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3203198](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3203198) [Last accessed: 08 March 2019].

<sup>103</sup> Hacker, P. (2017) *Corporate governance for complex cryptocurrencies? A framework for stability and decision making in blockchain-based organizations*. Available at: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2998830](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2998830) [Last accessed: 22 February 2019]. Hacker proposes a Blockchain Governance Code, with each blockchain-based organisation deciding whether to comply with the Code's provisions or explain why it does not wish to comply with any of its provisions.

<sup>104</sup> The EU Forum and Observatory on Blockchain (2018) *Blockchain and the GDPR*. Available at: <https://www.eublockchainforum.eu/reports> [Last accessed: 16 February 2019].

<sup>105</sup> Idem.

<sup>106</sup> People's Bank of China (2018) *China Financial Stability Report 2018*. Available at: <http://www.pbc.gov.cn/goutongjiaoliu/113456/113469/3656006/2018110214365877856.pdf> [Last accessed: 14 February 2019].

a hard fork, custodial service providers may be assigned the responsibility of selecting the appropriate chain on behalf of their clients, and credit newly created tokens accordingly.<sup>107</sup> A hard fork may also require so-called “replay protection” for users, which could be implemented by developers of the newly forked blockchain or through custom solutions offered by wallet providers.<sup>108</sup>

Forks create a substantial opportunity for “wealth-tunnelling” (i.e. the use of rights within a system to transfer wealth from one group to another in a legal but improper manner) and things akin to minority shareholder oppression. For example, forks could be created by majority holders to change governance and profit rights of minority holders. If minority holders refuse to run the newly forked chain, they may be left with worthless cryptoassets.<sup>109</sup>

While airdrop claims may appear risk-free, it involves security risks and may create privacy concerns; claiming airdropped tokens requires users to sign a transaction with the private key associated with a specific address. Performing this action in a compromised environment (e.g. infected computer) may result in the loss of all funds associated with that address – including the original tokens.<sup>110</sup> Moreover, a distributor may set specific conditions for a claim (e.g. provide personal details to fulfill compliance requirements), which might result in disclosure of private information to third parties or a risk of data breach. Apart from collecting personal information, many airdrops have been criticised for their weak privacy practices (for instance, MoneroV’s airdrop attempt in April 2018).<sup>111</sup>

## Decentralised exchanges (DEXes)

Despite being in their infancy, decentralised exchanges raise new concerns for regulators given their (supposedly) decentralised nature. While most regulatory responses have only focused on centralised or peer-to-peer exchanges, it remains unclear whether DEXes are included and, if so, how regulatory requirements can be enforced for this type of exchange.<sup>112</sup>

Some steps to address this regulatory challenge could be to gauge the level of decentralisation of these exchanges, clarify the applicability and enforcement of AML/CFT and CDD, and assess whether practices (e.g. collecting transfer fees) may automatically bring them under existing regulation. For instance, the Monetary Authority of Singapore (MAS) is considering changes to its market monitoring rules that would extend AML/CFT and KYC obligations to decentralised exchanges.<sup>113</sup>

<sup>107</sup> Currently, custodial storage providers have sole discretion over deciding whether to credit customer balances with an equal amount of forked tokens.

<sup>108</sup> In case of a hard fork, a blockchain is split into two different chains. Tokens held on the chain before the fork will now exist on both chains after the fork. If Alice decides to spend her tokens in a transaction on one chain, her signature information from that transaction could be copied by Bob to spend Alice’s tokens on the other chain, even without Alice’s consent (‘replay’). Replay protection ensures that Alice’s transaction on one chain cannot be copied (replayed) on the other chain. Different types of replay protection exist.

<sup>109</sup> The first high-profile fork was in the context of TheDAO, which was effectively a collective investment scheme that purported to be a form of post-corporate ‘virtual’ entity but became the subject of an SEC investigative report. After a hacker stole millions of dollars worth of ether from The DAO by exploiting a vulnerability in the smart contract, Ethereum developers decided to create a hard fork on the Ethereum blockchain to move funds locked in TheDAO smart contract to a new smart contract to enable affected token holders to withdraw their funds. However, we could imagine a different scenario, in which a fork is created that benefits a majority of DAO members but disadvantages minority members (e.g. by taking away governance or profit rights from minority members).

<sup>110</sup> The same issue applies to hard forks: for instance, claiming Bitcoin Cash (BCH) after the 2017 hard fork exposed Bitcoin users to the risk of losing both their BTC and BCH associated with the same address.

<sup>111</sup> O’Leary R. (2018) Airdrop Attack? Monero Fork Condemned as Privacy Threat. *Coindesk*. Available at: <https://www.coindesk.com/airdrop-attack-coming-monero-fork-condemned-as-privacy-threat> [Last accessed: 17 January 2019].

<sup>112</sup> The autonomous (and supposedly leaderless) nature of a DEX complexifies the enforcement of regulatory requirements such as AML and KYC checks on the platform.

<sup>113</sup> Monetary Authority of Singapore (2018) *Consultation Paper - Review of the Recognised Market Regime*. Available at: <http://www.mas.gov.sg/~media/MAS/News%20and%20Publications/Consultation%20Papers/2018%20May%2022%20RMO%203P/Consultation%20Paper%20on%20RMO%20Regime.pdf> [Last accessed: 19 February 2019].

## Privacy coins

Highly private cryptoassets (sometimes called “privacy coins”), such as Zcash, Monero, and Grin, present some unique considerations for regulators. Regulators are often able to track cryptoasset transactions by using metadata stored on the relevant blockchain and applying pattern analysis. Given that a design specification of privacy coins’ underlying software is to make it more difficult to track on-chain transactions, privacy coins are in theory a particular challenge for AML/CFT, tax avoidance, and illicit trade. Although they may not achieve full anonymity<sup>114</sup> and their current use remains relatively small in terms of transaction volume, privacy coins may require particular attention from regulators. Some regulators have started looking into privacy coins, for instance, the Japanese FSA has indicated its intention to tighten regulations on intermediaries handling privacy coins.<sup>115</sup>

## Stablecoins

Stablecoins are cryptoassets designed to maintain price stability, either in relation to a pegged asset or a basket of goods (“purchasing power”). Stablecoins can be classified into two major categories:

- **Asset-backed:** the stablecoin is backed by collateral in the form of an asset (or basket of assets). Conventional assets (financial and non-financial, e.g. fiat currency and gold) as well as cryptoassets (e.g. bitcoin, ether) can be used as collateral, which is generally held in custody by the stablecoin issuer.
- **Algorithmic:** smart contract programmed to regulate issuance and redemption of the stablecoin to match supply and demand, and hence reduce price volatility.

Stablecoins have recently gained in popularity, especially among traders who use them for arbitrage between cryptoasset exchanges. This development has raised questions regarding the regulatory treatment of stablecoins and the intermediaries dealing with them. The regulatory response remains unclear to date in most jurisdictions as a result of the substantial differences that exist between stablecoins; asset-backed stablecoins and algorithmic stablecoins are likely to fall under different sets of regulation.

Fiat-backed stablecoins constitute a new form of electronic money and will thus be regulated under E-money, AML/CFT, and other relevant regulations, as indicated for instance by the FCA in the UK and by the New York Department of Financial Services (NYDFS) in the USA.<sup>116</sup> Applicable regulations to other conventional asset-backed stablecoins will depend on the nature of the collateral.

There is greater ambiguity on cryptoasset-backed and algorithmic-based stablecoins. In jurisdictions where cryptoassets are explicitly regulated (either under existing regulations or under a bespoke regulatory framework), cryptoasset-backed stablecoins are expected to abide by the same regulations. However, algorithmic stablecoins, that attempt to maintain price stability via the use of algorithms that control and adjust the supply, have not been on the radar of regulators to date.

Given the on-chain nature of cryptoasset-backed and algorithmic stablecoins, they should theoretically provide greater transparency to holders than conventional asset-backed stablecoins as reserves (or the supply matching algorithm, respectively) are auditable.

While these types currently only represent a relatively small share of the existing stablecoin market, there are concerns over long-term stability prospects and the additional exposure to cybersecurity risks.

<sup>114</sup> Kappos, G. et al. (2018) *An Empirical Analysis of Anonymity in Zcash*. Available at: <https://www.usenix.org/system/files/conference/usenixsecurity18/sec18-kappos.pdf> [Last accessed: 22 February 2019].

<sup>115</sup> For further information, please see <https://www.fsa.go.jp/news/30/singi/kasoukenkyuukai.html> [Last accessed: 07 January 2019].

<sup>116</sup> New York Department of Financial Services (2018) *DFS Continues to Foster Responsible Growth in New York’s Fintech Industry with New Virtual Currency Product Approvals*. Available at: <https://www.dfs.ny.gov/about/press/pr1809101.htm> [Last accessed: 07 March 2019].

## 3.2 Establishing a Clear Regulatory Perimeter

### Lack of clear terminology

The absence of consensus over terminology, definitions, and classification can be a key barrier to the development of a robust regulatory framework and may hamper further regulatory harmonisation across jurisdictions. Given the inherent cross-border nature of cryptoasset transactions, diverging interpretations of terms among regulatory bodies may facilitate regulatory arbitrage. In general, regulators can take steps to develop more suitable and robust definitions and classifications by gathering empirical evidence and engaging key stakeholders, including other regulators.

With regards to token classification, regulators can consider some of the questions listed below to help them develop their own framework:

1. Which cryptoassets are similar in nature to traditional assets and can therefore fit into the existing regulatory framework?
2. Is a distinction warranted between cryptoassets on open and permissionless DLT systems as opposed to cryptoassets on private, permissioned infrastructure?
3. Should a differentiation be made between tokens that are a tokenised representation of traditional assets and tokens that constitute new assets by themselves?
4. For a hybrid token (e.g. a payment token that is also a security token), will laws be applied cumulatively (i.e. both payments and securities laws) or hierarchically?

### Regulatory arbitrage

The lack of harmonised and coordinated regulatory responses allows cryptoasset market participants to exploit regulatory loopholes and circumvent stringent regulations.

International regulatory collaboration and cooperation can mitigate potential harms of regulatory arbitrage by creating a more consistent, harmonised, and coordinated regulatory framework, in addition to enforcement measures across jurisdictions. These have been the key objectives of existing supranational and intergovernmental bodies: for instance, the FATF aims to facilitate AML/CFT regulatory harmonisation among its member states.

In this context, the “geopolitics of digital governance” may contribute to divergent regulatory responses as regulators in different jurisdictions pursue a regulatory strategy consistent with their state’s approach to the Internet generally.<sup>117</sup> This may, in turn, affect the nature and scope of international regulatory cooperation.

### Enhanced clarity over regulatory supervision

At the national level, defining the boundaries of national regulatory bodies and their responsibilities is necessary to provide further clarity over regulatory supervision to both industry players and users. When a Canadian exchange was declared bankrupt and likely to have lost \$190 million in investor assets in early 2019, investors were surprised to learn that the country’s first licensed exchange was not actually supervised by any regulator. The average investor is unlikely to discern between a license from an AML authority (in this case FINTRAC) and supervision by the securities and exchange regulator, in this case the British Columbia Securities Commission.

Enhanced regulatory clarity can have significant impact on cryptoasset markets: it is commonly believed that clearer regulatory oversight would foster trust and attract new types of customers in the

<sup>117</sup> For example, the Californian “open Internet” model has been contrasted to the Washington DC “commercial Internet”, the Chinese “authoritarian Internet”, the European “bourgeois Internet”, and certain states have been criticised for using the Internet as a vector for bad-faith interference. See O’Hara, K. & Hall, W. (2018) *The Four Internets: The Geopolitics of Regulatory Governance*. Available at: <https://www.cigionline.org/publications/four-internets-geopolitics-digital-governance> [Last accessed: 08 March 2019].

cryptoasset market, such as institutional investors whose growing appetite for cryptoassets is generally believed to have been withheld because of lack of regulatory certainty.

### Limitations of technology-neutrality (substance over form) principle

Several regulators adopted an approach focussing on substance over form, whereby new technologies are treated on par with existing technologies. The principle of technology neutrality enjoys wide in-principle acceptance but is not always fleshed out in sufficient detail. In broad terms, it is usually taken to mean that rules should not require or assume a particular technology and that rules should not hinder the use or development of technologies in the future, or (what is closely related) that rules should apply equally online and offline and that rules through not favour one or the other technology.<sup>118</sup>

While an obvious *desideratum* of regulation of new forms of commercial and financial activity, there are limits to this approach in practice. For example, if taken to mean “technology indifference”, the drafters of regulation might simply find it impossible to address cryptoassets effectively at all. For example, as bitcoins do not qualify as “things” capable of ownership under certain civil codes, it would be necessary to address the question specifically, for example by making cryptoassets “property” by dint of legal fiction.<sup>119</sup> This already impinges on the idea of not assuming any technology when drafting regulations.

The nature of disruptive innovation is that it does things that were not obvious previously, perhaps least of all to regulators. In other words, technology-neutrality may be more of an ideal that guides regulators than something that can be said of existing regulations at any given time.

## 3.3 Identifying Potential Risks

### Consumer protection and information disclosure

The G20 OECD Financial Consumer Protection Principles, covering acts, and regulations but also both statutory and voluntary codes, assert that consumer protections should address:

- Financial literacy and education;
- Access to basic financial products and services;
- Disclosure requirements and transparency,
- Responsible business conduct;
- Lending practices;
- Data protection and privacy; and
- Effective resolution schemes/complaint handling mechanisms.<sup>120</sup>

Other key issues include access to best execution price, segregation of customers’ funds from those of any custodian or other intermediary, and questions of suitability of investment. Such principles may be equally necessary for certain aspects of cryptoassets. Exchanges, issuers and custodians, for example, may be assigned numerous responsibilities which closely match the equivalent functions - and therefore responsibilities - as regards to traditional assets.

<sup>118</sup> See for example the US Government *Framework for Global Electronic Commerce* (1997) and the *Bonn Ministerial Conference Declaration of 6-8 July 1997* (1997) in Reed, C. (2007) *Taking Sides on Technology Neutrality*. SCRIPT-ed 4(3).

<sup>119</sup> As suggested in the recent position paper by the German Federal Ministry of Finance and the Federal Ministry of Justice and Consumer Protection, *Eckpunkte für die regulatorische Behandlung von elektronischen Wertpapieren und Krypto-Token* (7 March 2019). Available at: [https://www.bundesfinanzministerium.de/Content/DE/Standardartikel/Themen/Internationales\\_Finanzmarkt/2019-03-08-eckpunkteelektronische-wertpapiere.pdf?\\_\\_blob=publicationFile&v=2](https://www.bundesfinanzministerium.de/Content/DE/Standardartikel/Themen/Internationales_Finanzmarkt/2019-03-08-eckpunkteelektronische-wertpapiere.pdf?__blob=publicationFile&v=2) [Last accessed: 18 March 2019].

<sup>120</sup> G20/OECD Task Force on Financial Consumer Protection (2011) *G20/OECD High-Level Principles on Financial Consumer Protection*. Available at: <http://www.oecd.org/daf/fin/financial-markets/48892010.pdf> [Last accessed: 05 March 2019].

There are often multiple points of supervision and control for these areas, such as exchange regulators (government or self-regulated), data protection agencies, securities commissions, financial ombudsmen and even general consumer protection agencies. Industry players must be cognisant of their responsibilities under each of these regulatory touchpoints, but especially as regards securities laws. Some laws may be easily applied to the new cryptoasset markets. On the other hand, while a number of regulators have identified most of the risks associated with cryptoassets and issued warnings cautioning users of these perceived risks, fraudulent activities still persist. Consumers may acquire cryptoassets without being aware of regulatory protections available to them, resulting in irreparable damages.<sup>121</sup> Regulators may need to implement new regulations to cover the idiosyncrasies of cryptoasset businesses, such as non-custodial wallet.

## Systemic risks

---

Regulators generally believe that cryptoasset markets currently do not present systemic risk to existing financial systems thus far.<sup>122</sup> However, they may begin to pose risks to financial stability should cryptoassets continue to grow as an asset class and mainstream financial entities increase their exposure to them. This risk is exacerbated by the cross-border nature of the cryptoasset markets: entities (including some of systemic importance) in one jurisdiction might be exposed to cryptoassets (and related activities) that are largely outside that jurisdiction's regulatory control. Systemic risks may become obvious only in hindsight and may need to be addressed counter-cyclically rather than pro-cyclically (i.e. after a risk has eventuated). It is therefore particularly important to monitor financial stability risks on an ongoing basis.

---

<sup>121</sup> Shifflett, S. & Jones, C. (2018) Buyer Beware: Hundreds of Bitcoin Wannabes Show Hallmarks of Fraud. *Wall Street Journal*. Available at: <https://on.wsj.com/2GsCV2e> [Last accessed: 20 February, 2019].

<sup>122</sup> See for instance the European Central Bank (2018) *Virtual Currencies Ante Portas*. Available at: <https://www.ecb.europa.eu/press/key/date/2018/html/ecb.sp180514.en.html> [Last accessed: 21 February 2019]

## SECTION 4: CASE STUDIES

The following case studies are organised according to the four types of regulation described in Section 2, namely existing regulation, retrofitted regulation, bespoke regulation, and bespoke regulatory regime. To facilitate reading, “bespoke regulatory regime” and “bespoke regulation” have been merged together. Both automatically entail the applicability of AML/CFT law.

Bills that have not been passed yet are included in the classification. For instance, Russia’s law on digital financial assets has been classified as “bespoke regulation”, while Canada’s amendments to AML law have been categorised as “retrofitted regulation”. The same approach was used for transpositions of supranational instruments into national law that have not occurred yet (e.g. the transposition of 5AMLD in the UK or Germany, due by January 2020).

Finally, relevant regulations listed in the European Union case study also apply to jurisdictions that are member states of the EU. As a result, they have not been explicitly listed in these case studies (Estonia, France, Germany, Malta, and the UK).

### Bespoke Regulatory Regime and/or Regulation

#### Abu Dhabi

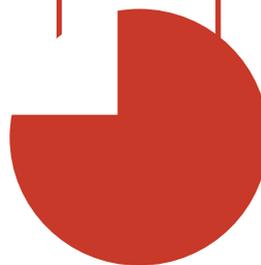


#### RESPONSIBLE REGULATORY AUTHORITIES

Financial Services  
Regulatory Authority (FSRA)

#### RELEVANT REGULATIONS

Spot Crypto Asset Framework  
Financial Services and Market Regulations (FSRM)



Date of enforcement of bespoke regulatory regime [Crypto Asset Spot Framework, 2018]:  
June 25, 2018

#### Cryptoasset Definition and Terminology

The Spot Crypto Asset Framework defines a *crypto asset* as:

*a digital representation of value that can be digitally traded and functions as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but does not have legal tender status in any jurisdiction. A Crypto Asset is (a) neither issued nor guaranteed by any jurisdiction, and fulfils the above functions only by agreement within the community of users of the Crypto Asset; and (b) distinguished from Fiat Currency and E-money.*<sup>123</sup>

<sup>123</sup> Abu Dhabi Global Market (2018) *Guidance – Regulation of Crypto Asset Activities in ADGM*. Available at: <https://www.adgm.com/doing-business/adgm-legal-framework/guidance-and-policy-statements/adgm-wide-guidance/> [Last accessed: 02 January 2019].

## Relevant Regulations

The FSRA's *Guidance – Regulation of Initial Coin/Token Offerings (ICOs) and Crypto Assets* and *Guidance – Regulation of Crypto Asset Activities in Abu Dhabi Global Market*, together called the *Spot Crypto Asset Framework*, were issued under the *Financial Services and Market Regulations* established in 2015 (2015 FSRM) and were published on October 8, 2017 and June 25, 2018 respectively. The scope of the *Spot Crypto Asset Framework* is limited to the Abu Dhabi Global Market (ADGM).

The FSRA has full power to create, amend, and revoke legislation in the ADGM. The ADGM is exempt from regulation issued by the United Arab Emirates (UAE) 's financial regulators including the Central Bank and the Securities and Commodities Authority (SCA).

The Spot Crypto Asset Framework introduces a new type of regulated activity, referred to as “Operating a Crypto Asset Business” (OCAB). This approach allows the regulator to treat this new type of activity similarly to existing activities albeit with new rules. These rules apply to businesses incorporated in and/or operating in Abu Dhabi. Such businesses have to comply with specific requirements and apply for licensing with the FSRA.<sup>124</sup> Of note, the FSRA considers cryptoasset exchanges and custodians as activities that require further regulatory oversight. Exchanges should meet additional market infrastructure rules and custodians should meet conduct of business rules.<sup>125</sup>

The Spot Crypto Asset Framework also provides the FSRA with the power to determine a whitelist of accepted cryptoassets. Only listed cryptoassets can be used to carry out cryptoasset activities (e.g. exchange, storage) within the ADGM. The acceptance of a cryptoasset as an “Accepted Crypto Asset”, is based on several conditions, such as market capitalisation, cybersecurity, and market demand. The objective is to prevent additional risks that might be associated with immature and illiquid cryptoassets. The *Accepted Crypto Asset* list is not disclosed to the public.

With regards to ICOs, the FSRA's ICO Guidance contains a classification of cryptotokens based on the nature of the token, with each determination made on a case-by-case basis.<sup>126</sup>

- **Security tokens:** are treated like any other security and regulated under the 2015 FSRM, approved by the FSRA and recognised as a Financial Services Permission holders, Recognised Investment Exchanges or Recognised Clearing Houses. In most cases, a Prospectus is required;<sup>127</sup>
- **Cryptoassets:** intermediaries fall under the Spot Crypto Asset Framework, described above, and will have to hold an OCAB stipulation on its Recognition Order and be licensed as an OCAB holder;
- **Utility tokens:** are not cryptoassets. The issuance of utility tokens via an ICO is not considered as a regulated activity.

## Future Outlook

Regulators and officials expect that the implementation of the bespoke regime will contribute to make Abu Dhabi a jurisdiction of choice for cryptoasset businesses and position it as a leader in the cryptoasset space.

<sup>124</sup> These specific requirements are set out in a new chapter of the FSRA *Conduct of Business Rules* (COBS) and the 2015 *Financial Services and Market Regulations* (FSRM) and include capital requirement, AML/CFT, appropriate technology governance and controls, risk disclosure.

<sup>125</sup> P.25 of Abu Dhabi Global Market (2018) *Guidance - Regulation of Crypto Asset Activities in ADGM*. Available at: <https://www.adgm.com/media/327606/guidance-regulation-of-crypto-asset-activities-in-adgm-25th-june-2018-2.pdf> [Last accessed: 02 January 2019].

<sup>126</sup> A similar approach has been observed in other jurisdictions, such as the FINMA in Switzerland.

<sup>127</sup> The regulation sets out a set of criteria under which a business would be exempt to publish a Prospectus.

## Bermuda



### RESPONSIBLE REGULATORY AUTHORITIES

Bermuda Monetary Authority (BMA)

### RELEVANT REGULATIONS

Digital Asset Business Act  
Companies (Initial Coin Offering) Regulations  
Limited Liability Company (Initial Coin Offering) Regulations



Date of enforcement of bespoke regulation [Digital Asset Business Act, 2018]: September 10, 2018

### Cryptoasset Definition and Terminology

The regulation defines a *digital asset* as:

*anything that exists in binary format and comes with the right to use it and includes a digital representation of value that— is used as a medium of exchange, unit of account, or store of value and is not legal tender, whether or not denominated in legal tender; is intended to represent assets such as debt or equity in the promoter; is otherwise intended to represent any assets or rights associated with such assets; or is intended to provide access to an application or service or product by means of distributed ledger technology; but does not include— a transaction in which a person grants value as part of an affinity or rewards program, which value cannot be taken from or exchanged with the person for legal tender, bank credit or any digital asset; or a digital representation of value issued by or on behalf of the publisher and used within an online game, game platform, or family of games sold by the same publisher or offered on the same game platform.*<sup>128</sup>

### Relevant Regulations

As the sole financial services regulator in the country, the BMA has a full suite of powers to regulate cryptoasset activities. The *Digital Asset Business Act* (DABA) empowers the BMA to supervise cryptoasset exchanges, storage service providers, payment service providers, cryptoasset service vendors and any entity assisting in the issuance of cryptoasset, such as coin and token design, administration of the ICO process. In addition to the AML/CFT regulation amendments which include cryptoasset undertakings, the prudential regulatory framework seeks to prevent fraud, price manipulation and ensure the integrity of owners. Activities captured by the DABA are referred to as *Digital Asset Businesses*.<sup>129</sup>

Mining and contributing to the protocol of a cryptocurrency (i.e. developers writing and reviewing the code underlying the DLT (e.g. Bitcoin Core) are not regarded as a *Digital Asset Business* and therefore are not a regulated activity in Bermuda.

An ICO launched in order to fund one's own company is regulated under the *Companies (Initial Coin Offering) Regulations 2018* and *Limited Liability Company (Initial Coin Offering) Regulations 2018*. Under the amended legislation, businesses conducting an ICO are treated as a restricted business activity and

<sup>128</sup> The Government of Bermuda (2018) *Digital Asset Business Act*. Available at: <http://www.bermulaws.bm/laws/Annual%20Laws/2018/Acts/Digital%20Asset%20Business%20Act%202018.pdf> [Last accessed: 11 March 2019].

<sup>129</sup> Idem.

subject to compliance reporting. Consent from the Ministry of Finance is required. ICO requirements set forth in the regulations include, for instance, a white paper modelled on existing requirements for IPOs to provide sufficient information to customers.

Digital Asset Business must adhere to licensing requirements. Two types of license exist. The first one (class F) is a full and permanent license granted to established businesses in the cryptoasset industry. The second one (class M) is temporary and licenses intermediaries for a defined period of time set by the BMA. The latter is tantamount to a regulatory sandbox. The BMA is the sole decision-maker in determining which license should apply. It also has the power to impose a penalty, or to restrict or revoke any granted license. It should be noted that no ownership and licensing requirement will be imposed merely by virtue of holding digital assets, unless the person does it so in the course of business. In this case, they would be regarded as a digital asset services vendor and subject to *DABA*.

Licenses require the nomination of a senior representative of the company, the establishment of a head office in Bermuda, preparation of annual audit accounts, and the payment of license fees.<sup>130</sup> A code of practice and additional explanatory guidelines on risk management, cybersecurity and client disclosure rules further protect consumers against inherent cryptoasset risks.<sup>131</sup>

The *DABA* provides that licensed custodial intermediaries should maintain indemnity insurance, a surety bond or a trust account with a qualified custodian. In addition to this, licensed businesses that control cryptocurrencies on behalf of their clients must maintain a “sufficient amount” of each virtual currency.<sup>132</sup>

### Future Outlook

Several industry players have already supported Bermuda’s initiative by investing in blockchain activities on the Island, while others have announced the establishment of an office in Bermuda.<sup>133</sup>

---

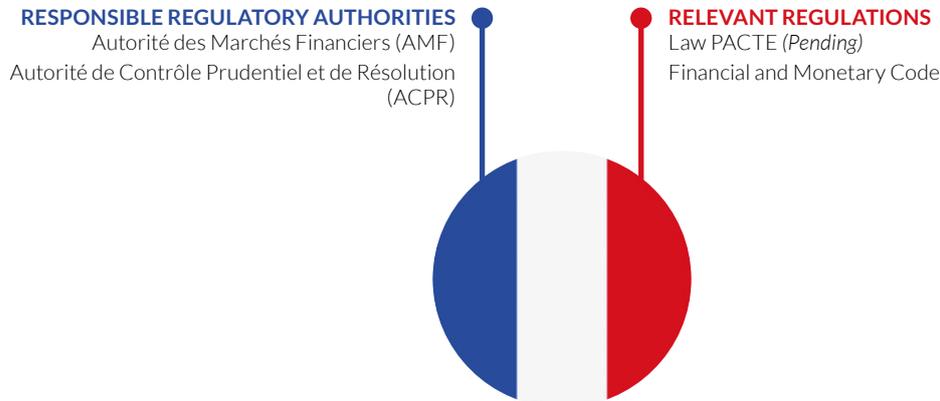
<sup>130</sup> Idem.

<sup>131</sup> Full documentation is available at: <http://www.bma.bm/document-centre/consultation-papers/SitePages/Digital%20Asset%20Business.aspx>

<sup>132</sup> “Sufficient amount” is not explicitly defined in the legislation.

<sup>133</sup> Bermuda News (2018) *Premier sign MOU with Binance*. Available at: <http://bernews.com/2018/04/live-video-premier-david-burt-press-conference-2/> [Last accessed: 02 January 2019].

## France



Expected date of enforcement of bespoke regulatory regime [Law PACTE, 2018]: mid-2019

### Cryptoasset Definition and Terminology

The forthcoming law *Business Growth and Transformation Action Plan* (PACTE Law) defines a token as:

*any intangible asset representing, in digital form, one or more rights, which may be issued, registered, retained or transferred by means of a distributed electronic ledger that identifies, directly or indirectly, the owner of such asset.*<sup>134</sup>

It also defines a *digital asset* as:

*any digital representation of value which is not issued by a central bank or a public authority, not necessarily linked to a legal tender, and does not possess the legal status of currency, but which is accepted by any natural and legal person as a means of exchanges and can be transferred, stored, or exchanged electronically.*<sup>135</sup>

### Relevant Regulations

#### Payment services

Cryptoassets are not recognised as a means of payment and are not classified as legal tender by French regulators. However, if a trading platform collects funds in fiat money from the payer in order to transfer them to the seller, it may fall under the legal category of payment service provider, a regulated activity that requires a license from the ACPR.<sup>136</sup> Furthermore, businesses involved in stable value tokens may require a license if they operate as electronic money issuer.<sup>137</sup> A license is not required when a trading platform sells its own cryptoasset.

#### AMF optional label

After a public consultation in late 2017, the AMF proposed the introduction of an optional authorisation regime (“AMF optional visa”) for ICO projects. Under this regime, entities planning to launch an ICO will be able to solicit an optional visa from the AMF to confirm their compliance with best practices on users’

<sup>134</sup> As currently adopted by the Senate, see National Assembly (2019) *Projet de loi modifié par le Sénat relatif à la croissance et la transformation des entreprises*. Available at: <http://www.assemblee-nationale.fr/15/projets/pl1673.asp> [Last accessed: 21 February 2019].

<sup>135</sup> Idem.

<sup>136</sup> Autorité de Contrôle Prudentiel et de Résolution (2014) *Position de l'ACPR relative aux opérations sur Bitcoins en France*. Available at: [https://acpr.banque-france.fr/sites/default/files/20140101\\_acpr\\_position\\_bitcoin.pdf](https://acpr.banque-france.fr/sites/default/files/20140101_acpr_position_bitcoin.pdf) [Last accessed: 28 January 2019].

<sup>137</sup> These criteria are enumerated in article L 315-1 of the French Financial and Monetary Code: (i) monetary value (ii) as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions (iii) and which is accepted by a natural or legal person other than the electronic money issuer.

rights protection and AML requirements. The AMF will review whether the company has given proper information to its investors in its ‘white paper’, examine whether the company has taken necessary measures to establish their subscribers’ identity (KYC) and to place the funds raised into an escrow account. The AMF visa should, however, not be viewed as an assessment of the project’s investment viability.

The aim of this optional regime for ICOs is to reduce the regulatory uncertainty for entrepreneurs and encourage the players that respect sound risk management practices to establish themselves in France.

However, the AMF will not have the ability to supervise ICO projects issuing security tokens, which would instead be regulated under the financial instrument law. According to an estimation by the regulator, 90% of ICO projects will not fall within the scope of this optional authorisation regime.<sup>138</sup>

This new framework has been provided in *PACTE Law*, which is currently under consideration by the French Government (acquired by the Senate and now back to the National Assembly).<sup>139</sup> It also plans to expand this optional regime to certain digital assets activities, such as the offering of exchange and storage services.<sup>140</sup> The actors opting for these regimes will be subject to AML obligations and will be supervised by the AMF. A recent amendment grants the ACPR and the French Central Bank the ability to review the list of actors registered by the AMF.<sup>141</sup>

### **Investment Services and Financial instruments**

Cryptoasset activities may fall under financial instrument laws if:

- A security token provides its holder with governance and/or financial rights in the company launching the ICO;<sup>142</sup>
- A cryptoasset is a derivative of an underlying asset - it will be subject to the relevant rules on derivatives, in particular, the prohibition of electronic advertising;<sup>143</sup>
- A cryptoasset is commercialised as an opportunity for investment profit without being qualified as a financial instrument, such investment offering can only emanate from an intermediary in “atypical investments”.<sup>144</sup>

<sup>138</sup> Interview with AMF representatives on October 10, 2018 in Paris.

<sup>139</sup> National Assembly (2019) *Projet de loi modifié par le Sénat relatif à la croissance et la transformation des entreprises*. Available at: <http://www.assemblee-nationale.fr/15/projets/pl1673.asp> [Last accessed: 21 February 2019].

<sup>140</sup> This category includes custodial wallet providers, entities selling or buying cryptoassets in exchange of fiat money, platforms exchanging cryptoassets for other cryptoassets, platforms of negotiation in digital assets, reception and transmission of orders for digital assets on behalf of clients, digital assets portfolio management, advice in digital assets subscription, placing of digital assets on a firm commitment basis, guaranteed and non-guaranteed placing of digital assets.

<sup>141</sup> National Assembly (2019) *Projet de loi modifié par le Sénat relatif à la croissance et la transformation des entreprises*. Available at: <http://www.assemblee-nationale.fr/15/projets/pl1673.asp> [Last accessed: 21 February 2019].

<sup>142</sup> In this respect it should be noted that since Decree 2017-1674 of 8 December 2017 on the use of a shared electronic registration device to represent and transmit financial the use of distributed ledger is allowed for representation, transmission and pledge of unlisted securities; and a decision of the issuer is required to register securities on a distributed ledger. Therefore, this legislature concerns the tokens having the features of securities (i.e. provide for governance rights and right for dividends with respect to the moral person initiating the ICO).

<sup>143</sup> AMF (2018) *Analysis of the legal qualification of cryptocurrency derivatives*. Available at: [https://www.amf-france.org/en\\_US/Reglementation/Dossiers-thematiques/Marches/Produits-derives/Analyse-sur-la-qualification-juridique-des-produits-d-riv-s-sur-crypto-monnaies?langSwitch=true](https://www.amf-france.org/en_US/Reglementation/Dossiers-thematiques/Marches/Produits-derives/Analyse-sur-la-qualification-juridique-des-produits-d-riv-s-sur-crypto-monnaies?langSwitch=true) [Accessed: 07 January 2019].

The AMF has also published a list of unauthorised websites offering to invest in derivatives on cryptoassets.

In this respect also see ESMA Decision (EU) 2018/796 of 22 May 2018 to temporarily restrict contracts for differences in the Union in accordance with Article 40 of Regulation (EU) No 600/2014 of the European Parliament and of the Council.

<sup>144</sup> The investment proposals highlighting the possibility of a financial returns or a similar economic effect involve intermediation in miscellaneous assets and are subject to ex ante control by the AMF. Consequently, no offer can be directly marketed in France on without prior allocation by the AMF of a registration number (The Law “Sapin II” as of December 9, 2016).

The AMF is publishing a list on its website of unauthorised companies proposing atypical investments without being authorised to do so available at: [https://www.amf-france.org/en\\_US/Actualites/Communiqués-de-presse/AMF/annee-2018?docId=workspace://SpacesStore/3f85fe88-fc1f-45b8-a55e-0bc5aeb298ce](https://www.amf-france.org/en_US/Actualites/Communiqués-de-presse/AMF/annee-2018?docId=workspace://SpacesStore/3f85fe88-fc1f-45b8-a55e-0bc5aeb298ce)

## Future Outlook

The French Government has expressed its determination to provide crypto businesses with a supportive regulatory framework. The optional visa for ICO projects and other intermediated activities is the first step towards the development of a bespoke regulatory regime. It is expected that the optional authorisation regime will improve cryptoasset firms' access to traditional financial services, while bringing greater competitiveness and higher-quality projects in the market. The cryptoasset industry - generally through trade associations - has begun to develop its own self-regulatory framework to protect consumers, as well as engage with regulatory authorities.<sup>145</sup>

France's *PACTE Law* was adopted at first reading by the National Assembly in October 2018. The Senate approved a revised version and the text has been sent back to the National Assembly on February 21, 2019.<sup>146</sup>

France is also required to implement the EU's 5AMLD by January 10, 2020, which will bring cryptoasset exchanges and custodial wallet providers under its AML obligations requiring a license.<sup>147</sup>

---

<sup>145</sup> ChainTech and France Digitale (2018) *Toward a Regulatory Framework for Crypto-asset*. Available at: <http://www.francedigitale.org/actu-europe/europe-est-le-nouveau-icontinent-et-paris-est-place/> [Last accessed: 07 January 2019].

<sup>146</sup> National Assembly (2019) *Projet de loi modifié par le Sénat relatif à la croissance et la transformation des entreprises*. Available at: <http://www.assemblee-nationale.fr/15/projets/pl1673.asp> [Last accessed: 21 February 2019].

<sup>147</sup> See the *European Union* section. European Parliament and European Council (2018) *Directive (EU) 2018/843*. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L0843&from=EN> [Last accessed: 21 December 2018].

## Gibraltar

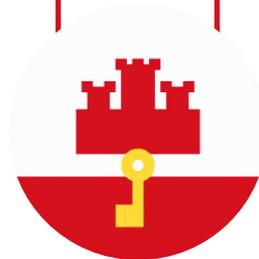


### RESPONSIBLE REGULATORY AUTHORITIES

Gibraltar Financial Services Commission (GFSC)

### RELEVANT REGULATIONS

Financial Services (Distributed Ledger Technology Providers) Regulations  
Token Regulations (*Pending*)



**Date of enforcement of bespoke regulation [Distributed Ledger Technology Framework, 2018]:**  
January 1, 2018

### Cryptoasset Definition and Terminology

The current *DLT Framework* solely defines *DLT* as a:

*database system in which: (a) information is recorded and consensually shared and synchronised across a network of multiple nodes; and (b) all copies of the database are regarded as equally authentic; and “value” includes assets, holdings and other forms of ownership, rights, or interests with or without related information such as agreements or transaction for the transfer of value or its payment, clearing or settlement.*<sup>148</sup>

Further definitions of tokens are expected to be put forth in the proposed regulation for cryptotokens.<sup>149</sup>

### Relevant Regulations

#### *DLT Providers Regulations*

The *DLT Providers Regulations*, encompassed in the *DLT Framework*, provide that any firm using *DLT* for storing or transmitting value belonging to others in or from Gibraltar, is required to obtain authorisation from the GFSC as a “*DLT Provider*”. There is no specific reference to miners and no distinction between custodial and non-custodial service providers. *DLT Providers* will be required to demonstrate compliance with the Principles, including:

- Conduct its business with honesty and integrity;
- Rules including fairness for customers, governance and cybersecurity;
- Maintaining adequate financial and non-financial resources;<sup>150</sup> and
- Having systems in place to prevent, detect and disclose financial crime risks such as money laundering and terrorist financing.

Firms who are currently licensed under existing financial services legislation and use *DLT* will not need to obtain a separate license under the *DLT framework*, unless the activities are not currently caught within

<sup>148</sup> Gibraltar Financial Services Commission (2017) *Financial Services (Distributed Ledger Technology Providers) Regulation 2017*. Available at: [http://www.gfsc.gi/uploads/DLT%20regulations%20121017%20\(2\).pdf](http://www.gfsc.gi/uploads/DLT%20regulations%20121017%20(2).pdf) [Last accessed: 07 January 2019].

<sup>149</sup> No specific date has been mentioned for the proposed regulations to be passed. Preparations for the regulations are in the final stages, according to a governmental source.

<sup>150</sup> Gibraltar Financial Services Commission (2018) *DLT Providers Guidance Notes - Financial and Non-Financial Resources*. Available at: <http://www.gfsc.gi/uploads/Guidance%20Note%203%20-%20Resources%20GFSC.pdf> [Last accessed: 13 January 2019].

the scope of the license they hold. However, if a licensed bank intends to provide virtual currency wallets and/or services, a licence under the DLT regime will be required.

### **Investment Fund Regulations**

The GFSC has no objection to Experienced Investor Funds (EIFs) investing in digital assets. However, the unique characteristics and inherent risks associated with investing in digital assets must be considered by a fund's directors. In particular, the GFSC expects the following matters to be considered: sufficient knowledge and expertise, risk factors, disclosures, security and custody arrangements, cyber-security arrangements, valuation policy, subscription in digital assets, and procedures and controls for AML/KYC purposes.<sup>151</sup>

### **AML/CFT Regulations**

*The Proceeds of Crime Act 2015* was amended to extend AML/CFT requirements to “undertakings that receive, whether on their own account or on behalf of another person proceeds in any form from the sale of tokenised digital assets”.

Until such time that the proposed Token Regulations are brought into effect, issuers of coins or tokens (ICOs) are required to comply with AML/CFT regulation. KYC requirements kick in at pre-public offering stage and AML/CFT obligations, other than record-keeping obligations, end upon the distribution of the tokens. It is generally accepted by the GFSC that, unless tokens can be withheld, due diligence is required to be collected on potential contributors before a public token sale takes place, this is also known as a “whitelisting” process.

### **Future Outlook**

At the time of writing, the Government of Gibraltar and the GFSC were in the process of drafting a legislative framework for tokenised digital assets based on distributed ledger technology, referred to as the proposed *Token Regulations*. Preparation of the *Token Regulations* is currently in the final stages.

Rather than seeking to regulate the underlying technology *per se*, the proposed Token Regulations deal with three complementary facets, being:

- The promotion, sale and distribution of tokens;
- Secondary market activities relating to tokens, (i.e. cryptoassets exchanges);
- The provision of investment advice and other services in relation to tokens.

The proposed Token Regulations will deal with “virtual currencies” and “hybrid tokens”, the latter being those tokens that are neither security tokens nor mere gifts/donations. Such Token Regulations contemplate the concept of “Authorised Sponsors”, who will act as gatekeepers for token issuers, and who will be responsible for ensuring regulatory compliance, including adherence with competency and operational requirements. In addition, insofar as cryptoasset exchanges and investment or professional services in relation to tokens and virtual currencies are concerned, the proposed Token Regulations will adopt the requirements set out under MiFID II.

Until the proposed Token Regulations are formally drafted and enacted, the general position is that ICOs or token sales will not be caught under the DLT framework. However, there may be instances where, depending on usage and structure, a token may fall within existing financial services legislation (for example, it could be deemed as a Collective Investment Scheme, Alternative Investment Fund, etc.).

On October 17, 2018, the GFSC noted that it is considering specific regulation for EIFs seeking to invest in digital assets such as cryptocurrencies and similar DLT-based tokens.

---

<sup>151</sup> Gibraltar Financial Services Commission (2018) *DLT Provider Guidance Notes - Resilience*. Available at: <http://www.gfsc.gi/uploads/Guidance%20Note%209%20-%20Resilience%20GFSC.pdf> [Last accessed: 07 January 2019].

## Israel



Date of enforcement of bespoke regulatory regime [Control of Financial Services (Regulated Financial Services) Law, 5776 – 2016]: June 1, 2018

### Cryptoasset Definition and Terminology

In 2016, the *Financial Services Law* was passed and included *virtual currencies* into its definition of *financial asset*, but does not provide further definition of the term.<sup>152</sup> Additionally in January 2017, the Israel Tax Authority has defined *virtual currencies*, for tax purposes, as a “means of virtual payment” and financial assets used for the purpose of bartering.<sup>153</sup>

### Relevant Regulations

The *Financial Services Law* requires entities providing financial asset services to obtain a license from the Supervisor of Financial Services Providers, as part of the Ministry of Finance.<sup>154</sup> Entities engaging in activities involving virtual currencies will have to be granted either a Basic License for the Provision of Financial Asset Services or an Expanded License for the Provision of Financial Asset Services (applicable if the business turnover attributable to financial asset services exceeds NIS 30 million). Criteria for obtaining a basic license differ between individual and corporate license applicants, i.e. an expanded license will be issued solely to corporate entities located in Israel.<sup>155</sup>

Entities that are supervised by other financial laws (*Banking Law*, *Securities Law* and the *Control over Financial Services (Insurance) Law*) and private individuals who are providing credit through internet platforms serving solely as brokers (P2P platforms) are exempted from the license obligation.

In March 2018, ISA announced it would ban cryptoasset companies from indices on the Tel Aviv Stock Exchange (TASE) to protect passive investors, although not from TASE itself.<sup>156</sup>

<sup>152</sup> Supervision on Financial Service (2016) *Financial Services Law 5766-2016*. Available at: [https://www.nevo.co.il/law\\_html/Law01/501\\_439.htm#Seif12](https://www.nevo.co.il/law_html/Law01/501_439.htm#Seif12) [Last accessed: 20 December 2018].

<sup>153</sup> Tax Authority (2018) *Taxation of activities in a distributed payment system (known as “virtual currencies”)*. Available at: [https://taxes.gov.il/incometax/documents/hozrim/hor\\_acc%2015.2.18.pdf](https://taxes.gov.il/incometax/documents/hozrim/hor_acc%2015.2.18.pdf) [Last accessed: 20 December 2018].

<sup>154</sup> Even-Chen, A. (2016) *New Financial Services Law Establishes Mandatory Licensing Requirement for Financial Service-Providers*. Available at: <https://www.barlaw.co.il/client-updates/new-financial-services-law-establishes-mandatory-licensing-requirement-for-financial-service-providers/> [Last accessed: 20 December 2018].

<sup>155</sup> Idem.

<sup>156</sup> Israel Security Authority (2018) *Israel Securities Authority Determines: Cryptocurrency Companies Not to Be Included in TASE Indices*. Available at: <http://www.isa.gov.il/%D7%94%D7%95%D7%93%D7%A2%D7%95%D7%AA%20%D7%95%D7%A4%D7%A8%D7%A1%D7%95%D7%9E%D7%99%D7%9D/175/2018/Pages/eitonot14318.aspx> [Last accessed: 26 February 2019].

### Applicability of financial instrument regulations

The ISA has not yet adopted binding regulation on cryptoassets but published an interim report in March 2018 dealing with ICOs as securities, with a number of recommendations for future policy-making, inviting comments from the public.<sup>157</sup> A classification was developed to determine the applicability of securities law as follows:

- **Currency tokens:** tokens intended to be used exclusively as a means of payment, exchange or clearing that are not limited to a specific venture;
- **Security or investment tokens:** tokens conferring ownership rights, membership or participation in a specific venture, or rights to future cash flows from said venture. This type of token will be deemed a security;
- **Utility tokens:** tokens conferring access or use rights in a service or product offered by a certain venture. Such tokens, acquired solely for the purpose of consumption and use, will not be deemed securities. A test will verify the impossibility to use tokens when issued or the possibility to trade them on a secondary market.

An Interdepartmental Committee within the ISA emphasised that applying securities law to cryptoasset activities needs to be tailored. It warned that imposing a general obligation to publish a prospectus and cumbersome securities regulation on cryptoasset activities could prevent entrepreneurs from launching their ICO in Israel, leading to business relocation and fewer investments. Therefore, the Interdepartmental Committee recommended to adjust disclosure requirements defined in the Securities Law to the unique features of ICO projects, much like disclosure obligations were adjusted for other sectors (e.g. real estate).<sup>158</sup>

### Other applicable regulations and court decision

Directives issued by the Banking Supervision Department of the Central Bank would require *cryptoasset businesses*, much like banks, to use cautionary measures and to meet the rules of the Financial Action Task Force (FATF).<sup>159</sup>

### Future Outlook

On May 23, 2018, the Ministry of Finance published a draft amending the “prohibition of money-laundering” order to accompany a revised *Financial Services Law*.<sup>160</sup> The draft version imposes a requirement on cryptoasset service providers to include the IP addresses of all clients and any public addresses of cryptoasset wallets used to transfer tokens, along with their own personal data. All service providers will also be required to maintain full documentation of cryptoasset activity for the next five years.<sup>161</sup>

In its recommendations for future policy-making on cryptoassets, the Interdepartmental Committee emphasised the need for a regulatory sandbox for small scale ICOs. Although there is no obligation to follow the Committee’s recommendations, its findings are likely to form the basis for future regulatory or legislative discussions.

<sup>157</sup> Israel Security Authority (2018) *The Committee to Examine the Regulation of Decentralized Cryptographic Currency Issuance to the Public Interim Report*. Available at: <http://www.isa.gov.il/sites/ISAEng/1489/1513/Documents/DOH17718.pdf> [Last accessed: 20 December 2018].

<sup>158</sup> Israel Security Authority (2018) *The Committee to Examine the Regulation of Decentralized Cryptographic Currency Issuance to the Public Interim Report*. Available at: <http://www.isa.gov.il/sites/ISAEng/1489/1513/Documents/DOH17718.pdf> [Last accessed: 20 December 2018].

<sup>159</sup> Deputy Governor of the Bank of Israel (2018) *Remarks at the Knesset Finance Committee meeting on the activity and use of virtual currencies*. Available at: <https://www.boi.org.il/he/NewsAndPublications/LecturesSpeechesAndPresentations/Pages/8-1-2018.aspx> [Last accessed: 20 December 2018]; Bank of Israel (2014) *Notice to the public regarding possible risks in decentralized virtual currencies (such as Bitcoin)*. Available here: <http://www.boi.org.il/en/NewsAndPublications/PressReleases/Pages/19-02-2014-BitCoin.aspx> [Last accessed: 26 February 2019].

<sup>160</sup> Kalman, M. (2018) “Israel seeks “Uniform” law to fight money laundering, tax evasion” *Bloomberg*. Available at: <https://www.bna.com/israel-seeks-uniform-n73014476524/> [Last accessed: 20 December 2018].

<sup>161</sup> Ministry of Justice (2018) *The Ministry of Finance published a draft Amendment to the Prohibition on Money Laundering Order for financial assets service providers*. Available at: <http://www.justice.gov.il/Units/HalbantHon/News/Pages/DraftOrderFinancialProduct.aspx> [Last accessed: 20 December 2018].

## Malta



### RESPONSIBLE REGULATORY AUTHORITIES

Maltese Financial Services Authority (MFSA)  
Maltese Digital Innovation Authority (MDIA)



### RELEVANT REGULATIONS

Malta Digital Innovation Authority Act  
Innovative Technology Arrangements and Services Act  
Virtual Financial Assets Act  
Financial Institutions Act  
Investment Services Act

Date of enforcement of bespoke regulation [Virtual Financial Assets Act, 2018]: November 1, 2018<sup>162</sup>

### Cryptoasset Definition and Terminology

The *Virtual Financial Assets Act* (VFAA) sets out a series of definitions for *DLT assets*, as follows:<sup>163</sup>

*DLT assets are: (i) virtual tokens; (ii) virtual financial assets; (iii) electronic money; or (iv) financial instruments, that are intrinsically dependent on or utilises, Distributed Ledger Technology.*

Accordingly, references must be made to the definitions of the four classes of *DLT assets* referred to above:

- Electronic money;
- Financial instruments;
- Virtual tokens: a form of digital medium recordation whose utility, value or application is restricted solely to the acquisition of goods or services, either solely within the DLT platform on or in relation to which it was issued or within a limited network of DLT platforms;
- Virtual financial assets: any form of digital medium recordation that is used as a digital medium of exchange, unit of account, or store of value and that is not: (a) electronic money; (b) a financial instrument; or (c) a virtual token.

The latter category constitutes a whole new asset class catering to the peculiarities of crypto assets and forms the crux of the framework developed under the VFAA.

The MFSA has introduced the “Financial Instrument Test”, favouring substance over form, formulated in an easy-to-follow question and answer excel format, to classify *DLT Assets*.

Where the cryptoasset in question is classified under the Financial Instrument Test as a Financial Instrument or Electronic Money, then EU legislation, namely the Prospectus Directive, MiFID II, and the E-Money Directive (in each case, as transposed into domestic Maltese law) shall apply.

<sup>162</sup> Please note November 1, 2018 is the date the VFAA entered into force, however some requirements are subject to transitory provisions ranging from 1 to 12 months.

<sup>163</sup> Government of Malta (2018) *Virtual Financial Assets Act* (VFAA). Available at: <http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lp&itemid=29079&l=1> [Last accessed: 14 February 2018].

## Relevant Regulations

### **Applicability of Virtual Financial Asset Act**

The VFAA regulates: (i) ICOs and secondary trading of virtual financial assets (“IVFAOs”); (ii) the provision of professional and investment services when rendered in relation to virtual financial assets (i.e. ‘VFA Service Providers’ via which transactions involving crypto assets may be carried out); and (iii) Virtual Financial Asset Agents (VFA Agents).

IVFAO or ICO issuers are required to establish a legal entity in Malta, properly register a whitepaper, carry out the financial instrument test, appoint mandatory functionaries and comply with governance, I.T. (including cybersecurity), and ongoing disclosure requirements.

VFA Service Providers (which includes VFA Exchanges) require a license from the MFSA. Initial and ongoing licencing requirements include the procedural, competency, capital, prudential, governance, risk management, regulatory compliance conduct of business, and reporting requirements applicable thereto. A market abuse regime in the VFAA treats dealing in crypto assets as identically as possible to traditional assets.

The MFSA will accept registration and/or licensing applications where a VFA Agent has not been appointed. A VFA Agent, as a registered and regulated intermediary, is responsible for assessing the fitness and properness of prospective applicants and guiding applicants throughout the process. A System Auditor registered with the MDIA vets the technological arrangements and reports to MFSA any act resulting in breach of applicable requirements for license holders.

### **Other existing regulations**

Additionally, the Malta Gaming Authority (MGA) will be opening a regulatory sandbox that focuses on virtual financial assets and virtual tokens. The will test in the sandbox for 10 months. Application for the sandbox opened on January 1, 2019.<sup>164</sup>

### **AML/CFT regulations**

The VFAA provides that Issuers of VFAs, licensed VFA Service Providers, and VFA Agents are deemed to be “*subject persons*”, and thus subject to AML and KYC obligations. Malta’s AML requirements gold-plate the requirements of the impending 5AMLD, which includes specific requirements for cryptoasset wallets and cryptoasset exchanges.

Moreover, on October 30, 2018, the Financial Intelligence Analysis Unit published an industry consultation on the revised draft implementing procedures and sector-specific guidelines, which now include specific guidelines relating to the risks associated with virtual currencies.<sup>165</sup>

## Future Outlook

The Innovative Technology Arrangements and Services Act is expected to enter into force early in 2019.

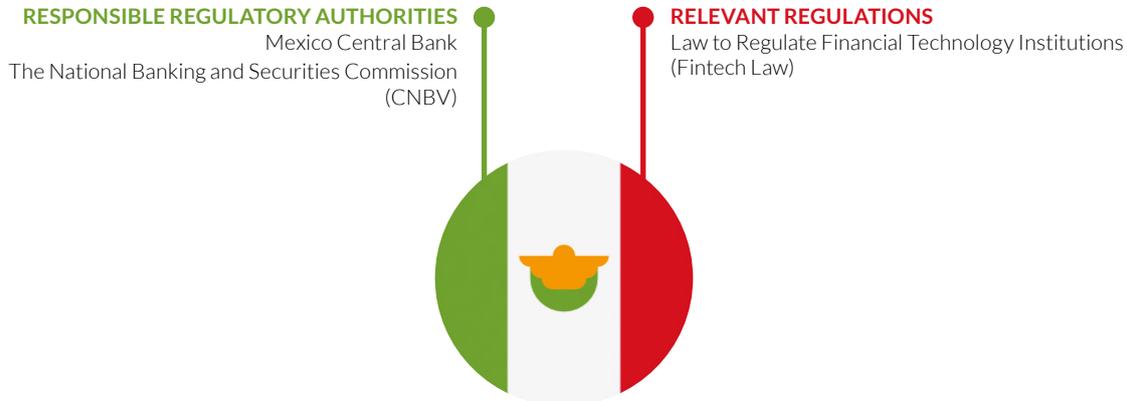
The MFSA has expressed its intention to revise the regulatory framework for virtual financial assets on an ongoing basis to reflect the peculiarities and risks associated with the latest developments. In this regard, the MFSA has already issued an ‘*Industry FAQs*’ relating to virtual financial assets, together with a number of explanatory circulars, to aid in the interpretation and application of the law to particular scenarios and business models. As of March 2019, 28 entities have applied for a license and await MFSA decision.<sup>166</sup>

<sup>164</sup> Malta Gaming Authority (2018) *Guidance on the use of Innovative Technology Arrangements and the acceptance of Virtual Financial Assets and Virtual Tokens through the implementation of a Sandbox Environment*. Available at: <https://www.mga.org.mt/wp-content/uploads/MGA-VFA-and-ITA-Sandbox.pdf> [Last accessed: 02 January 2019].

<sup>165</sup> Financial Intelligence Analysis Unit Malta (2018) *Consultation Document. Amendment to the Implementing Procedure Part 1*. Available at: <http://www.fiumalta.org/library/PDF/misc/2018.10.30%20-%20Consultation%20Document%20-%20Revised%20Version%20of%20the%20FIAU%20Implementing%20Procedures%20Part%20I.pdf> [Last accessed: 12 February 2019].

<sup>166</sup> The Block (2019) *Blockchain and cryptocurrency firms trying to open bank accounts face troubles in Malta*. Available at: <https://www.theblockcrypto.com/tiny/blockchain-and-cryptocurrency-firms-trying-to-open-bank-accounts-face-troubles-in-malta/> [Last accessed: 05 March 2019].

## Mexico



**Date of enforcement of bespoke regime [Law to Regulate Financial Technology Institutions, 2018]:**  
March 10, 2018

### Cryptoasset Definition and Terminology

The Fintech Law defines *virtual assets* 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.*<sup>167</sup>

### Relevant Regulations

The Fintech Law sets the regulatory framework for Electronic Payment Funds Institutions (including Virtual Assets payments)<sup>168</sup> and Virtual Asset activities.<sup>169</sup>

Collective Financing Institutions (crowdfunders) and Electronic Payment Funds Institutions are collectively called Fintech Institutions (FTIs). Only FTIs authorised by a special committee of the CNBV<sup>170</sup> and the Mexican Central Bank can deal and trade Virtual Assets. The *General rules applicable to FTIs* issued by the CNBV set forth what conditions need to be complied with to obtain such authorisation, including provisions on documentation and minimum capital as well as accounting and valuation rules.<sup>171</sup> The other implementing measures of the Fintech Law are:

- *General rules pursuant to article 58 of the Law to regulate Financial Technology Institutions* issued by the Secretariat of Finance and Public Credit (SHCP) (AML Provisions);<sup>172</sup>

<sup>167</sup> Art. 30 of Fintech Law. Mexico's House of Representatives (2018) *Law to Regulate Financial Technology Companies*. Available at: [http://www.diputados.gob.mx/LeyesBiblio/pdf/LRITF\\_090318.pdf](http://www.diputados.gob.mx/LeyesBiblio/pdf/LRITF_090318.pdf) [Last accessed: 11 December 2018].

<sup>168</sup> Electronic Payment Funds Institutions mean firms that provide services of emission, administration, redemption or transmission of electronic payment of funds including fiat currency or virtual assets (commonly identified as e-money or online payment companies).

<sup>169</sup> President of the Republic (2018) *Law to Regulate Financial Technology Institutions*, *Diario Oficial de la Federación*. Available at: [http://www.dof.gob.mx/nota\\_detalle.php?codigo=5515623&fecha=09/03/2018](http://www.dof.gob.mx/nota_detalle.php?codigo=5515623&fecha=09/03/2018) [Last accessed: 11 December 2018].

<sup>170</sup> According to the *Fintech Law*, a prior consent of the Inter-institutional Committee comprising of six members and their alternates, appointed jointly by the SHCP, CNBV and Mexican Central Bank is required by FTIs to operate.

<sup>171</sup> National Banking and Securities Commission (2018) *Disposiciones de carácter general aplicables a las Instituciones de Tecnología Financiera*. Available at: [http://www.dof.gob.mx/nota\\_detalle.php?codigo=5537450&fecha=10/09/2018](http://www.dof.gob.mx/nota_detalle.php?codigo=5537450&fecha=10/09/2018) [Last accessed: 14 January 2019].

<sup>172</sup> Idem.

- *General rules applicable to the operations of electronic payment funds institutions* issued by the Mexican Central Bank (Central Bank Provisions).<sup>173</sup>

The Fintech Law also sets forth minimum obligations for virtual asset service providers, including disclosure to clients of volatility, fraud and cybersecurity risks, as well as the potential irreversibility of Virtual Asset transactions.

The Fintech Law grants the Mexican Central Bank the power to determine and authorise the specific type of Virtual Assets that FTIs can deal with. In doing so, the Central Bank has to take into account a number of general criteria set forth by the Law, including the use to the general public and the regulatory approach in other jurisdictions. The Central Bank Provisions however do not provide a list of authorised Virtual Assets, but lay down additional requirements on the operations of crypto-exchanges and other companies dealing with cryptoasset-based electronic payments (e.g. rules on the opening of accounts or redemption of funds). The CNBV, SHCP and Mexican Central Bank are also required to issue corresponding enabling regulations for effective enforcement of the Fintech Law, which, as published in the official gazette on September 10, 2018, provide for certain additional requirements to operate as an FTI<sup>174</sup>, including minimum compliance requirements under the AML provisions<sup>175</sup> and operative rules applicable to e-money institutions.<sup>176</sup>

Furthermore, the Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF) has statutory powers to issue additional regulations to monitor such entities and ensure equal and fair relationships with their users.

The Fintech Law imposed AML/CFT reporting and KYC obligations on FTIs and mandated the SHCP to publish implementing measures.<sup>177</sup> FTIs, including individuals, are bound by the *Federal Law to Identify, Prevent and Eliminate Money Laundering* (AML Law) to provide the means to store, protect or transfer virtual assets.

### Future Outlook

The Fintech Law is relatively recent, and its implementing measures are only a few months old. It is not yet clear which cryptoassets the Mexican Central Bank will be willing to authorise under the Fintech Law. The interplay between securities laws and the new Fintech Law, particularly regarding token offerings, is also yet to be developed.<sup>178</sup>

<sup>173</sup> Idem.

<sup>174</sup> General Provisions applicable to Financial Technology Institutions. Idem

<sup>175</sup> General Provisions pursuant to Article 58 of the Fintech Law. Idem

<sup>176</sup> Mexican Central Bank (2018) *Circular 12/2018 containing operative Rules applicable to E-money Institutions*. Available at: <http://www.banxico.org.mx/marco-normativo/normativa-emitida-por-el-banco-de-mexico/circular-12-2018/%7BA6023AE0-8135-44ED-04DA-2068117ED5FD%7D.pdf> [Last accessed: 24 February 2019].

<sup>177</sup> Art. 58 of Fintech Law. Mexico's House of Representatives (2018) *Law to Regulate Financial Technology Companies*. Available at: [http://www.diputados.gob.mx/LeyesBiblio/pdf/LRITF\\_090318.pdf](http://www.diputados.gob.mx/LeyesBiblio/pdf/LRITF_090318.pdf) [Last accessed: 11 December 2018].

<sup>178</sup> Mexican Central Bank (2017) *Las autoridades financieras advierten de los riesgos asociados al uso de activos virtuales y a la participación en los esquemas de inversión conocidos como Oferta Inicial de Monedas o "Initial Coin Offerings"*. Available at: <http://www.banxico.org.mx/publicaciones-y-prensa/miscelaneos/%7B6D5AAB8C-3BFA-0A8B-5EDD-7EDC04E1931C%7D.pdf> [Last accessed: 07 January 2019].

## Russia



### RESPONSIBLE REGULATORY AUTHORITIES

Central Bank of Russia (CBR)  
Ministry of Finance

### RELEVANT REGULATIONS

Federal Law on Digital Financial Assets (*Pending*)



Expected date of enforcement of bespoke regulation [Federal Law on Digital Financial Assets, 2018]: mid-2019

### Cryptoasset Definition and Terminology

The draft law on *Digital Financial Assets* defines *cryptocurrency* as:

*a type of digital financial asset created and accounted for in the distributed registry of digital transactions by participants in this registry in accordance with the rules of maintaining the registry of digital transactions.*<sup>179</sup>

Further, the draft law defines a *Token* as

*a type of a digital financial asset that is issued by a legal entity or an individual entrepreneur in order to attract financing and is recorded in the registry of digital records.*

### Relevant Regulations

The *Digital Financial Assets Bill* includes restrictions on the use of cryptoassets and requires CBR and the Government to determine ways in which cryptoassets can be used. Additionally, the *Digital Economy* programme also provides for certain amendments to the Russian Civil Code (aimed at incorporating new objects such as digital rights and digital money) and a draft law on investment platforms for governance of crowdfunding and related investment activities. These two bills are expected to improve the conditions of doing business through the use of information technologies in Russia.<sup>180</sup>

The draft law provides for conditions relating to token offering and issuance, while intending to keep ICOs outside the scope of securities law. It allows any legal person to launch an ICO on completion of specific obligations, including the release of two documents: an investment memorandum and a public offer (equivalent to a prospectus, with lower level of details). The investment memorandum must be placed with a depository. Additional restrictions include a cap on the amount a single investor can acquire, a prohibition on cryptoasset-to-cryptoasset exchanges, and a requirement that ICOs be distributed on a cryptoasset exchange.<sup>181</sup>

<sup>179</sup> Ministry of Finance (2018) *Draft Federal Law on Digital Financial Assets*. Available at: [https://www.minfin.ru/ru/document/?id\\_4=121810&order\\_4=P\\_DATE&dir\\_4=DESC&is\\_new\\_4=1&page\\_4=1&area\\_id=4&page\\_id=2104&popup=Y#](https://www.minfin.ru/ru/document/?id_4=121810&order_4=P_DATE&dir_4=DESC&is_new_4=1&page_4=1&area_id=4&page_id=2104&popup=Y#) [Last accessed: 07 January 2019].

<sup>180</sup> Duma (2018) *A project law on digital financial assets has passed the first reading*. Available at: <http://duma.gov.ru/news/27027/> [Last accessed: 07 January 2019].

<sup>181</sup> Idem.

The draft law also provides for a governance framework for ‘operators of digital financial assets trade’, which must be a legal entity holding a financial license from the CBR.

Under the law, miners may be required to hold a license depending on their “level of activity”, based on the amount of energy consumed.<sup>182</sup>

### Future Outlook

Russia’s *Digital Financial Assets Bill* was expected to be enacted by mid-2018. The Bill passed the first reading, but so far no second reading has been scheduled yet. Amendments to the Civil Code are also under review to ensure “digital financial assets” can be dealt with in bankruptcy or inheritance proceedings.

Furthermore, the regulatory policy action plan within the Digital Economy program provides opportunities for the creation of regulatory sandboxes.<sup>183</sup> The Russian Government and the Bank of Russia are currently working on the regulatory framework for a regulatory sandbox for FinTech projects which is likely to include cryptoasset projects. The regulatory sandbox is expected to become available by the end of 2018.<sup>184</sup>

As a member state of the Eurasian Economic Commission (EEC), Russia has participated in the development of a cryptoeconomy glossary.<sup>185</sup> In January 2019, the EEC issued a report on cryptoassets to promote regulation, with the Ministry of Finance considering plans to launch a digital currency backed by countries in the Eurasian Economic Union (EAEU).

---

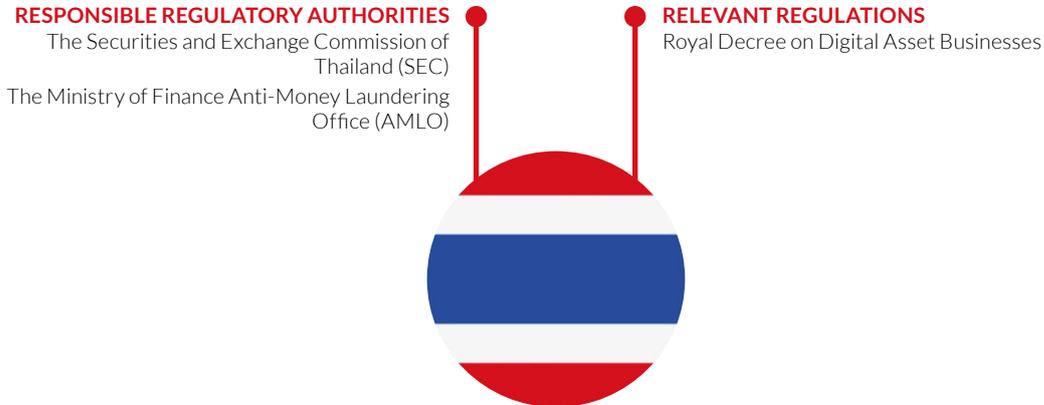
<sup>182</sup> Ministry of Finance (2018) *Draft Federal Law on Digital Financial Assets*. Available at: [https://www.minfin.ru/ru/document/?id\\_4=121810&order\\_4=P\\_DATE&dir\\_4=DESC&is\\_new\\_4=1&page\\_4=1&area\\_id=4&page\\_id=2104&popup=Y#](https://www.minfin.ru/ru/document/?id_4=121810&order_4=P_DATE&dir_4=DESC&is_new_4=1&page_4=1&area_id=4&page_id=2104&popup=Y#) [Last accessed: 07 January 2019].

<sup>183</sup> Kremlin (2017) *List of instructions following the meeting on the use of digital technologies in the financial sector*. Available at: <http://kremlin.ru/acts/assignments/orders/55899> [Last accessed: 07 January 2019].

<sup>184</sup> Currently, the Bank of Russia’s website invites companies and interested parties to send proposals of the projects for a regulatory sandbox.

<sup>185</sup> Eurasian Economic Commission (2018) *The ECE and the OECD have common areas for cooperation in the field of cryptocurrency and blockchain technology*. Available at: <http://www.eurasiancommission.org/ru/nae/news/Pages/31-07-2018-3.aspx> [Last accessed: 07 January 2019].

## Thailand



**Date of enforcement of bespoke regulation [Royal Decree on the Digital Asset Businesses, 2018]:**  
May 13, 2018

### Cryptoasset Definition and Terminology

The *Royal Decree* provides the following definitions:

- A cryptocurrency means 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.;
- A digital token means 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.;
- Cryptocurrency and Digital Tokens are both *digital assets*.<sup>186</sup>

### Relevant Regulations

Entities participating in digital tokens issuance (“Issuer” and “ICO portals” of non utility tokens) must seek approval from the SEC, unless they are projects issuing cryptocurrencies and utility tokens that do not bear the characteristics of fundraising and provide investors with the immediate ability to use the offered product or services.

Such an approval requires: (i) pre-file a registration statement and prospectus before launching their offering, (ii) being an established Thai company with registered capital of THB 5 million,<sup>187</sup> (iii) having a proper functioning system and staff team, (iv) audited financial statements aligned with Thai Financial Reporting standards, (v) disclosure requirements, (vi) the appointment of a director or other executive to represent the company, and (vii) the payment of application fees.

<sup>186</sup> Securities and Exchange Commission (2018) *Royal Decree on Digital Asset Business B.E.2561*. Available at: [https://www.sec.or.th/EN/SECInfo/LawsRegulation/Documents/actandroyal/digitalasset\\_decree\\_2561\\_EN.pdf](https://www.sec.or.th/EN/SECInfo/LawsRegulation/Documents/actandroyal/digitalasset_decree_2561_EN.pdf) [Last accessed: 07 December 2018].

<sup>187</sup> Around US \$150,000.

The offering must be conducted via an SEC-authorized ICO portal, meeting specific requirements that include: (i) registered capital of THB 5 million, (ii) compliance with AML/CFT laws, and (iii) proper working IT system. Venture capital and private equity funds, as well as other institutional investors can invest without limit, whereas retail investors may invest up to a limit of THB 300,000 per ICO.

All digital asset businesses are considered financial institutions, and must obtain a license from the Ministry of Finance and comply with the SEC regulations.<sup>188</sup> The rules prescribe that the applicant must be a company established in Thailand, meet paid-up capital requirements, pay application fees, have a proper system to secure funds and assets of its customers, and have an appropriate operating IT system. They must also abide by AML/CFT laws. Once registered with the SEC, the Ministry of Finance will deliver a license to digital asset businesses.

### Future Outlook

The level of cryptoasset activity in the country was expected to increase significantly after the implementation of the *Royal Decree*.<sup>189</sup> However at the time of writing, no ICO portal has been approved by the SEC. Since the issuance of the decree, four entities have been granted a digital business license by the Ministry of Finance. The Thai Stock Exchange has recently announced its intention to apply for a digital asset exchange license.<sup>190</sup>

---

<sup>188</sup> *Digital Asset Business* refers to digital asset exchange, broker, dealer, and other types of businesses as identified by the Ministry of Finance and the P.2 in Securities and Exchange Commission (2018) *Royal Decree on Digital Asset Business B.E.2561*. Available at: [https://www.sec.or.th/EN/SECInfo/LawsRegulation/Documents/actandroyal/digitalasset\\_decree\\_2561\\_EN.pdf](https://www.sec.or.th/EN/SECInfo/LawsRegulation/Documents/actandroyal/digitalasset_decree_2561_EN.pdf) [Last accessed: 07 December 2018].

<sup>189</sup> Interview conducted with Butree Vangsirungruang from the Securities and Exchange Commission on August 28, 2018.

<sup>190</sup> Athawasya, A. (2019) *Thailand's National Stock Exchange venturing into the cryptocurrency space*. Available at: <https://ambcrypto.com/thailands-national-stock-exchange-venturing-into-the-cryptocurrency-space/> [Last accessed: 21 January 2019].

## Retrofitted Regulation

### Australia



Date of enforcement of retrofitted regulation [Anti Money Laundering and Counter Terrorism Financing Act, 2006]: April 3, 2018

#### Cryptoasset Definition and Terminology

The AML/CFT Act and Rules defines *digital currency* as:

- (a) a digital representation of value that:
- (i) functions as a medium of exchange, a store of economic value, or a unit of account; and
  - (ii) is not issued by or under the authority of a government body; and
  - (iii) is interchangeable with money (including through the crediting of an account) and may be used as consideration for the supply of goods or services; and
  - (iv) is generally available to members of the public without any restriction on its use as consideration; or
- (b) a means of exchange or digital process or crediting declared to be digital currency by the AML/CFT Rules.<sup>191</sup>

#### Relevant Regulations

##### Applicability of Securities Laws

In September 2017, ASIC released an information sheet, subsequently updated in May 2018, providing guidance on the regulation of ICOs and cryptoassets.<sup>192</sup> The information sheet clarifies that cryptoassets qualifying as financial products under the *Corporations Act* will attract relevant regulatory obligations. ASIC's primary aim is to ensure that products are not misleading or deceptive.<sup>193</sup> For non-financial cryptoassets, ASIC has powers to prevent misleading or deceptive conduct under the *Australian Consumer Law*. Whereas, for financial cryptoassets, the *Corporations Act* prevents misleading and/or deceptive conduct.

<sup>191</sup> Australian Government (2017) *Anti-Money Laundering and Counter-Terrorism Financing Amendment Act 2017*. Available at: <https://www.legislation.gov.au/Details/C2017A00130> [Accessed: 02 January 2019].

<sup>192</sup> Australian Securities and Investments Commission (2018) *Initial coin offering and crypto-currency*. Available at: <https://asic.gov.au/regulatory-resources/digital-transformation/initial-coin-offerings-and-crypto-currency/> [Last accessed: 02 January 2019].

<sup>193</sup> Australian Securities and Investments Commission (2018) *18-274MR ASIC acts against misleading Initial Coin Offerings and crypto-asset funds targeted at retail investors*. Available at: <https://asic.gov.au/about-asic/news-centre/find-a-media-release/2018-releases/18-274mr-asic-acts-against-misleading-initial-coin-offerings-and-crypto-asset-funds-targeted-at-retail-investors/> [Last accessed: 02 January 2019].

A cryptoasset is considered by ASIC to be a financial product and thus subject to the *Corporations Act 2001*, if it is:

- **A Managed Investment Scheme (MIS):** an MIS is defined under the *Corporation Act* as a scheme where people contribute money or assets to obtain an interest in the scheme and do not have day to day control over its operations, but may have some voting rights as typically outlined in the white paper or offer document;
- **An offer of shares:** if an ICO is created to fund a company, then the rights attached to the ICO may be considered a share, and the issuer will need to prepare a prospectus;
- **An offer of a derivative;**
- **A non-cash payment (NCP) facility:** an arrangement in which a person makes payments other than by physical delivery of currency. An ICO may involve an NCP facility if it includes an arrangement that allows payments to be started in token form and converted to fiat currency to enable completion of the payment. NCP facilities typically will need an Australian Financial Service license.

#### **Applicability of AML regulations**

Amendments to the *AML/CFT Act* and amendments to the *AML/CFT Rules* and updates to the AUSTRAC guidance material were made to bring entities offering exchange services under its scope.<sup>194</sup>

The *AML/CFT Act* and corresponding *Rules* introduced a digital exchange register. Any business engaging in the exchanges of digital currency for a fiat currency or vice versa will have to comply with a number of registration, compliance and record keeping obligations, as well as maintaining an AML/CFT program. AUSTRAC has released guidance material to assist businesses with this process.<sup>195</sup>

#### **Future Outlook**

Since the introduction of the legislation enabling exchanges to register and comply with AML/CFT requirements, there have been a number of local exchanges which have confirmed that they are successfully registered to provide digital currency exchange services. Regulatory certainty in this area is likely to encourage the development of more local currency exchanges.

---

<sup>194</sup> Australian Government (2017) *Anti-Money Laundering and Counter-Terrorism Financing Amendment Act 2017*. Available at: <https://www.legislation.gov.au/Details/C2017A00130> [Last accessed: 02 January 2019].

<sup>195</sup> Australian Transaction Report and Analysis Centre (2018) *AUSTRAC Compliance Guide*. Available at: <http://www.austrac.gov.au/businesses/obligations-and-compliance/austrac-compliance-guide> [Last accessed: 02 January 2019].

## Canada



### RESPONSIBLE REGULATORY AUTHORITIES

Canadian Securities Administrators (CSA)  
Financial Transactions and Reports Analysis  
Centre (FINTRAC)

### RELEVANT REGULATIONS

Proceeds of Crime (Money Laundering) and  
Terrorist Financing Act (*Pending*)  
Securities Act



Date of key guidance issuance [CSA Staff Notice 46-307 Cryptocurrency Offerings]: August 24, 2017

### Cryptoasset Definition and Terminology

A definition of *virtual currency* is proposed in the amendment to *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* as follows:

(a) a digital currency that is not a fiat currency and that can be readily exchanged for funds or for another virtual currency that can be readily exchanged for funds; or (b) information that enables a person or entity to have access to a digital currency referred to in paragraph (a).<sup>196</sup>

The CSA guidance does not explicitly define cryptoassets.

### Relevant Regulation

Key guidance issued under CSA Staff Notice 46-307 outlines how Canadian Securities Laws and ‘substance over form’ tests may apply to ICOs, cryptoasset investment funds and exchanges. Staff Notice 46-308 reiterated the CSA’s views, adding that many purported ‘utility’ tokens were not eligible to be exempt from securities laws, therefore requiring both a prospectus and the registration of the securities issuer. Under the “Pacific Coin Test”, based on the US “Howey Test”, a cryptoasset is a security if it involves an “investment of money in a common enterprise with the expectation of profit that is to come significantly from the efforts of others”.<sup>197</sup>

On August 16, 2017, the first exemption order was issued to an ICO issuer under a February 2017 Regulatory Sandbox Initiative by the CSA.<sup>198</sup> The exemptions from prospectus and registration requirements were subject to a number of conditions, including:

- Delivery of an offering memorandum and certain ongoing information to investors;
- Implementation of various KYC, suitability, AML/CFF procedures;

<sup>196</sup> Parliament of Canada (2014) *Bill C-21, Statute of Canada*. Available at: <http://www.parl.ca/DocumentViewer/en/41-2/bill/C-31/royal-assent> [Last accessed: 21 February 2019].

<sup>197</sup> Canadian Securities Administrators (2018) *Staff Notice 46-308 Securities Law Implications for Offerings of Tokens*. Available at: [https://www.osc.gov.on.ca/documents/en/Securities-Category4/csa\\_20180611\\_46-308\\_implications-for-offerings-of-tokens.pdf](https://www.osc.gov.on.ca/documents/en/Securities-Category4/csa_20180611_46-308_implications-for-offerings-of-tokens.pdf) [Last accessed: 21 February 2019]. The test is based on *Pacific Coast Coin Exchange v. Ontario (Securities Commission)*, [1978] 2 SCR 112.

<sup>198</sup> Radu, A. (2018) “Canada has its first approved cryptocurrency”, *IT World Canada*. Available at: <https://www.itworldcanada.com/article/canada-has-its-first-approved-cryptocurrency/395922> [Last accessed: 21 February 2019].

- A maximum investment limit of \$2,500 for non-accredited investors; and
- Limits on secondary trading.

### Future Outlook

Federal Bill C-31, first tabled in 2014, proposes to treat those dealing in virtual currencies as Money Services Business under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*.<sup>199</sup> Those “dealing in digital currencies” will be required to follow detailed KYC and AML policies and register with the FINTRAC. Such amendments are, however, not currently in force, though it is unclear when they will come into force.

The CSA has been engaged in discussions with industry platforms on applicable guidelines through its regulatory sandbox.<sup>200</sup> On March 14, 2019, Investment Industry Regulatory Organization of Canada (IIROC) issued a joint CSA/IIROC Consultation Paper inviting market participants, investors, fintech community and other stakeholders on how requirements may be tailored for Platforms whose operations engage securities law.<sup>201</sup>

---

<sup>199</sup> Parliament of Canada (2014) *Bill C-21, Statute of Canada*. Available at: <http://www.parl.ca/DocumentViewer/en/41-2/bill/C-31/royal-assent> [Last accessed: 21 February 2019].

<sup>200</sup> Canadian Securities Administrators (2018), CSA Regulatory Sandbox. Available at: [https://www.securities-administrators.ca/industry\\_resources.aspx?id=1588](https://www.securities-administrators.ca/industry_resources.aspx?id=1588) [Last accessed: 15 March 2019]

<sup>201</sup> Investment Industry Regulatory Organization of Canada (2018), “Joint CSA/IIROC Consultation Paper 21-402 Proposed Framework for CryptoAsset Trading Platforms”. Available at: [http://www.iiroc.ca/documents/2019/196069ad-9053-4d8b-8022-a8e11a6c4385\\_en.pdf](http://www.iiroc.ca/documents/2019/196069ad-9053-4d8b-8022-a8e11a6c4385_en.pdf) [Last accessed: 15 March 2019]

## Estonia

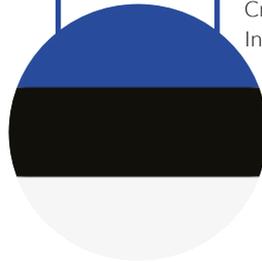


### RESPONSIBLE REGULATORY AUTHORITIES

Financial Intelligence Unit (FIU)  
Financial Supervisory Authority FSA

### RELEVANT REGULATIONS

Money Laundering and Terrorism Financing  
Prevention Act  
Securities Market Act  
Law of Obligations Act  
Credit Institutions Act  
Investment Funds Act (IFA)



**Date of enforcement of retrofitted regulation [Money Laundering Act and Terrorism Financing Prevention Act, 2007]:** November 27, 2017

### Cryptoasset Definition and Terminology

A virtual currency is defined as:

*a value represented in the digital form, which is digitally transferable, preservable or tradable and which natural persons or legal persons accept as a payment instrument, but that is not the legal tender of any country or funds.*<sup>202</sup>

### Relevant Regulations

#### **Applicability of AML/CFT regulations**

In 2017, Estonia was among the first EU member states to implement the 5AMLD proposals to bring cryptoasset exchange and storage activities under the AML/CFT regulations. A licensing regime for cryptoasset exchanges and wallets is embedded in the *Money Laundering Act and Terrorism Financing Prevention Act*.<sup>203</sup> A license decision is based on, *inter alia*, the submission of criminal record documents, a presentation of KYC/AML procedural rules, and the documentation of internal auditing rules. Licensed activities are exchanges and custodial wallet service providers.<sup>204</sup>

#### **Applicability of Securities Law**

A token issuance will be considered a security by the FSA - and require a prospectus - under the *Securities Market Act and the Law of Obligations Act* when (1) its transfer is conditioned by the consent of at least one party; (2) it provides with voting rights or making decisions about the issuer's activities in any other form; (3) it provides with an investment profit.

ICOs used to finance a loans business will likely fall under the purview of the *Credit Institutions Act*.<sup>205</sup>

In other cases, when a token plays a role of a value transfer or a payment medium there are no requirements with regard to its issuer as described above.

<sup>202</sup> Section 3 (9) of the Anti-Money Laundering Act and Terrorism Finance Act in Riigi Teataja (2017) *Money Laundering and Terrorism Financing Prevention Act*. Available at: <https://www.riigiteataja.ee/en/eli/517112017003/consolide> [Last accessed: 14 December 2018].

<sup>203</sup> Para. 70. Idem.

<sup>204</sup> Financial Supervisory Authority (2018) *Information for entities engaging with virtual currencies and ICOs*. Available at: <https://www.fi.ee/en/investment/aktuaalsed-teemad-investeerimises/virtuaalraha-ico/information-entities-engaging-virtual-currencies-and-icos> [Last accessed: 24 January 2019].

<sup>205</sup> For more information, please visit <https://www.fi.ee/index.php?id=21662>.

Operating security token secondary market transactions implies providing investment services and thus requires an authorisation from the FSA as an investment services provider.

### **Future Outlook**

Various stakeholders in Estonia have discussed the idea of launching a state cryptocurrency, Estcoins, in order to invest in a country by means of an ICO within its e-Residency system. European Union institutions have, however, expressed their unsupportive attitude with regard to this project, while the Estonian Government has exhibited indifference. If adopted this project can change policy landscape in Estonia and bring greater regulatory innovations.

## European Union



### RESPONSIBLE REGULATORY AUTHORITIES

European Securities and Markets Authority (ESMA)  
European Banking Authority (EBA)  
European Commission and Parliament

### RELEVANT REGULATIONS

AML Directive (5AMLD)  
MiFID II and a number of related directives (e.g., Prospectus Directive, Transparency Directive, Market Abuse Directive)  
E-Money Directive  
Payment Services Directive



**Date of enforcement of retrofitted regulation [EU AML directive 2018/843 (AMLD5), 2018]:** All member states must translate the 5AMLD into their national legislation by January 10, 2020

### Cryptoasset Definition and Terminology

Regulatory authorities in the EU initially used the term “virtual currency” rather than “cryptoasset”, focusing on the payment function of the underlying tokens. The revised 5AMLD still uses the term *Virtual Currency* (VC), which is defined as:

*a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically.*<sup>206</sup>

However, recent reports use “crypto-asset” as a wider umbrella term rather than “virtual currency”. ESMA provided the following definition of *Crypto-Asset* in its 2019 *Crypto-Asset Advice*:<sup>207</sup>

*a type of private asset that depends primarily on cryptography and Distributed Ledger Technology (DLT) or similar technology as part of their perceived or inherent value. Unless otherwise stated, ESMA uses the term to refer to both so-called ‘virtual currencies’ and ‘digital tokens’. Crypto-asset additionally means an asset that is not issued by a central bank.*

The EBA’s definition is almost identical, adding (i) that crypto-assets can also not be *guaranteed* by a central bank or *public authority* (adding the words “guaranteed” and “public authority”, in line with 5AMLD’s definition of VCs) and (ii) that the asset “can be used as a means of exchange and/or for investment purposes and/or to access a good or service”. Note that previous EBA documents had adopted the term *Virtual Currency*, focusing on the payment function of tokens, but switched to *Crypto-Asset* in its most recent report.<sup>208</sup>

<sup>206</sup> European Banking Authority (2014) *Opinion on ‘Virtual Currencies’*. Available at: <https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08%2BOpinion%2Bon%2BVirtual%2BCurrencies.pdf>. [Last accessed: 10 January 2019]. EU (2018) *5th AMLD 2018/843 Art. 1(2)*. Available at: [https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL%3APE\\_72\\_2017\\_INIT&from=LT](https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL%3APE_72_2017_INIT&from=LT) [Last accessed: 21 December 2018].

<sup>207</sup> European Securities and Markets Authority (2019) *Advice - Initial Coin Offerings and Crypto-Assets*. Available at <https://www.esma.europa.eu/document/advice-initial-coin-offerings-and-crypto-assets> [Accessed: 10 January 2019].

<sup>208</sup> P. 11 in European Banking Authority (2019) *Report with Advice to the European Commission on cryptoassets*. Available at: <https://eba.europa.eu/-eba-reports-on-crypto-assets> [Last accessed: 14 January 2019].

Digital Token is defined by ESMA as:

*any digital representation of an interest, which may be of value, a right to receive a benefit or perform specific functions or may not have a specified purpose or use.*

ESMA's Advice furthermore defined:

- an "Investment-type Crypto-asset" as "a type of crypto-asset that resembles a financial instrument" (a term defined in MiFID II, see below);
- a "Payment-type Crypto-asset" as "a type of crypto-asset that is meant to be used as a means of payment or exchange for goods or services that are external to the DLT ecosystem on which they are built"; and
- a "Utility-type Crypto-asset" as "a type of crypto-asset that provides some 'utility' function other than as a means of payment or exchange for external goods or services".

The EBA's Report uses the same broad classification but describes the three categories slightly differently:

- "Payment/exchange/currency tokens (often referred to as VCs or cryptocurrencies)" "[t]ypically do not provide rights (as is the case for investment or utility tokens) but are used as a means of exchange (e.g. to enable the buying or selling of a good provided by someone other than the issuer of the token) or for investment purposes or for the storage of value." Examples include Bitcoin, Litecoin and Stablecoins, according to the EBA.
- "Investment tokens" "[t]ypically provide rights (e.g. in the form of ownership rights and/or entitlements similar to dividends)."
- "Utility tokens" "[t]ypically enable access to a specific product or service often provided using a DLT platform but are not accepted as a means of payment for other products or services."

Note that the EBA's taxonomy does not classify all tokens "for investment purposes" as an investment-type token: these tokens can be considered payment/exchange/currency tokens if they "do not provide rights". Bitcoin is classified as a payment token, while Ether may be considered a 'hybrid' token, i.e. bearing the characteristics of multiple categories.

## Relevant Regulations

The official position of the three European Supervisory Authorities (ESAs) on cryptoassets was set out in February 2018 warning consumers and investors of the risks associated with cryptoassets.<sup>209</sup>

Different EU supervisory bodies have meanwhile published separate reports on cryptoassets, assessing the applicability and suitability of EU laws within their respective mandates. The paragraphs below look at ESMA's assessment of the applicability of EU financial securities laws to cryptoassets and the EBA's assessment of the EU's e-money laws.

### **Financial Instrument Regulation (MiFID II)**

In a statement released in November 2017, ESMA emphasised that the issuance (ICO) of tokens qualifying as financial instruments is likely to constitute regulated investment activity. *Financial Instruments* are defined in MiFID II and include "'transferable securities', 'money market instruments', 'units in collective investment undertakings' and various derivative instruments."<sup>210</sup>

ESMA provided much more detailed guidance on the EU's legal instruments that may be applicable to cryptoasset activities that qualify as *Financial Instruments* ("Digital Tokens"). It also highlighted a number

<sup>209</sup> European Securities and Markets Authority (2018) *ESMA, EBA and EIOPA warn consumers on the risks of Virtual Currencies*. Available at: [https://www.esma.europa.eu/sites/default/files/library/esma50-164-1284\\_joint\\_esas\\_warning\\_on\\_virtual\\_currencies1.pdf](https://www.esma.europa.eu/sites/default/files/library/esma50-164-1284_joint_esas_warning_on_virtual_currencies1.pdf) [Last accessed: 21 December 2018]

<sup>210</sup> MiFID II consists of Directive 2014/65/EU (MiFID2) and Regulation (EU) No 600/2014 (MiFIR).

of gaps in the EU's regulatory framework, both for tokens that qualify as *Financial Instruments* and those that do not.

Cryptoassets “that qualify as transferable securities or other types of MiFID financial instruments”<sup>211</sup> are likely to be subject to a number of EU laws, such as:

- the Prospectus Directive<sup>212</sup>;
- the Transparency Directive;<sup>213</sup>
- MiFID II;<sup>214</sup>
- the Market Abuse Directive;<sup>215</sup>
- the Short Selling Regulation;<sup>216</sup>
- the Central Securities Depositories Regulation;<sup>217</sup> and
- the Settlement Finality Directive.<sup>218</sup>

These laws create obligations not only for cryptoasset issuers, but also for companies providing “related activities ... likely to qualify as investment services/activities such as placing, dealing on own account, operating an MTF or OTF or providing investment advice.”<sup>219</sup>

**Prospectus Directive:** securities issuance is exempt from a prospectus requirement if the offer is below €1 million (within a 12-month period). Member States may also exempt offers below €8 million.<sup>220</sup>

**MiFID II:** ESMA's preliminary view is that “where crypto-assets qualify as financial instruments, platforms trading crypto-assets with a central order book and/or matching orders under other trading models are likely to qualify as multilateral systems” and will be subject to MiFID II and should therefore either operate under Title III of MiFID 2.”<sup>221</sup>

**Safekeeping:** ESMA's preliminary view is that “having control of private keys on behalf of clients might be regarded as safekeeping services and that rules to ensure the safekeeping and segregation of client assets should apply to the providers of those services.”<sup>222</sup>

### ***E-Money and Payment Services Directives***

The EBA concluded that cryptoassets could be covered by EMD2, PSD2 or neither one, depending on the characteristics of the asset, but did not provide detailed guidance on when this would be the case. It found that “a significant portion of activities involving crypto-assets do not fall within the scope of current EU financial services law (but may fall within the scope of national laws).”

<sup>211</sup> Para. 7, p. 5. in European Securities and Markets Authority (2019) *Advice - Initial Coin Offerings and Crypto-Assets*. Available at <https://www.esma.europa.eu/document/advice-initial-coin-offerings-and-crypto-assets> [Last accessed: 10 January 2019]

<sup>212</sup> Directive 2003/71/EC.

<sup>213</sup> Directive 2004/109/EC.

<sup>214</sup> See note 208.

<sup>215</sup> Directive 2014/57/EU.

<sup>216</sup> Regulation (EU) No 236/2012.

<sup>217</sup> Regulation (EU) No 909/2014.

<sup>218</sup> Directive 2009/44/EC.

<sup>219</sup> Para. 103, p. 24. in European Securities and Markets Authority (2019) *Advice - Initial Coin Offerings and Crypto-Assets*. Available at <https://www.esma.europa.eu/document/advice-initial-coin-offerings-and-crypto-assets> [Last accessed: 10 January 2019].

<sup>220</sup> Art. 3(2) Prospectus Regulation.

<sup>221</sup> Para. 106, p. 25. in European Securities and Markets Authority (2019) *Advice - Initial Coin Offerings and Crypto-Assets*. Available at <https://www.esma.europa.eu/document/advice-initial-coin-offerings-and-crypto-assets> [Last accessed: 10 January 2019].

<sup>222</sup> Para. 164, p. 35. in European Securities and Markets Authority (2019) *Advice - Initial Coin Offerings and Crypto-Assets*. Available at <https://www.esma.europa.eu/document/advice-initial-coin-offerings-and-crypto-assets> [Last accessed: 10 January 2019].

However, the EBA warned that institutions, including e-money and payment institutions, may be bound by procedural and governance obligations under existing EU law even if their activities do not constitute regulated financial services under EU law (e.g. governance risk management requirements). PSD2 and EMD2 furthermore allow authorities to impose measures such as additional capital or reporting requirements.

### **The 5AMLD**

5AMLD extends the scope of AMLD4 to include certain virtual currency exchanges and custodial wallet providers as “Obligated Entities”. “Obligated Entities” will have to be registered, conduct customer due diligence controls and report suspicious transactions to the competent national authorities.<sup>223</sup> Member States have until January 10, 2020 to transpose 5AMLD into their national legislation. Only exchanges providing fiat-to-VCs are covered by 5AMLD, while exchanges providing services for VCs only (i.e. crypto-to-crypto only) and ICO projects remain outside its the scope.

### **Future Outlook**

Although there are very few cryptoasset-specific rules at the EU supranational level at present, this is likely to change in the near future. Both ESMA and the EBA recommended EU-wide regulation on cryptoassets, citing risks to the level playing field where national laws of EU Member States diverge.

ESMA’s Crypto-Asset Advice and the EBA’s Cryptoasset Report recommend a number of legislative changes to regulate cryptoassets at the EU level. Both the EBA and ESMA call on EU policymakers to consider FATFs’ AML/CFT guidelines on cryptoassets and to consider extending 5AMLD to crypto-to-crypto exchanges and providers of financial services for ICOs.<sup>224</sup> It remains to be seen to what extent the EU institutions will follow suit.

ESMA called for EU policymakers to address a number of gaps in the EU’s existing legal framework, which it identified in greater details compared to the EBA guidance. ESMA recommended a bespoke regulatory regime for cryptoassets not qualifying as Financial Instruments under MiFID II, which at this stage should be limited to warning buyers, according to ESMA. More recently, however, ESMA’s chair stated: “we believe that a more elaborate bespoke regime for those crypto-assets that do not qualify as financial instruments is premature” as it “may risk legitimising crypto-assets”.<sup>225</sup>

The EBA called on the European Commission to carry out a cost-benefit analysis to assess whether further action at the EU level is required. This included a call to clarify accounting rules for cryptoassets, which may also be linked to prudential regimes (such as Basel III). The EBA will issue a common monitoring template in 2019, which member states may decide to use in their monitoring for domestic payments (or even financial) institutions.

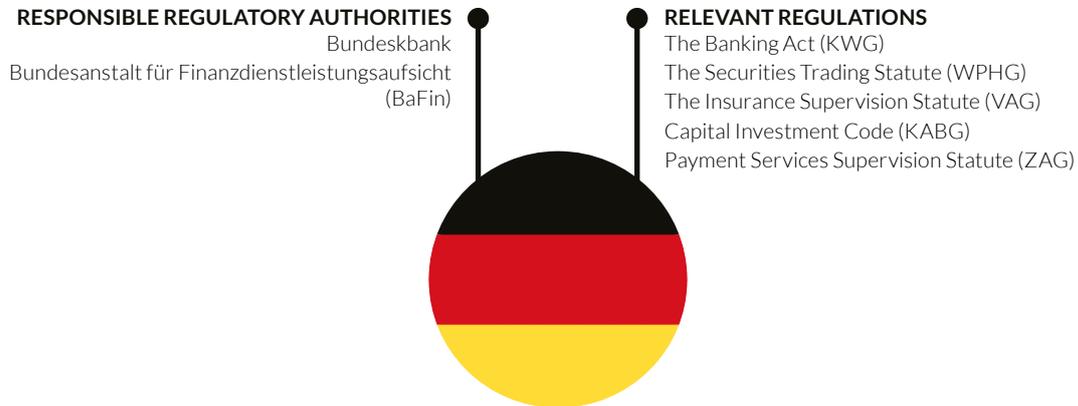
Additionally, the ESAs were expected to publish a Joint Opinion on AML/CFT relating to cryptoasset in January 2019, at the time of this report, the Joint Opinion has not been published.

<sup>223</sup> European Parliament and European Council (2018) *Directive (EU) 2018/843*. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L0843&from=EN> [Last accessed: 21 December 2018].

<sup>224</sup> Para. 169, p. 36. in European Securities and Markets Authority (2019) *Advice - Initial Coin Offerings and Crypto-Assets*. Available at <https://www.esma.europa.eu/document/advice-initial-coin-offerings-and-crypto-assets> [Last accessed: 10 January 2019].

<sup>225</sup> TheTrade (2019) *ESMA chair wants objectivity, open minds for cryptoasset regulation*. Available at: <https://www.thetradenews.com/esma-chair-wants-objectivity-open-minds-crypto-asset-regulation> [Last accessed: 01 March 2019].

## Germany



Date of key guidance issuance [BaFin Statement (GZ: WA 11-QB 4100-2017/0010), 2018]:  
 February 20, 2018

### Cryptoasset Definition and Terminology

German regulators use the term *crypto-token* for digital representations of value in a blockchain data structure.<sup>226</sup>

BaFin takes a case-by-case approach to the classification of cryptoassets under the existing regulations. This approach stresses the material characteristics of a cryptoasset consistent with the principle of technology neutrality. BaFin made a legally binding determination in 2011 (updated in 2016) that ‘virtual currencies’ (i) were not ‘e-money’<sup>227</sup> as defined in the *E-Money Directive 2009/110/EC*, and (ii) were to be considered as financial instruments (*Finanzinstrumente*) being ‘units of account’ (*Rechnungseinheiten*) analogous to foreign currency (*Devisen*) under §1 Abs. 1 Satz 1 of the KWG. Note, however, that the European Banking Authority stated in a January 2019 report that cryptoassets could be covered by the *E-Money Directive* or neither one, depending on the asset’s characteristics.<sup>228</sup> Whether BaFin’s determination on virtual currencies and the *E-Money Directive* is correct, is ultimately subject to review by the Court of Justice of the European Union.

### Relevant Regulations

The mere creation and use of “virtual currencies”, including mining, does not require any authorisation. However, once created, a cryptoasset may be regulated. German law imposes licensing requirements on platforms and exchanges (including miners who trade on their own account or mining pools that offer share in proceeds from mined and sold virtual currencies on commercial basis), but not for miners *per se* or consumers.<sup>229</sup>

<sup>226</sup> The term “token” is perceived as more neutral.

<sup>227</sup> As defined in the *E-Money Directive 2009/110/EC*.

<sup>228</sup> See above, in the section on the European Union.

<sup>229</sup> Bafin (2016) *Virtual Currencies*. Available at: [https://www.bafin.de/EN/Aufsicht/FinTech/VirtualCurrency/virtual\\_currency\\_node\\_en.html](https://www.bafin.de/EN/Aufsicht/FinTech/VirtualCurrency/virtual_currency_node_en.html) [Last accessed: 07 January 2019].

BaFin has clarified the characteristics of regulated financial instruments<sup>230, 231</sup> and has issued an advisory letter on ICOs.<sup>232</sup> Together BaFin letters provide an indication for regulated activities such as:

- **Equity tokens:** Cryptoassets qualify as securities [*Wertpapiere*] if they are transferable and tradable on the capital market and are not used purely as payment instruments;
- **Payment tokens:**
  - The commercial exchange of e.g. bitcoins for euros may require authorisation;
  - The sale of e.g. bitcoins for commission on behalf of another, or the sale of e.g. Bitcoins on behalf of another whereby the Bitcoins are first sold to the intermediary;
  - Trading tokens on a platform may be a payment service;
- **Utility tokens:** Cryptoassets that display hybrid characteristics (either as payment tokens or equity tokens) may trigger regulations, even though pure utility tokens are not subject to any licensing requirements.

## Future Outlook

Currently there is a degree of uncertainty in the future outlook in Germany, arising from the recent decision of the *Kammergericht Berlin* (state court) in a criminal trial concerning an unauthorised bitcoin exchange. In its Judgment of September 25, 2018, the court held that bitcoins were not financial instruments nor units of account, as they lacked the defining characteristics of such (e.g. issuance by a known entity and statutory validity as legal tender).<sup>233</sup> Trading in bitcoins therefore did not require authorisation from BaFin. The court made some direct statements criticising BaFin for overstepping the bounds of its competence by adopting such a broad interpretation.

This criminal law decision is not, in the first instance, binding for BaFin; the latter has been cited expressing the intention to maintain its position,<sup>234</sup> and the Federal Government has spoken out in support of that position.<sup>235</sup> The judgment offers no clear alternative definition of how cryptoassets should be characterised, creating uncertainty. This controversy does not relate to cryptoassets which, unlike Bitcoin, are meant to embody rights (e.g. to securities or investments).

A recent study reveals widespread critical views of cryptoassets among the conventional financial services industry in Germany, and a clear preference for regulation of cryptoassets and ICOs in particular.<sup>236</sup>

<sup>230</sup> BaFin (2018) *Hinweise zu Finanzinstrumenten nach § 1 Abs. 11 Sätze 1 bis 3 KWG (Aktien, Vermögenanlagen, Schuldtitel, sonstige Rechte, Anteile an Investmentvermögen, Geldmarktinstrumente, Devisen, Rechnungseinheiten und Emissionszertifikate)*. Available at: <https://www.bafin.de/dok/7852552> [Last accessed: 07 January 2019].

<sup>231</sup> BaFin (2018) *Merkblatt Finanzinstrumente (Derivate)*. Available at: <https://www.bafin.de/dok/7852554> [Last accessed: 07 January 2019].

<sup>232</sup> BaFin (2018) *Advisory Letter WA 11-QB 4100-2017/0010: Supervisory classification of tokens or cryptocurrencies underlying "initial coin offerings" (ICOs) as financial instruments in the field of securities supervision*. Available at: <https://www.bafin.de/dok/10690958> [Last accessed: 07 January 2019].

<sup>233</sup> Kammergericht Berlin (2018) *Urteil von 25.09.2018 - Az.: (4) 161 Ss 28/18 (35/18)*. Available at: <https://www.online-und-recht.de/urteile/Handel-mit-Bitcoin-ist-nicht-straftbar-da-Bitcoin-kein-Finanzinstrument-im-Sinne-des-KWG-Kammergericht-Berlin-20180925/> [Last accessed: 07 January 2019].

<sup>234</sup> Heise (2018) *Gericht rügt BaFin: Bitcoin-Handel ist nicht strafbar*. Available at : <https://www.heise.de/newsticker/meldung/Gericht-ruegt-BaFin-Bitcoin-Handel-ist-nicht-straftbar-4192635.html> [Last accessed: 30 January 2019].

<sup>235</sup> Frankfurter Allgemeine (2018) *Bundesregierung prüft Gesetze zum Bitcoin-Handel*. Available at: <https://www.faz.net/aktuell/finanzen/digital-bezahlen/finanzministerium-will-aufgaben-der-finanzaufsicht-bafin-im-bereich-des-bitcoin-handels-absichern-15914301.html> [Last accessed: 30 January 2019].

<sup>236</sup> Centre for Financial Studies (2018) *German financial industry takes a critical view of ICOs, calls for stronger regulation*. Available at: <https://www.ifk-cfs.de/media-lounge/news-newsletter/detail/article/cfs-survey-german-financial-industry-takes-a-critical-view-of-icos-calls-for-stronger-regulation.html> [Last accessed: 07 January 2019].

The approach of applying existing regulations to cryptoassets (possibly with incremental changes) is likely to remain the dominant approach in Germany. BaFin President Felix Hufeld confirmed a categorical rejection of the sandbox approach as being opposed to the notion of a regulated market and the fundamental principles of the rule of law.<sup>237</sup> However, the German Ministry of Finance and Ministry for Justice and Consumer Protection have recently published a position paper that sets out a supportive framework for cryptoassets of different kinds, including a more rational treatment under German property law.<sup>238</sup>

---

<sup>237</sup> Hoffman, A. (2018) *Wie der Bafin-Chef zu Fintechs, Big Data und Künstlicher Intelligenz steht (Interview with Felix Hufeld, 15 June 2018)*. Available at: <https://www.gruenderszene.de/fintech/bafin-chef-interview> [Last accessed: 07 January 2019].

<sup>238</sup> Ministry of Finance and Ministry for Justice and Consumer Protection (2019) *Eckpunkte für die regulatorische Behandlung von elektronischen Wertpapieren und Krypto-Token*. Available at: [https://www.bundesfinanzministerium.de/Content/DE/Standardartikel/Themen/Internationales\\_Finanzmarkt/2019-03-08-eckpunkteelektronische-wertpapiere.pdf;jsessionid=589FAD1DC885D403BF31C2ABE0BCEFB6?\\_\\_blob=publicationFile&v=5](https://www.bundesfinanzministerium.de/Content/DE/Standardartikel/Themen/Internationales_Finanzmarkt/2019-03-08-eckpunkteelektronische-wertpapiere.pdf;jsessionid=589FAD1DC885D403BF31C2ABE0BCEFB6?__blob=publicationFile&v=5) [Last accessed: 20 March 2019].

## Japan



### RESPONSIBLE REGULATORY AUTHORITIES

Financial Services Agency (FSA)

### RELEVANT REGULATIONS

Payment Services Act  
Financial Instrument and Exchange Act  
Act on the Prevention of Transfer of Criminal Proceeds



Date of enforcement of retrofitted regulation [Payment Services Act, Act No. 59 of 2009]: April 1, 2017

### Cryptoasset Definition and Terminology

The *Payment Services Act* distinguishes between two types of *virtual currencies*.<sup>239</sup> The first category of virtual currencies is primarily defined as:

*a means of payment...to an unspecified number of people for purchase of goods, lease of goods or as consideration for services rendered...electronically recorded...and not denominated in fiat currency.*

The second category consists of those cryptoassets that can be mutually exchanged with the first category with unspecified persons and can be transferred by means of electronic data processing systems.

### Relevant Regulations

#### *Applicability of Payment Services Act*

Under the *Payment Services Act*, virtual currency exchange services are categorised into:

- Purchase and sale of virtual currencies or exchange for other virtual currencies;
- Any intermediary, brokerage or agency for above purposes;
- Management of user's money or virtual currencies in relation to the previous two activities.

The *Payment Services Act* introduced a registration system for such businesses. Registration is approved on completion of financial and regulatory requirements set out in the legislation, and include:<sup>240</sup>

- Capital requirement: stock capital must be at least JPY 10 million and net assets must not be negative;
- Customer protection: exchanges must provide appropriate information to clients, segregate customer assets, comply with system security measures and AML obligations. As the *Payment Services Act* was amended, AML law was revised to include cryptoasset exchanges as "specified business operators". It requires cryptoasset exchanges to establish an internal control system to prevent money laundering (e.g. KYC requirements upon opening an account and reporting requirements for suspicious trades);

<sup>239</sup> For an English translation of the Act, see <http://www.japaneselawtranslation.go.jp/law/detail/?id=3078&vm=04&re=01> [Last accessed: 07 January 2019].

<sup>240</sup> It should be noted that the term "registration" is commonly used in Japan, but the registration process is akin to a licensing regime.

- Supervision: exchanges must provide the FSA with the right to conduct on-site inspections and to seek clarification in business improvement. The Act furthermore imposes reporting obligations on exchanges. The FSA has full discretion to terminate an exchange registration.

### **Applicability of Financial Instrument Regulations**

With regards to ICOs, the FSA concluded the direction for regulation in the report *Study Group on Virtual Currency Exchange* published on December 21, 2018.<sup>241</sup> According to the report, the issuance of tokens that qualify as a security, such as with profit share, will be regulated under the *Financial Instrument and Exchange Act*.

### **Future Outlook**

From April to December 2018, the FSA held eleven meetings with the Study Group on Virtual Currency Exchanges to discuss legal regulations for cryptoasset exchanges and ICOs.<sup>242</sup> The main points that could lead to the revision of the law are the following:

- Imposing mandatory disclosure of financial statement and transaction price information on cryptoasset exchanges;
- Strengthening countermeasures against the risk of hacking attacks;
- Tightening regulations on the handling of highly anonymous crypto assets (e.g. DASH and ZCash);
- Introducing regulations on margin trading based on cryptoasset;
- Clarifying direction for regulations on ICOs

Based on these directions, the Financial Instruments and Exchange Act and the Payment Services Act are expected to be amended in the near future. Additionally, ICO-related rules are expected to be included in the Japan Virtual Currency Exchange Association (JVCEA) self-regulatory framework.<sup>243</sup>

---

<sup>241</sup> Financial Services Agency (2018) *Study Group on the Virtual Currency Exchange Services*. Available at: <https://www.fsa.go.jp/en/refer/councils/virtual-currency/20181228.html> [Last accessed: 14 March 2019].

<sup>242</sup> All materials prepared for this study group and meeting transcripts are available at: <https://www.fsa.go.jp/news/30/singi/kasoukenkyuukai.html> [Last accessed: 07 January 2019].

<sup>243</sup> Financial Services Agency (2018) *仮想通貨交換業に関する自主規制の概要について*. Available at: <https://www.fsa.go.jp/news/30/singi/20180912-4.pdf> [Last accessed: 07 January 2019].

## Singapore



### RESPONSIBLE REGULATORY AUTHORITIES

Monetary Authority of Singapore (MAS)

### RELEVANT REGULATIONS

Securities and Futures Act (SFA)

Financial Advisers Act (FAA)

Payment Services Bill (Pending)



**Date of Key Guidance Issuance:** November 14, 2017

**Expected date of enforcement of bespoke regime [Payment Services Bill, 2018]:** mid-2019

### Cryptoasset Definition and Terminology

A draft *Payment Services Bill* (Bill) was read for the first time in Parliament on November 19, 2018.<sup>244</sup> The Bill defines the term *virtual currency* as:

*any digital representation of value that— (a) is expressed as a unit; (b) is not denominated in any currency; (c) is a medium of exchange accepted by the public or a section of the public, as payment for goods or services or the discharge of a debt; (d) can be transferred, stored or traded electronically; and (e) satisfies such other characteristics as the Authority may prescribe, but does not include such other digital representation of value that the Authority may prescribe.*<sup>245</sup>

In addition, MAS has referred to *Digital Token* as:

*a cryptographically-secured representation of a token-holder's rights to receive a benefit or to perform specified functions* in several of its statements.<sup>246</sup>

### Relevant Regulations

#### *Applicability of Securities Laws*

MAS released *A Guide to Digital Token Offerings* (the Guide) in 2017, though it is “not exhaustive, it has no legal effect and does not modify or supersede any applicable laws, regulations or requirements”.<sup>247</sup>

An offer or issue of digital tokens may be regulated by MAS if MAS determines that the token is a *capital markets product* under the *Securities and Futures Act* (SFA) (i.e. it resembles either an ownership interest

<sup>244</sup> Kit, T.S. (2018) Bill proposes changes to enhance Singapore's payment services regulations. *Channel News Asia*. Available at: <https://www.channelnewsasia.com/news/singapore/payment-services-bill-enhances-regulations-10946048> [Last accessed: 20 December 2018].

<sup>245</sup> Payment Services Bill s2(1), entry in force pending.

<sup>246</sup> Monetary Authority of Singapore (2018) *MAS warns Digital Token Exchanges and ICO Issuer*. Available at: <http://www.mas.gov.sg/News-and-Publications/Media-Releases/2018/MAS-warns-Digital-Token-Exchanges-and-ICO-Issuer.aspx> [Last accessed: 20 December 2018]; Monetary Authority of Singapore (2017) *MAS clarifies regulatory position on the offer of digital tokens in Singapore*. Available at: <http://www.mas.gov.sg/News-and-Publications/Media-Releases/2017/MAS-clarifies-regulatory-position-on-the-offer-of-digital-tokens-in-Singapore.aspx> [Last accessed: 20 December 2018].

<sup>247</sup> Monetary Authority of Singapore (2017) *A Guide to Digital Token Offerings*. Available at: <http://www.mas.gov.sg/~media/MAS/Regulations%20and%20Financial%20Stability/Regulations%20Guidance%20and%20Licensing/Securities%20Futures%20and%20Fund%20Management/Regulations%20Guidance%20and%20Licensing/Guidelines/A%20Guide%20to%20Digital%20Token%20Offerings%20%2014%20Nov%202017.pdf> [Last accessed: 13 December 2018]. An updated version of the Guide was released on November 30, 2018.

in a corporation or product, debt, or a share in an investment scheme).<sup>248</sup> Such a token will be treated identically to any other capital market product under SFA, which includes the requirement that the offer be accompanied by a properly prepared prospectus registered with MAS.<sup>249</sup>

A prospectus exemption may apply if: (a) the total value of the offering does not exceed S\$5 million or the equivalent in foreign currency within a 12-month period; (b) the offering is a private placement offer made to maximum 50 people within a 12-month period; (c) the offer is only made to institutional investors; (d) the offer is made to accredited investors. MAS stressed that the above-mentioned exemptions are subject to certain conditions, which includes advertising restrictions, authorisation and recognition requirements (when an offer is made in relation to units of a collective investment scheme).<sup>250</sup>

The Guide specifies that certain intermediaries might be required to hold various licenses or seek approval from MAS, unless otherwise exempt. First, any intermediary who facilitates primary offers or issues of digital tokens that constitute a capital markets product must hold a Capital Markets Services License for that regulated activity under the SFA.<sup>251</sup> Second, any intermediary that provides financial advice in Singapore in respect of any digital token must have a financial adviser's license under the FAA.<sup>252</sup> Third, any intermediary that establishes or operates a trading platform in Singapore in relation to digital tokens must be approved by MAS as an approved exchange or recognised by MAS as a recognised market operator under the SFA.<sup>253</sup>

SFA requirements apply to a person that operates a primary platform, or trading platform, partly in or partly outside of Singapore, or outside of Singapore.<sup>254</sup> FAA requirements apply to a person who is based overseas and engages in any activity or conduct that is intended to or likely to induce the public, or a section of the public, in Singapore to use any financial advisory service provided by the person.<sup>255</sup>

### **Applicability of AML regulations**

Digital tokens not under the supervision of MAS' regulatory purview may nonetheless be subject to other laws for combating money laundering and terrorism financing, including Notices on *Prevention of Money Laundering and Countering the Financing of Terrorism*.<sup>256</sup>

### **Applicability of Payment Services Bill**

The *Payment Services Bill* streamlines the regulation of payment services within a single activity-based legislation.<sup>257</sup> Providers of payment or exchange services will be required to obtain a license and comply with specific conduct of business requirements. The activity of "buying or selling virtual currency, or providing a platform to allow persons to exchange virtual currency in Singapore" will become an activity regulated under the Bill once it enters in force.<sup>258</sup>

<sup>248</sup> Idem. Paras. 2.1., 2.3 and 2.4. Under section 2(1) of the SFA, "capital market products" means any securities, futures contracts or arrangements for the purposes of foreign exchange trading, contracts or arrangements for the purposes of leveraged foreign exchange trading, and such other products as MAS may prescribe as capital markets products.

<sup>249</sup> Idem. Para. 2.4.

<sup>250</sup> Idem. Paras. 2.6. and 2.7. On these exemptions in detail in the context of crowdfunding Hofmann, C. (2018) An Easy Start for Start-ups: Crowdfunding Regulation in Singapore. *Berkeley Business Law Journal* 219, 15:1 236-239. Available at: <https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1127&context=bbjl> [Last accessed: 20 December 2018].

<sup>251</sup> Para. 2.9. Monetary Authority of Singapore (2017) *A Guide to Digital Token Offerings*. Available at: <http://www.mas.gov.sg/~media/MAS/Regulations%20and%20Financial%20Stability/Regulations%20Guidance%20and%20Licensing/Securities%20Futures%20and%20Fund%20Management/Regulations%20Guidance%20and%20Licensing/Guidelines/A%20Guide%20to%20Digital%20Token%20Offerings%20%2014%20Nov%202017.pdf> [Last accessed: 13 December 2018].

<sup>252</sup> Idem. Para. 2.10.

<sup>253</sup> Idem. Para. 2.11.

<sup>254</sup> Idem. Para. 2.12. Section 339 SFA.

<sup>255</sup> Idem. Para. 2.13. Section 6(2).

<sup>256</sup> Idem. Para. 3.2.

<sup>257</sup> Payment services are currently regulated under the *Payment Systems (Oversight) Act* and *Money-Changing and Remittance Businesses Act*.

<sup>258</sup> The bill has not passed parliamentary hearings yet.

## Future Outlook

The *Payment Services Bill* has been moved to Parliament for the First Reading and is expected to be passed shortly.<sup>259</sup> It is likely that MAS's regulatory approach towards cryptocurrencies and cryptoassets will strive to strike a balance between investor protection and encouraging innovation in the cryptoasset space.<sup>260</sup>

---

<sup>259</sup> Linklaters (2019) *The Payment Services Bill has been moved for First Reading in Singapore Parliament*. Available at: <https://www.linklaters.com/en/insights/publications/asia-news/asia-financial-regulation/2019/the-payment-services-bill-has-been-moved-for-first-reading-in-singapore-parliament> [Last accessed: 21 February 2019].

<sup>260</sup> Monetary Authority of Singapore (2018) *"Crypto Tokens: The Good, The Bad, and The Ugly" - Speech by Mr Ravi Menon, Managing Director, MAS, at Money20/20*. Available at: <http://www.mas.gov.sg/News-and-Publications/Speeches-and-Monetary-Policy-Statements/Speeches/2018/Crypto-Tokens-The-Good-The-Bad-and-The-Ugly.aspx> [Last accessed: 20 December 2018].

## United Kingdom



### RESPONSIBLE REGULATORY AUTHORITIES

Bank of England (BoE)  
Financial Conduct Authority (FCA)  
Her Majesty Treasury (HMT)

### RELEVANT REGULATIONS

Payment Services Regulations (PSRs)  
E-Money Regulations (EMRs)



Date of key guidance issuance [Cryptoasset Taskforce Final Report]: October 26, 2018

### Cryptoasset Definition and Terminology

The UK Parliament Treasury Committee views *cryptocurrencies* as:

*intended to function as a means of payment for goods and services. They differ from traditional currencies in that they are not issued by central banks, and in that they can be transferred electronically between users without involvement of intermediaries (i.e. private banks) or the oversight of a central authority (i.e. central bank). Instead holdings of cryptocurrency are typically stored on a publicly-visible, decentralised electronic ledger (known as blockchain) and transactions (changes to the ledger) are verified through consensus among users.*<sup>261</sup>

### Relevant Regulations

As a Member of the European Union, the UK is required to transpose 5AMLD, into its domestic law by 10 January 2020, which will bring fiat-to-crypto exchanges and custodial wallet providers under the scope of AML regulations.

Beyond the issuance of warnings to consumers and investors, the FCA uses a case-by-case approach to determine if a cryptoasset falls under existing regulations, by for instance mimicking an IPO, a private placement of securities, a crowdfunding or a collective investment scheme.<sup>262</sup> Additionally, the FCA stated that cryptoasset derivatives qualify as financial instruments. Entities engaged in regulated activities in cryptoasset derivatives (futures, CFDs, and options) must comply with the FCA Handbook and requirements under MiFID II.<sup>263</sup>

<sup>261</sup> House of Commons Treasury Committee (2018) *Crypto-assets*. Available at: <https://publications.parliament.uk/pa/cm201719/cmselect/cmtreasy/910/910.pdf> [Last accessed: 08 January 2019].

<sup>262</sup> Financial Conduct Authority (2017) *Consumers warning about the risk of Initial Coin Offerings (ICOs)*. Available at: <https://www.fca.org.uk/news/statements/initial-coin-offerings> [Last accessed: 08 January 2019].

<sup>263</sup> Financial Conduct Authority (2018) *Cryptocurrencies Derivatives*. Available at: <https://www.fca.org.uk/news/statements/cryptocurrency-derivatives> [Last accessed: 08 January 2019]. For further information about applicable European regulations please refer to the *European Union* section.

In January 2019, the FCA published its consultation on cryptoasset guidance.<sup>264</sup> The guidance provides industry with an explanation of where cryptoassets interact with its regulatory perimeter. In particular, it looks at three types of cryptoasset tokens: exchange (e.g., Bitcoin and Litecoin), utility and security. The draft guidance indicates the following:

- Security tokens will fall within the regulatory perimeter under securities;
- Utility and exchange tokens will be outside the regulatory perimeter unless they constitute e-money or are used to facilitate regular payments;
- Transferable securities (under MiFID II) will be subject to additional regulatory requirements.

### Future Outlook

Later in 2019 the FCA will consult on banning the sale of derivatives linked to certain types of cryptoassets to retail investors. Additionally, the Government is planning to consult on whether to expand the regulatory perimeter to include further cryptoasset activities.

The FCA continues to support its Regulatory Sandbox, which saw 38% of firms testing in Cohort 4 using DLT or blockchain technology. Setting out these actions has generally been welcomed by industry and shows that the UK is open to cryptoasset and DLT innovations. The Taskforce report itself demonstrates that the authorities are committed to promoting innovation in a joined up and collaborative approach.

---

<sup>264</sup> Financial Conduct Authority (2019) CP19/3: *Guidance on Cryptoassets*. Available at: <https://www.fca.org.uk/publications/consultation-papers/cp19-3-guidance-cryptoassets> [Last accessed: 08 March 2019].

## Existing Regulation

### China



#### RESPONSIBLE REGULATORY AUTHORITIES

People's Bank of China (PBC)  
State Council

#### RELEVANT REGULATIONS

AML Law  
Ban on cryptoasset-to-fiat exchanges  
Ban on ICOs



Date of key guidance issuance [Announcement of the People's Bank of China, the Office of the Central Leading Group for Cyberspace Affairs, the Ministry of Industry and Information Technology and Other Departments on Preventing the Financing Risks of Initial Coin Offerings, 2017]:  
September 4, 2017

#### Cryptoasset Definition and Terminology

No government body has provided definitions for *cryptoasset*.

#### Relevant Regulations

The scope of a 2013 Notice on Bitcoin<sup>265</sup> was expanded on September 4, 2017, when the PBC and other government ministries issued a joined statement – the *Announcement of the People's Bank of China, the Office of the Central Leading Group for Cyberspace Affairs, the Ministry of Industry and Information Technology and Other Departments on Preventing the Financing Risks of Initial Coin Offerings*.<sup>266</sup>

This Notice affirmed the legal ban on trading platforms offering cryptoasset to fiat currency exchange, explicitly mentioning Bitcoin and Ethereum, and reiterated that ICOs are considered unauthorised public financing. Any ICOs and ICO-related businesses are banned and will be considered an illegal issuance of securities, illegal fundraising and financial fraud.

Other PBC guidelines do not make reference to cryptoassets specifically, yet still define P2P, asset management, private equity and third-party payments as false advertising, which is of relevance for cryptoassets.<sup>267</sup> The PBC has also made it clear that cryptoasset activities may incur criminal sanctions under foreign exchange management and AML laws.<sup>268</sup>

<sup>265</sup> People's Bank of China (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: <http://www.pbc.gov.cn/zhengwugongkai/127924/128038/128109/969289/index.html> [Last accessed: 07 January 2019].

<sup>266</sup> People's Bank of China (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: <http://www.pbc.gov.cn/goutongjiaoliu/113456/113469/3374222/index.html> [Last accessed: 07 January 2019].

<sup>267</sup> General Office of the State Council (2016) *Notice of the General Office of the State Council on Issuing the Implementation Plan for Special Rectification on Risks in Internet Finance No. 21*. Available at: <http://lasa.pbc.gov.cn/lasa/120476/3159644/index.html> [Last accessed: 07 January 2019].

<sup>268</sup> Idem.

In October 13, 2016, the Leading Group of Internet Financial Risks Remediation issued instructions to local governments for an “orderly exit” of Bitcoin miners, who were to be gradually phased out.<sup>269</sup>

In a notice of September 28, 2018, the PBC reiterated China’s cautionary stance on cryptoassets and ICOs as illegal financing.<sup>270</sup> It reinforces the regulatory view of the Central Bank that speculative investment in cryptoassets is a threat to the economic, financial and social order.

### Future Outlook

Though the Government’s negative stance on cryptoassets and the risk of criminal sanctions for cryptoasset activities dampened Chinese local trading,<sup>271</sup> the Government may be exploring a different regulatory path for cryptoassets, shifting from an outright ban to a regulated cryptoasset industry. Several observers suggest that China’s current ban is not definitive and expect the country to allow cryptoasset companies to operate again in the near future but under stringent control of the Government.<sup>272</sup> Furthermore, the Government entered into a *Financial Supervisory Cooperation Agreement* with South Korea to facilitate information exchange and strengthen monitoring efforts between the two countries.<sup>273</sup>

---

269 Wu, Y (2018) China clamps down on down on preferential treatment for Bitcoin mines. *Caixin Global*. Available at: <https://www.caixinglobal.com/2018-01-04/china-clamps-down-on-preferential-treatment-for-bitcoin-mines-101193622.html> [Last accessed: 07 January 2019].

270 People’s Bank of China (2018) *Continued Prevention of the Risks in ICO and Virtual Currency trading*. Available at: <http://shanghai.pbc.gov.cn/fzhshanghai/113571/3629984/index.html> [Last accessed: 07 January 2019].

271 Red Li, [https://twitter.com/redtheminer/status/1032163259300737024?ref\\_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwtterm%5E1032163259300737024&ref\\_url=https%3A%2F%2Fwww.coininsider.com%2Fchinese-govt-ban%2F](https://twitter.com/redtheminer/status/1032163259300737024?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwtterm%5E1032163259300737024&ref_url=https%3A%2F%2Fwww.coininsider.com%2Fchinese-govt-ban%2F) [Last accessed: 07 January 2019].

272 Flux Podcast (2017) *Arthur Hayes: The Wild West of Crypto Futures*. Available at: <https://medium.com/@TheFluxPodcast/15-arthur-hayes-the-wild-west-of-crypto-futures-b21af4773768> [Last accessed: 07 January 2019].

273 Helms, K. (2018) South Korea’s Crypto Regulation Shakeup: New Bureau, Agreement With China. *Bitcoin.com*. Available at: <https://news.bitcoin.com/south-koreas-crypto-regulation-agreement-china/> [Last accessed: 14 January 2019].

## Hong Kong

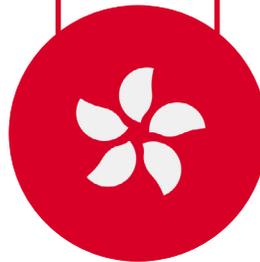


### RESPONSIBLE REGULATORY AUTHORITIES

Securities and Futures Commissions (SFC)  
Hong Kong Monetary Authority

### RELEVANT REGULATIONS

Securities and Futures Ordinance  
Anti-Money Laundering and Counter-Terrorist  
Financing Ordinanc



Date of key guidance issuance [Statement on regulatory framework for virtual asset portfolios managers, fund distributors and trading platform operators]: November 1, 2018

### Cryptoasset Definition and Terminology

The Hong Kong Securities and Futures Commission (SFC) uses the term *virtual asset*, for which it provides an open-ended definition:

*a virtual asset is a digital representation of value, which is also known as 'cryptocurrency', 'crypto-asset' or 'digital token'. The polymorphous and evolving features of virtual assets mean that they may be, or claim to be, a means of payment, may confer a right to present or future earnings or enable a token holder to access a product or service, or a combination of any of these functions.*<sup>274</sup>

Cryptoasset that do not qualify as a security, such as Bitcoin, are considered virtual commodities by Hong Kong's regulatory authorities.

### Relevant Regulations

#### Applicability of Securities Law

Since no new legislation has been introduced in Hong Kong specifically governing cryptoassets, related activities are primarily regulated under the *Securities and Futures Ordinance* (SFO), when the cryptoasset fall within the definition of *securities* or *future contracts*.<sup>275</sup> Such activities may require a license.<sup>276</sup>

In November 2018, the SFC issued an initial regulatory framework for virtual assets funds,<sup>277</sup> applicable to licensed and registered intermediaries, as well as all funds investing in any cryptoassets. This circular restricts the sale of cryptoasset products not authorised by the SFC to professional investors. The circular requires funds without an authorisation from the SFC to conduct an examination of the

<sup>274</sup> Securities and Future Commission (2018) *Statement on regulatory framework for virtual asset portfolios managers, fund distributors and trading platform operators*. Available at <https://www.sfc.hk/web/EN/news-and-announcements/policy-statements-and-announcements/reg-framework-virtual-asset-portfolios-managers-fund-distributors-trading-platform-operators.html> [Last accessed: 10 April 2019].

<sup>275</sup> *Securities and Futures Ordinance, Chapter 571 Laws of Hong Kong*. Available at: <https://www.elegislation.gov.hk/hk/cap571> [Last accessed: 10 April 2019].

<sup>276</sup> Section 114(1), SFO.

<sup>277</sup> Securities and Futures Commission (2018) *Circular to intermediaries: Distribution of virtual asset funds*. Available at: <https://www.sfc.hk/edistributionWeb/gateway/EN/circular/doc?refNo=18EC77> [Last accessed: 10 April 2019].

fund manager, its operations and risk management, and provide background and pricing information for customers on the products sold. In this respect, firms engaged in the distribution of funds that invest in cryptoassets are required to be licensed with the SFC, irrespective of the cryptoassets' legal qualification.

The SFC notice, *Regulatory standards for licensed corporations managing virtual asset portfolios*, sets out the regulatory standards imposed by the SFC on licensed corporations managing portfolios that invest in cryptoassets.<sup>278</sup> Under the SFO, an asset manager would only be subject to SFC regulation if it manages assets classifiable as securities or futures contracts. However, under the notice, if it distributes a fund under its management that includes a collective investment scheme investing in cryptoassets, even if these are neither securities nor futures contracts, the manager will be required to be licensed by the SFC for asset management. Moreover, licensed asset managers that invest 10% or more of their gross asset value in cryptoassets will be subjected to specific investor protection rules. The SFC requires all asset managers, licensed or not, and regardless of how the cryptoassets are classified, to seek out an SFC opinion on the applicable regime of regulation.

The SFC's *Conceptual framework for the potential regulation of virtual asset trading platform operators* follows the same experimentation route by asking platforms that trade cryptoassets *not* constituting securities to volunteer for placement in the SFC regulatory sandbox.<sup>279</sup> If the SFC finds that they comply with the regulatory standards for automated trading systems of securities as seen necessary in light of the activity undertaken, the trading platform may be considered for licensing.

### **Applicability of AML regulations**

The use of cryptoassets is also subject to existing AMF regulations, primarily governed by the Anti-Money Laundering and Counter-Terrorist Financing Ordinance (AMLO), requiring financial institutions and designated non-financial businesses and professions (DNFBP) to report any suspicious transactions to the Joint Financial Intelligence Unit (JFIU) under domestic criminal statutes. In addition, entities dealing with cryptoasset and involved in money changing or remittance services are required to apply to the Commissioner of Customs and Excise for a "money service operator" licence under the AMLO, and subsequently comply with CDD and reporting requirement.

### **Future Outlook**

In March 2019, the Hong Kong Monetary Authority endorsed the Basel Committee on Banking Supervision's statement on cryptoassets, demonstrating the regulator's willingness to address regulatory issues surrounding cryptoasset activities and align its position with other domestic and supranational regulatory bodies.<sup>280</sup>

As an international financial centre that has primary focus on fund flows into and out of mainland China, it is quite certain that Hong Kong will continue to search for the optimal balance between allowing the distribution of attractive financial products and protecting the order (and reputation) of its market. The SFC's current use of case-by-case analysis and sandbox observation serve the purpose of seeking this balance. Knowledge derived from this experimentation will likely feed into a more generalised source of regulatory guidance in the future, which could reduce contingent legal risk for financial institutions.

<sup>278</sup> Securities and Futures Commission (2018) *Regulatory standards for licensed corporations managing virtual asset portfolios*. Available at: [https://www.sfc.hk/web/EN/files/ER/PDF/App%201%20-%20Reg%20standards%20for%20VA%20portfolio%20mgrs\\_eng.pdf](https://www.sfc.hk/web/EN/files/ER/PDF/App%201%20-%20Reg%20standards%20for%20VA%20portfolio%20mgrs_eng.pdf) [Last accessed: 10 April 2019].

<sup>279</sup> Securities and Futures Commission (2018) *Conceptual framework for the potential regulation of virtual asset trading platform operators*. Available at: [https://www.sfc.hk/web/EN/files/ER/PDF/App%202\\_%20Conceptual%20framework%20for%20VA%20trading%20platform\\_eng.pdf](https://www.sfc.hk/web/EN/files/ER/PDF/App%202_%20Conceptual%20framework%20for%20VA%20trading%20platform_eng.pdf) [Last accessed: 10 April 2019].

<sup>280</sup> Hong Kong Monetary Authority (2019) *Endorsement letter – BCBS statement on Crypto-Assets*. Available at: <https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2019/20190318e1.pdf> [Last accessed: 10 April 2019].

## India



### RESPONSIBLE REGULATORY AUTHORITIES

Reserve Bank of India (RBI)

### RELEVANT REGULATIONS

Payment and Settlements System Act (PSSA)  
Prevention of Money Laundering Act (PMLA)



**Date of directive issuance [Directive on Prohibition on dealing in Virtual Currencies]:** April 6, 2018

### Cryptoasset Definition and Terminology

The RBI's 2018 Prohibition of Virtual Currencies uses the term *virtual currencies*, however this term has not been defined within the country's legal framework.<sup>281</sup>

### Relevant Regulations

The RBI's directive prohibits regulated entities from dealing in virtual currencies or provide services for facilitating any person or entity in dealing with or settling those assets. Such services include 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 the purchase/sale of cryptoassets.<sup>282</sup> Though users may be able to deal in virtual currencies, they cannot exchange or redeem them through banking channels (i.e. regulated entities within the ambit of the directive).

The Indian Government has also undertaken other measures including, primarily, restricting the primary business of cryptoasset trading platforms and a series of press releases by the RBI cautioning users, holders and traders of cryptoassets such as Bitcoin about the potential financial, operational, legal, customer protection and security related risks.<sup>283</sup>

### Applicability of KYC/AML/CFT regulations

The use of cryptoassets may be covered under the *Prevention of Money Laundering Act, 2002* (PMLA), which foresees statutory penalties of up to 10 years of imprisonment. However, it is unclear whether the reporting obligations prescribed under Chapter IV of the PMLA extend to wallet operators, cryptoasset exchanges or third-party Bitcoin services. A majority of cryptoasset trading platforms are self-regulatory and follow extensive KYC/AML norms. It is also likely, based on the Government press comments, that

<sup>281</sup> Reserve Bank of India (2018) *Prohibition on dealing in Virtual Currencies (VCs)*. Available at: [https://www.rbi.org.in/scripts/FS\\_Notification.aspx?Id=11243&fn=2&Mode=0](https://www.rbi.org.in/scripts/FS_Notification.aspx?Id=11243&fn=2&Mode=0) [Last accessed: 07 January 2019].

<sup>282</sup> Idem.

<sup>283</sup> A similar approach is seen in countries like China and Iran. In this regard, RBI has said, "The absence of information of counterparties in such peer-to-peer anonymous/ pseudonymous systems could subject the users to unintentional breaches of anti-money laundering and combating the financing of terrorism (AML/CFT) laws." Reserve Bank of India (2017) *RBI Cautions users of Virtual Currencies*. Available at: [https://www.rbi.org.in/Scripts/BS\\_PressReleaseDisplay.aspx?prid=39435](https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=39435) [Last accessed: 07 January 2019]. Similar warning have also been issued on December 24, 2013 (Available at: [https://rbi.org.in/Scripts/BS\\_PressReleaseDisplay.aspx?prid=30247](https://rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=30247)) and December 5, 2017 (Available at: [https://rbi.org.in/scripts/BS\\_PressReleaseDisplay.aspx?prid=42462](https://rbi.org.in/scripts/BS_PressReleaseDisplay.aspx?prid=42462)) [Last accessed: 07 January 2019].

many cryptoasset businesses may come under the scope of a new regulation which would oblige them to comply with KYC/AML obligations. It is also important to note that India is a signatory to the U.S. *Foreign Account Tax Compliance Act* (FATCA) and the OECD's Common Reporting Standards (CRS) which require the Reporting Financial Entities (RFIs) to maintain and report information in respect of reportable accounts. The existing AML/CFT regime therefore does enable limited oversight of convertible cryptoassets.

#### **Applicability of financial instrument regulations**

Although there is no specific law on cryptoassets yet, a number of existing laws may be applicable. For ease of reference, we grouped these laws, based on the 3-category token classification adopted in many other jurisdictions (note that this classification has not been adopted by Indian regulators):

- **Security tokens:** currently, there is regulatory uncertainty regarding applicability of the *Securities Contracts (Regulation) Act, 1956* (SCRA) to tokens, though some tokens issued through ICOs may fall within its remit if, *inter alia*, they are issued by an identifiable issuer and backed by the underlying assets of the issuer. Some tokens may also fall within the purview of collective investment schemes which are regulated by the Securities and Exchange Board of India (SEBI).
- **Utility tokens:** certain cryptoassets could be considered acknowledgements issued in return for advance paid for services (i.e. deposits) to be rendered in the future. If these are classified as such, the regulations under the Companies Act, 2013 and rules thereunder would be triggered, along with other RBI regulations. Further, a bill entitled *Banning of Unregulated Deposit Schemes Bill, 2018* has been tabled in Parliament, which proposes to prohibit all unregulated deposits. ICO issuers would need to ensure that any money received should not be liable to be returned in order to be outside the purview of this Bill.
- **Payment tokens:** a token may be intended to be used as means of payment for trading goods and services. In such cases, the payment tokens may be subject to regulation under PSSA.

#### **Payment systems regulation**

There is nothing in the *Payments and Settlements Systems Act, 2007* (PSSA) to exclude virtual currency, since only the term payment is referred to, as opposed to currency, legal tender or money.<sup>284</sup> Thus, if a cryptoasset activity were to constitute a "payment system" or other regulated activity, the issuer would need payment system authorisation from the RBI under PSSA and would require compliance with KYC/AML norms.

#### **Licensing Requirements**

Though licensing requirements are not directly applicable to intermediaries performing storage, exchange, payments, mining etc., Indian laws do regulate various kinds of financial services. Under Indian laws, cryptoassets may be subject to import and export restrictions if a person resident in India enters into a purchase/sale transaction with any resident outside India, as per the provisions of the *Foreign Exchange Management Act* (FEMA).<sup>285</sup> In such cases, *FEMA (Current Account Transactions) Rules* may apply.

<sup>284</sup> It may be noted that many virtual currencies do not form a part of a system that constitutes payments, in which case they would not be subject to PSSA.

<sup>285</sup> The *Foreign Exchange Management Act* also apply to the broader category of intangible moveable property, capital accounts and current account transactions.

## Future Outlook

The Government is planning to regulate transactions with cryptoassets in the country, the framework for which is expected to be released soon.<sup>286</sup> Following the issuance of the 2018 Directive, a number of industry players have petitioned the Supreme Court on constitutional grounds which include, *inter alia*, a violation of the fundamental right to trade.<sup>287</sup> Despite the regulatory uncertainty and the crippling effect of the 2018 Directive, cryptoassets are still increasingly being used in India.

---

<sup>286</sup> As stated earlier, a government committee comprising of officials from Ministry of Finance and RBI is due to submit a report recommending steps to regulate cryptocurrencies. This report is expected by the end of 2018. Dasgupta N., Roy A. (2018) India's cryptocurrency investors bet trading will survive bank ban. *Reuters*. Available at: <https://www.reuters.com/article/us-cryptocurrencies-india/indias-cryptocurrency-investors-bet-trading-will-survive-bank-ban-idUSKBN1I50J7> [Last accessed: 07 January 2019].

<sup>287</sup> Article 19 in Government of India (1950) Constitution of India, 1950. Available at: [https://www.india.gov.in/sites/upload\\_files/mpi/files/coi\\_part\\_full.pdf](https://www.india.gov.in/sites/upload_files/mpi/files/coi_part_full.pdf) [Last accessed: 07 January 2019].

## South Korea



### RESPONSIBLE REGULATORY AUTHORITIES

Financial Services Commission (FSC)  
Financial Supervisory Service (FSS)  
Financial Intelligence Unit  
Bank of Korea

### RELEVANT REGULATIONS

Financial Investment Services and Capital Markets Act (FISCMA)  
Act on Reporting and Use of Certain Financial Transaction Information



**Date of key guidance issuance [Virtual Currency Anti- Money Laundering Guidelines, 2018]:** January 30, 2018 (revised on July 10, 2018)

### Cryptoasset Definition and Terminology

No official definition is currently available.

### Relevant Regulations

Existing Korean regulations such as the *Financial Investment Services and Capital Markets Act* (FISCMA), which regulates cryptoassets in the nature of securities, tax laws and anti-money laundering guidelines apply. Since the indictment of several individuals relating to a digital currency Ponzi scheme, several draft cryptoasset regulations proposed by the National Assembly have been tabled and are currently under consideration by the Parliament. In July 2017, a member of the National Assembly's Committee on Legislation initiated the revision of the *Financial and Electronic Commerce Act* which would make cryptocurrency transactions liable to taxation.

The Government has put forth successive measures to lower and monitor speculative behaviour involving cryptoassets and to avoid illegal activities. The first set of such measures were aimed at establishing strong penalties and preventing imprudent entry from new investors. There are also guidelines applicable on financial institutions mandating reporting of suspected financial transactions<sup>288</sup> and verification of identity/other information to prevent money laundering (AML Guidelines), by providing for expansion of monitoring to non-deposit accounts and share of the list of foreign cryptocurrency intermediaries among financial institutions.<sup>289</sup> The guidelines, along with the *Act on Reporting and Using Specified Financial Transaction Information* aims to impede illegal cryptoasset transactions.

In order to curb potential violations of lending/borrowing laws, the FSC announced a prohibition for individuals to transact cryptocurrencies on crypto-exchanges and also directed financial institutions to restrict such activities. Token offerings to the public in any form are considered illegal in South Korea and are liable to offering restrictions, irrespective of whether it is classified as 'securities' or not. The country also restricts foreigners and minors from trading in cryptocurrencies.<sup>290</sup>

<sup>288</sup> Korean Financial Intelligence Unit (2018) *Guidelines for Anti-Money Laundering with Cryptocurrency*. Available at: <http://m.fsc.go.kr/common/mFileDownload.do?BBS=BBS0030&FILENO=123190> [Last accessed: 26 February 2019].

<sup>289</sup> Financial Services Commission (2001) *Act on Reporting and Specified Financial Transaction Information*, art. 5. Available at: [https://elaw.klri.re.kr/kor\\_service/lawView.do?lang=ENG&hseq=44449](https://elaw.klri.re.kr/kor_service/lawView.do?lang=ENG&hseq=44449) [Last accessed: 26 February, 2019].

<sup>290</sup> Financial Services Commission (2017) *Special Measures for the Elimination of Virtual Currency Speculation, Enforcement of Financial Sector Measures*. Available at: <http://www.korea.kr/common/download.do?tblKey=GMN&fileId=185832583> [Last accessed: 14 February, 2019].

The South Korean Government has also enacted other measures such as the implementation of a ‘real-name trading system’ for cryptoasset transactions, whereby cryptocurrency trading could only take place through real-name bank accounts held at the same bank as those of crypto-exchanges, in an effort to curb money laundering.<sup>291</sup> The real-name system has been operating since January 2018.

### Future Outlook

The Korean Government’s position on cryptoasset exchanges being “speculation out of law” has been subject to severe criticism in the recent past. After the statements by the government, the regulatory uncertainty has resulted in a decreased volume of cryptoasset transactions and numerous projects initially established in South Korea have relocated their activity in other friendlier jurisdictions, such as Singapore.<sup>292</sup>

There are plans to conduct on-site inspections of intermediaries, jointly managed by Financial Intelligence Unit and Financial Supervisory Service. However, despite this position, the FSS, in a statement issued in February 2018 has encouraged financial institutions to do business with cryptocurrency exchanges and has indicated its support for ‘normal’ cryptocurrency trading. The FSC seems to be working on a comprehensive regulatory scheme that would be applicable on digital currency exchanges, which may provide some relief to traders and users alike.

---

<sup>291</sup> Financial Services Commission (2018), *Financial Measures to Curb Speculation in Cryptocurrency Trading*. Available at: <https://www.fsc.go.kr/downManager?bbsid=BBS0048&no=123388> [Last accessed: 26 February 2019].

<sup>292</sup> Gibbs, S. (2018) Bitcoin drops \$2,000 in value as South Korea announces planned trading ban. *The Guardian*. Available at: <https://www.theguardian.com/technology/2018/jan/11/bitcoin-drops-value-south-korea-trading-ban-cryptocurrencies-tax-gambling> [Last accessed: 14 February 2019].

## Switzerland

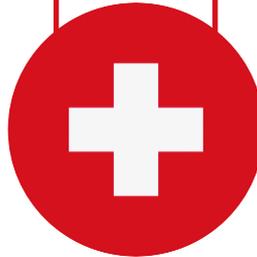


### RESPONSIBLE REGULATORY AUTHORITIES

Financial Market Authority (FINMA)

### RELEVANT REGULATIONS

AML Act  
Banking Act  
Financial Market Infrastructure Act (FMIA)  
Stock Exchange Act (SESTA)



Date of key guidance issuance [Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs), 2018]: February 16, 2018

### Cryptoasset Definition and Terminology

Swiss law at present does not offer a definition or taxonomy of cryptoassets, although FINMA has offered its own classification (see below). The Swiss Federal Government previously used the term *virtual currency* in a 2014 Report of the Federal Council, defined as:

*a digital representation of value which can be traded on the Internet and although it takes on the role of money - it can be used as a means of payment for real goods and services.*<sup>293</sup>

The 2014 Report excludes the possibility of considering virtual currencies as legal tender.<sup>294</sup> The term virtual currencies also appears, without a definition, in the *Anti Money Laundering Ordinance 2016*<sup>295</sup> (AMLO) and in FINMA's *Anti-Money Laundering Ordinance* (FINMA-AMLO).<sup>296</sup>

### Classification of tokens

In the absence of a token classification by Swiss lawmakers, FINMA issued its own token taxonomy in its 2018 Guidelines. FINMA distinguishes between three types of tokens:<sup>297</sup>

- **Payment tokens (or cryptocurrencies):** tokens “intended to be used, now or in the future, as a means of payment for acquiring goods or services or as a means of money or value transfer”, which “give rise to no claims on their issuer”;
- **Utility tokens:** tokens intended to provide digital access to an application or service through a blockchain-based infrastructure;

<sup>293</sup> The Federal Council (2014) *Federal Council report on virtual currencies in response to the Schwaab (13.3687) and Weibel (13.4070) postulates*. Available here: <https://www.news.admin.ch/NSBSubscriber/message/attachments/35355.pdf> [Last accessed: 08 January 2019].

<sup>294</sup> Idem.

<sup>295</sup> Art. 4 in The Federal Council (2015) *Verordnung über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung, Geldwäschereiverordnung, GwV*. Available at: <https://www.admin.ch/opc/de/classified-compilation/20152238/index.html> [Last accessed: 23 January 2019].

<sup>296</sup> Art. 2 in The Federal Council (2015) *Verordnung über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung, Geldwäschereiverordnung, GwV*. Available at: <https://www.admin.ch/opc/de/classified-compilation/20152238/index.html> [Last accessed: 23 January 2019].

<sup>297</sup> Financial Market Authority (2018) *Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs)*. Available at: <https://www.finma.ch/en/~media/finma/dokumente/dokumentencenter/myfinma/1bewilligung/fintech/wegleitung-ico.pdf?la=en> [Last accessed: 08 January 2019].

- **Asset tokens:** tokens that represent “assets such as a debt or equity claim on the issuer”, which are “similar to equities, bonds or derivatives” from an economic perspective. Tokens enabling “physical assets to be traded on the blockchain” are also included in this category.

These three categories are not mutually exclusive and FINMA recognises the possibility of hybrid tokens (e.g. asset tokens that are also payment tokens). In such cases, the legal requirements are cumulative.

### Relevant Regulations

FINMA’s 2017 Guidance on the *Regulatory Treatment of Initial Coin Offerings* listed four main areas of regulatory concern for ICOs, namely AML regulations, banking laws, securities regulation and collective investment schemes laws.<sup>298</sup> The list is non-exhaustive and ICO issuers bear the responsibility to undertake their own legal assessment.

*FINMA issued its own token taxonomy in its 2018 Guidelines, distinguishing between payment, utility and asset tokens.<sup>299</sup> Hybrid tokens are possible (e.g. utility tokens that are also securities tokens), and legal requirements are cumulative. Such Guidelines furthermore specify how market participants can initiate an enquiry with FINMA on an ICO’s regulatory framework.<sup>300</sup>*

FINMA’s 2018 Guidelines clarify that the following laws may apply to ICOs:

- **ICO of payment token:** considered a means of payment subject to the *Anti-Money Laundering Act* (AMLA); however, securities laws (financial market laws) may apply for pre-financing and pre-sale issuance of such tokens;
- **ICO of utility token:** not considered a security if it concerns exclusively a functioning utility token; but will be considered a security if it also or only has an investment purpose. Will generally not be considered a means of payment subject to AMLA.
- **ICO of asset token:** considered a security; typically not considered a means of payment subject to AMLA.

### Applicability of Securities Laws

Asset tokens (and some hybrids) fall under the definition of securities in the *Swiss Financial Market Infrastructure Act* (FMIA) if it:

- represents an uncertificated security<sup>301</sup> (i.e. “rights issued or established in large numbers and are generically identical”) and the “token is standardised and suitable for mass trading”;<sup>302</sup>
- represents a derivative and the “token is standardised and suitable for mass trading”; or
- represents a claim to acquire a token in the future in the case of the pre-financing and pre-sale phases of an ICO and the “token is standardised and suitable for mass standardised trading”.

Suitability for mass standardised trading means securities that are “publicly offered for sale in the same structure and denomination or are placed with more than 20 clients, insofar as they have not been

<sup>298</sup> Financial Market Authority (2017) *Regulatory treatment of initial coin offerings (ICOs)*. Available at: <https://www.finma.ch/en/~media/finma/dokumente/dokumentencenter/myfinma/4dokumentation/finma-aufsichtsmittelungen/20170929-finma-aufsichtsmittelung-04-2017.pdf> [Last accessed: 08 January 2019].

<sup>299</sup> Financial Market Authority (2018) *Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs)*. Available at: <https://www.finma.ch/en/~media/finma/dokumente/dokumentencenter/myfinma/1bewilligung/fintech/wegleitung-ico.pdf?la=en> [Last accessed: 08 January 2019].

<sup>300</sup> Idem.

<sup>301</sup> Cryptoassets will rarely be certificated securities, which require a physical deed. Intermediated securities, as the name suggests, involve an intermediary or custodian, which should be a licensed entity. Most asset tokens will be uncertificated securities. See p.4 in Financial Market Authority (2018) *Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs)*. Available at: <https://www.finma.ch/en/~media/finma/dokumente/dokumentencenter/myfinma/1bewilligung/fintech/wegleitung-ico.pdf?la=en> [Last accessed: 08 January 2019].

<sup>302</sup> Token suitable for mass standardised trading are “publicly offered for sale in the same structure and denomination or are placed with more than 20 clients, insofar as they have not been created especially for individual counterparties” (Art. 2 para. 1 FMIA).

created especially for individual counterparties”.<sup>303</sup> If an asset token qualifies as an uncertificated security under FMIA, the book-entry of such securities remains unregulated. ICOs of asset tokens that “are analogous to equities or bonds” may require a prospectus, although such prospectus does not currently need to be filed with Swiss authorities (this will change once the Financial Services Act comes into force).<sup>304</sup>

However, though uncertificated securities qualify as securities under FMIA, book entry of self-issued uncertificated securities remains unregulated. The remaining two categories are regulated under the Stock Exchange Ordinance (SESTO). Anyone offering such services has to comply with several licensing requirements, such as the description of the business area, the implementation of an internal control system, minimal capital, security deposit and the registration in the commercial register. Additionally, “the issuing of tokens, analogous to equities or bonds can also result in prospectus requirements under the Swiss Code of Obligations”.<sup>305</sup>

An asset token that qualifies as a derivative and is offered to the public on the primary market is, however, regulated under the Stock Exchange Ordinance (SESTO) and subject to a licensing requirement if done on a professional basis. Moreover, an intermediary “underwriting and offering tokens constituting securities of third parties publicly on the primary market”<sup>306</sup> is a licensed activity if done on a professional basis.

If the issuance of tokens comes with liabilities (e.g., the issuer promises to return capital with a guaranteed return), the company raising the funds must obtain a license (unless one of the exceptions apply).<sup>307</sup>

### **Applicability of Banking Laws**

Funds received through an ICO typically will not be considered deposits under the *Swiss Banking Act*, as there typically are no “claims for repayment on the ICO organiser”.<sup>308</sup> If, however, the funds obtained through an ICO qualify as debt capital (e.g. “promises to return capital with a guaranteed return”), they would be deposits covered by the *Banking Act*. A license may be required in that case, unless one of the exceptions apply. One exemption is the regulatory sandbox for ICO issuers that accept public funds not exceeding CHF 1 million (approximately US \$1.05 million). Funds obtained from investors after a prospectus subject to Swiss law are also not considered deposits under the *Banking Act*.

FINMA undertook enforcement actions against the issuers of a “fake cryptocurrency” that collected deposits without holding a banking license.<sup>309</sup>

### **Applicability of Collective Investment Laws**

If the funds obtained through an ICO are managed by a third party, the *Collective Investment Schemes Act* may apply.<sup>310</sup>

<sup>303</sup> Art. 2 para 1 of Financial Market Infrastructure Act.

<sup>304</sup> The Financial Services Act (FinSA) will enter into force on 1 January 2020. For further information see: <https://www.efd.admin.ch/efd/en/home/themen/wirtschaft--waehrung--finanzplatz/finanzmarktpolitik/fidleg-finig/fb-fidleg-finig.html> [Last accessed: 23 January 2019].

<sup>305</sup> Art. 3 para. 2 SESTO.

<sup>306</sup> P. 5 in Financial Market Authority (2018) *Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs)*. Available at: <https://www.finma.ch/en/~media/finma/dokumente/dokumentencenter/myfinma/1bewilligung/fintech/wegleitung-ico.pdf?la=en> [Last accessed: 08 January 2019].

<sup>307</sup> Idem.

<sup>308</sup> P. 6 in Financial Market Authority (2018) *Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs)*. Available at: <https://www.finma.ch/en/~media/finma/dokumente/dokumentencenter/myfinma/1bewilligung/fintech/wegleitung-ico.pdf?la=en> [Last accessed: 08 January 2019].

<sup>309</sup> FINMA (2017), *FINMA closes down coin providers and issues warning about fake cryptocurrencies*. Available at: <https://www.finma.ch/en/news/2017/09/20170919-mm-coin-anbieter/> [Last accessed: 23 January 2019].

<sup>310</sup> P.6 in Financial Market Authority (2018) *Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs)*. Available at: <https://www.finma.ch/en/~media/finma/dokumente/dokumentencenter/myfinma/1bewilligung/fintech/wegleitung-ico.pdf?la=en> [Last accessed: 08 January 2019].

### Applicability of AML Regulations

The *Anti-Money Laundering Act* (AMLA) applies to “anyone who provides payment services or who issues or manages a means of payment” and is therefore considered a financial intermediary.<sup>311</sup> As long as a payment token can “technically”<sup>312</sup> be transferred on a blockchain, whether at the time of the ICO or later, it will be a means of payment under AMLA. AMLA does not apply to utility tokens if “the main reason for issuing the tokens is to provide access rights to a non-financial application of blockchain technology”.<sup>313</sup>

Cryptoasset exchanges (crypto-to-crypto or fiat-to-crypto) are subject to AMLA, as are custody wallet providers.<sup>314</sup>

Due diligence requirements under AMLA can be met “by having the funds accepted via a financial intermediary who is already subject to the AMLA in Switzerland”. This allows cryptoasset providers to rely on a third party for the due diligence requirements under AMLA.

### Future Outlook

The Swiss State Secretariat for International Finance established a working group on blockchain and ICOs.<sup>315</sup> The working group collaborates with FINMA, industry players, and the Federal Ministry of Justice to develop a legal framework for ICOs and blockchain-related activities. The working group shared its findings with the Swiss Government, which discussed its conclusions and released a report in December 2018 (DLT Legal Framework Report).<sup>316</sup> The *DLT Legal Framework Report* confirms FINMA’s classification for financial market laws purposes (payment/utility/asset tokens). It suggests that “tokens which primarily represent a value within the blockchain context”, such as Bitcoin, are “purely factual intangible assets” on which civil law currently imposes no constraints for their transfer (as opposed to the transfer of tokens classified as securities). It also assesses the legal status of cryptoassets under other areas of law, such as insolvency law. The Swiss Federal Council concluded that “there is no need for fundamental adjustments to the Swiss legal framework, but that there is still a need for specific adjustments”.<sup>317</sup> One proposed adjustment is “the creation of a new authorisation category for infrastructure providers in the blockchain/DLT area” for financial market infrastructure law.<sup>318</sup> The Report does not propose fundamental changes to AMLA. It proposes a legislative clarification that decentralised trading platforms are subject to AMLA (except if they are fully decentralised platforms “that do not have the power to dispose of assets and merely connect supply with demand”).<sup>319</sup> It does not intend to bring non-custodial wallet providers under AMLA at this point, instead opting to await FATF guidance on this issue.

To prepare for the proposed adjustments, the Council tasked the Federal Department of Finance and the Federal Department of Justice and Police to draft a consultation in early 2019 on a variety of legal issues (including on civil, insolvency, banking, AML and financial market law). Whatever the eventual changes to the regulatory framework may be, it is clear the Swiss Government wishes to safeguard its position as a cryptoasset hub.

---

<sup>311</sup> Idem.

<sup>312</sup> Idem.

<sup>313</sup> Idem.

<sup>314</sup> Idem.

<sup>315</sup> The Federal Council (2018) *Blockchain/ICO Working Group Established*. Available at: <https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-69539.html> [Last accessed: 23 January 2019].

<sup>316</sup> The Federal Council (2018) *Legal framework for distributed ledger technology and blockchain in Switzerland - An overview with a focus on the financial sector*. Available at <https://www.sif.admin.ch/sif/en/home/dokumentation/medienmitteilungen/medienmitteilungen.msg-id-73398.html> [Last accessed: 23 January 2019].

<sup>317</sup> Idem.

<sup>318</sup> Idem.

<sup>319</sup> Idem.

## United States of America



**Date of guidance issuance [FinCen Guidance]:** March 18, 2013

Regulatory competence for cryptoasset regulation rests with both federal and state authorities. State-level policies on cryptoassets diverge widely, adding to the regulatory uncertainty for cryptoasset service providers. This overview only assesses cryptoasset regulation at the federal level.

### Cryptoasset Definition and Terminology

Cryptoassets have not yet been defined by U.S. federal lawmakers. Nevertheless, federal regulators such as the CFTC and FinCEN have formulated their own definitions.

The CFTC initially relied on the Internal Revenue Service (IRS) definition to provide “a general idea” of what was meant by *virtual currency*:

*a digital representation of value that functions as a medium of exchange, a unit of account, and/or a store of value” that does not have legal tender status.*<sup>320</sup>

The definition was also used by the CFTC in court filings<sup>321</sup> and other documents.<sup>322</sup>

The U.S. Department of the Treasury’s Financial Crimes Enforcement Network (FinCEN) issued Guidance in 2013 that described a *virtual currency* as:

*a medium of exchange that operates like a currency in some environments, but does not have all the attributes of real currency. In particular, virtual currency does not have legal tender status in any jurisdiction.*<sup>323</sup>

<sup>320</sup> Commodity Futures Trading Commission (2017) *A CFTC Primer on Virtual Currencies*. Available at: <https://www.cftc.gov/LabCFTC/Primers/index.htm> [Last accessed: 01 February 2019].

<sup>321</sup> CFTC v. Gelfman Blueprint, Inc. and Nicholas Gelfman (2017), CFTC v. My Big Coin Pay, Inc., et al. (2018). Note that the CFTC’s definition in these complaints added that a virtual currency “does not have legal tender status in any jurisdiction” (not limited to the US).

<sup>322</sup> Commodity Futures Trading Commission (2018) *An Introduction to Virtual Currency*. Available at: [https://www.cftc.gov/sites/default/files/idc/groups/public/@customerprotection/documents/file/oceo\\_aivc0218.pdf](https://www.cftc.gov/sites/default/files/idc/groups/public/@customerprotection/documents/file/oceo_aivc0218.pdf) [Last accessed: 01 February 2019].

<sup>323</sup> Financial Crime Enforcement Network (2013) *Application of FinCEN’s Regulations to Persons Administering, Exchanging, or Using Virtual Currencies” (FIN-2013-G001)*. Available at <https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering> [Last accessed: 31 January 2019].

## Relevant Regulations

### Applicability of Securities Law

The SEC has repeatedly stated that cryptoassets may qualify as securities and that ICOs may consequently need to comply with securities laws, in particular the *1933 Securities Act*.<sup>324</sup> The *Howey* test formulated by the U.S. Supreme Court is used by the SEC to decide whether an asset, including cryptoassets, are a “security” in the sense of securities law.<sup>325</sup>

The SEC’s chairman initially stated that every ICO examined should be considered a security, although later statements suggested neither Bitcoin nor Ether should currently be considered securities.<sup>326</sup> The SEC has issued several warnings about the risks of cryptoasset investments, in particular ICOs, and has taken an active approach in bringing enforcement actions against cryptoasset entities.<sup>327</sup> The first and perhaps most well-known SEC action in the crypto-space was against The DAO, qualifying DAO tokens as securities.<sup>328</sup> Whether or not a cryptoasset is a security will ultimately be decided by the courts, which have already reviewed a number of cases involving cryptoassets.<sup>329</sup>

The SEC has also received a number of applications for Bitcoin-based exchange-traded funds (ETFs), although so far none have been approved.<sup>330</sup> The SEC chairman has cited concerns around the lack of market surveillance and the risk of price manipulation.<sup>331</sup>

The Financial Industry Regulatory Authority (FINRA) filed its first disciplinary complaint on cryptoassets in September 2018. FINRA, overseen by the SEC, can impose remedies such as a fine, censure, suspension or bar from the securities industry on broker-dealers dealing in cryptoassets. In its disciplinary complaint, FINRA alleged securities laws violations by the president, director and sole shareholder of a “worthless” public company issuing cryptoassets backed by the company’s equity.<sup>332</sup>

### Applicability of AML Law

FinCEN issued guidance in 2013 stating that “virtual currency exchangers and administrators are money transmitters and must comply with the *Bank Secrecy Act* (BSA) and its implementing regulations.”<sup>333</sup>

Cryptoasset service providers have to register with FinCEN as a money service business (MSB) and comply with AML/KYC due diligence and reporting requirements. This includes ICOs and cryptoasset exchanges.<sup>334</sup> FinCEN will assess such activities on a case-to-case basis.<sup>335</sup>

<sup>324</sup> Securities and Exchange Commission (2018) Available at: <https://www.sec.gov/ICO> [Accessed: 01 February 2019].

<sup>325</sup> This includes stocks, bonds and the catch-all term “investment contract”.

<sup>326</sup> U.S. Securities and Exchange Commission (2018) *Digital Asset Transactions: When Howey Met Gary (Plastic)*. Available at <https://www.sec.gov/news/speech/speech-hinman-061418> [Last accessed: 31 January 2019].

<sup>327</sup> For a list of SEC enforcement actions on ICOs deemed see <https://www.sec.gov/spotlight/cybersecurity-enforcement-actions>

<sup>328</sup> The SEC ultimately decided not to bring enforcement actions but to publish its investigative report as a warning to the industry and the public. SEC (2017) *Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO*. Available at: <https://www.sec.gov/news/press-release/2017-131> [Last accessed: 31 January 2019].

<sup>329</sup> See for instance *US v. Zaslavskiy*, 2018 WL 4346339 (EDNY Sept. 11, 2018). See also the class action lawsuit brought by a Ripple investor against Ripple Labs, *Coffey v. Ripple Labs Inc.* (2018), N.D. Cal.

<sup>330</sup> For instance, on January 31, 2019, CBOE resubmitted a joint application with VanEck and SolidX for a US Bitcoin-based ETF (CBOE BZX), after withdrawing an earlier application. Nine applications have been rejected by the SEC so far. U.S. Securities and Exchange Commission (2017) *Release No. 34-80206*. Available at: <https://www.sec.gov/rules/sro/batsbzx/2017/34-80206.pdf> and U.S. Securities and Exchange Commission (2018) *Release No. 34-83723*. Available at: [https://www.sec.gov/rules/other/2018/34-83723.pdf?mod=article\\_inline](https://www.sec.gov/rules/other/2018/34-83723.pdf?mod=article_inline) [Last accessed: 01 February 2019].

<sup>331</sup> CNBC (2018) *SEC’s Clayton needs to see key upgrades in cryptocurrency markets before approving a bitcoin ETF*. Available at: <https://www.cnbc.com/2018/11/27/sec-wants-key-upgrades-in-crypto-markets-before-approving-bitcoin-etf.html> [Last accessed: 01 February 2019].

<sup>332</sup> Financial Industry Regulatory Authority Office of Hearing Officers (2018) *Disciplinary Proceeding No. 2016049307801*. Available at <https://www.finra.org/newsroom/2018/finra-charges-broker-fraud-and-unlawful-distribution-unregistered-cryptocurrency> [Last accessed: 28 January 2019].

<sup>333</sup> See footnote 307.

<sup>334</sup> *Idem*.

<sup>335</sup> *Idem*.

In August 2018, the agency indicated that it receives over 1,500 suspicious activity reports on cryptoassets per month.<sup>336</sup>

### **Applicability of Other Existing Regulations**

In 2014, the CFTC declared virtual currencies to be commodities, bringing cryptoasset derivatives such as futures or options under its perimeter.<sup>337</sup> The CFTC has brought a number of enforcement actions, imposing a fine and a cease-and-desist order.<sup>338</sup> Case laws has confirmed the CFTC’s power to regulate cryptoassets as commodities under the *Commodities Exchange Act*.<sup>339</sup>

The Treasury Department’s Office of Foreign Assets Control (OFAC) has made clear that cryptoasset transactions should not be used to circumvent US sanctions law. After the Venezuelan Government launched the Petro, OFAC prohibited US persons from transacting in the country’s cryptoasset.<sup>340</sup> OFAC also published the bitcoin addresses of two Iranian-based individuals considered to have violated US sanctions against Iran, for the first time “publicly attributing digital currency addresses to designated individuals”.<sup>341</sup>

### **Future Outlook**

In December 2018, two bipartisan bills were introduced on cryptoassets. The proposed *Virtual Currency Consumer Protection Act*<sup>342</sup> asks the CFTC to analyse how cryptoasset prices may be exposed to price manipulation and propose regulatory changes to increase its monitoring capacity to prevent such manipulation. The second bill, the *Virtual Currency Market and Regulatory Competitiveness Act*<sup>343</sup> requests the CFTC to do a comparative analysis on cryptoasset regulation in other jurisdictions and to recommend regulatory changes that can increase the US competitive position in the industry.

In December 2018, the CFTC published a request for public comments on Ethereum and ether. The public consultation invites feedback “on a range of questions related to the underlying technology, opportunities, risks, mechanics, use cases, and markets, related to Ether and the Ethereum Network.”<sup>344</sup> This public consultation is meant to help the CFTC assess Ether’s “potentially unique attributes relative to Bitcoin”. The list of 42 comments have been made available on the CFTC’s website.<sup>345</sup>

<sup>336</sup> Financial Crime Enforcement Network (2018) *Remarks of FinCEN Director Kenneth A. Blanco, delivered at the 2018 Chicago-Kent Block (Legal) Tech Conference*. Available at <https://www.fincen.gov/news/speeches/prepared-remarks-fincen-director-kenneth-blanco-delivered-2018-chicago-kent-block> [Last accessed: 31 January 2019].

<sup>337</sup> The CFTC’s competence in cryptoassets also extends to cases where there is fraud or manipulation involving a virtual currency traded in interstate commerce. Commodity Futures Trading Commission (2018) *CFTC Backgrounder on Oversight of and Approach To Virtual Currency Futures Markets*. Available at: <https://www.cftc.gov/Bitcoin/index.htm>. [Last accessed: 31 January 2019].

<sup>338</sup> See e.g. Commodity Futures Trading Commission (2016) *Release Number 7380-16*. Available at: <https://www.cftc.gov/PressRoom/PressReleases/pr7380-16> [Last accessed: 01 February]

<sup>339</sup> Commodity Futures Trading Commission (2018) *Memorandum & Order 18-CV-361*. Available at: <https://www.cftc.gov/sites/default/files/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfcoindroporder030618.pdf> [Last accessed: 01 February 2019].

<sup>340</sup> U.S. Department of Treasury (2018) *OFAC, Issuance of additional frequently asked questions on Venezuela*. Available at: [https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq\\_other.aspx#650](https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_other.aspx#650) [Accessed: 20 February 2019].

<sup>341</sup> U.S. Department of Treasury (2018) *Treasury designates Iran-based financial facilitators of malicious cyber activity and for the first time identifies associated digital currency addresses*. Available at: <https://home.treasury.gov/news/press-releases/sm556> [Last accessed: 20 February 2019]

<sup>342</sup> U.S. Congress (2018) H.R.7224. Available at <https://www.congress.gov/bill/115th-congress/house-bill/7224/text?format=txt> [Last accessed: 01 February 2019].

<sup>343</sup> U.S. Congress (2018) H.R.7225. Available at <https://www.congress.gov/bill/115th-congress/house-bill/7225> [Last accessed: 01 February 2019].

<sup>344</sup> Commodity Futures Trading Commission (2018) *Request for Input on Crypto-asset Mechanics and Markets*. Available at: <https://www.cftc.gov/sites/default/files/2018-12/federalregister121118.pdf> [Last accessed: 01 February 2019].

<sup>345</sup> Commodity Futures Trading Commission (2019) *Comments for orders and other announcements 83 FR 54563*. Available at: <https://comments.cftc.gov/PublicComments/CommentList.aspx?id=2941> [Last accessed: 21 February 2019].

In February 2019, a SEC Commissioner said SEC “The staff is working on some supplemental guidance to help people think through whether their crypto-fundraising efforts fall under the securities laws.”<sup>346</sup>

A number of cryptoasset companies established the Association for Digital Asset Market (ADAM) to draft a code of conduct for the digital asset market.<sup>347</sup> It plans to release a first version of its Code of Conduct in 2019.

---

<sup>346</sup> Speech by Securities and Exchange Commission Commissioner Pierce (2019), *Regulation: A view from inside the machine*. Available at: <https://www.sec.gov/news/speech/peirce-regulation-view-inside-machine> [Last accessed: 28 February 2019].

<sup>347</sup> See The Association for Digital Asset Markets. Available at: <http://www.theadam.io/> [Last accessed: April 13, 2019].

# APPENDIX A: REVIEW OF REGULATORY CRYPTOASSET DEFINITIONS

Jurisdiction	Terminology	Definition
Abu Dhabi	Crypto Asset	A <b>digital representation</b> of value that can be digitally traded and functions as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but does <b>not have legal tender</b> status in any jurisdiction. A Crypto Asset is (a) neither issued nor guaranteed by any jurisdiction, and fulfils the above functions only by agreement within the community of users of the Crypto Asset; and (b) distinguished from Fiat Currency and E-money.
Australia	Digital Currency	(a) a <b>digital representation</b> of value that: (i) functions as a medium of exchange, a store of economic value, or a unit of account; and (ii) is not issued by or under the authority of a government body; and (iii) is interchangeable with money (including through the crediting of an account) and may be used as consideration for the supply of goods or services; and (iv) is generally available to members of the public without any restriction on its use as consideration; or  (b) a means of exchange or digital process or crediting declared to be digital currency by the AML/CFT Rules.
Bermuda	Digital Asset	Anything that exists in binary format and comes with the right to use it and includes a <b>digital representation of value</b> that— is used as a medium of exchange, unit of account, or store of value and is <b>not legal tender</b> , whether or not denominated in legal tender; is intended to represent assets such as debt or equity in the promoter; is otherwise intended to represent any assets or rights associated with such assets; or is intended to provide access to an application or service or product by means of distributed ledger technology; but does not include— a transaction in which a person grants value as part of an affinity or rewards program, which value cannot be taken from or exchanged with the person for legal tender, bank credit or any digital asset; or a digital representation of value issued by or on behalf of the publisher and used within an online game, game platform, or family of games sold by the same publisher or offered on the same game platform.
Canada	Virtual Currency	(a) A <b>digital</b> currency that is <b>not a fiat currency</b> and that can be readily exchanged for funds or for another virtual currency; or (b) information that enables a person or entity to have access to a digital currency referred to in paragraph (a).
Estonia	Virtual Currency	A value represented in the <b>digital form</b> , which is digitally transferable, preservable or tradable and which natural persons or legal persons accept as a payment instrument, but that is <b>not the legal tender</b> of any country or funds.
European Union	Cryptoasset (1) and Virtual currency (2)	(1) A type of private asset that depends primarily on cryptography and Distributed Ledger Technology (DLT) or similar technology as part of their perceived or inherent value. Unless otherwise stated, ESMA uses the term to refer to both so-called 'virtual currencies' and 'digital tokens'. Crypto-asset additionally means an asset that is <b>not issued by a central bank</b> . (2) A <b>digital representation of value</b> that is <b>neither issued nor guaranteed by a central bank or public authority</b> and does not have the legal status of currency or money. In particular, the absence of regulation generates a risk because no guarantees are expressly associated with the respective operations. (EBA) A digital representation of value that is neither issued by a central bank or public authority nor necessarily attached to a fiat currency, but is used by natural or legal persons as a means of exchange and can be transferred, stored or traded electronically.

France	Token (1) and Digital asset (2)	any intangible asset representing, in digital form, one or more rights, which may be issued, registered, retained or transferred by means of a distributed electronic ledger that identifies, directly or indirectly, the owner of such asset. any digital representation of value which is not issued by a central bank or a public authority, not necessarily linked to a legal tender, and does not possess the legal status of currency, but which is accepted by any natural and legal person as a means of exchanges and can be transferred, stored, or exchanged electronically.
Germany	Crypto-token (1) and (2) Crypto-asset	(1) <b>Digital representations</b> of value in a blockchain data structure (2) (i) were not 'e-money' as defined in the E-Money Directive Directive 2009/110/EC, and (ii) were to be considered as 'units of account'.
Gibraltar	<i>Does not contain a definition of cryptoasset, but defines DLT as a whole.</i>	
Hong Kong	Virtual Asset	<i>A virtual asset is a digital representation of value, which is also known as 'cryptocurrency', 'crypto-asset' or 'digital token'. The polymorphous and evolving features of virtual assets mean that they may be, or claim to be, a means of payment, may confer a right to present or future earnings or enable a token holder to access a product or service, or a combination of any of these functions.</i>
India	Virtual Currency	<i>No official definition available</i>
Israel	Virtual Currency	Financial asset
Japan	Virtual Currency	The Payment Services Act distinguishes between two types of virtual currencies. The first category of virtual currencies are primarily defined as that which is "available as a means of payment", "able to be paid to an unspecified number of people for purchase of goods, lease of goods or as consideration for services rendered", " <b>electronically recorded</b> " and " <b>not denominated in fiat currency</b> ". The second category consists of those cryptoassets that can be mutually exchanged with the first category with unspecified persons and can be transferred by means of electronic data processing systems.
Malta	DLT Asset	(i) virtual tokens; (ii) virtual financial assets; (iii) electronic money; or (iv) financial instruments, that are intrinsically dependent on or utilises Distributed Ledger Technology. <ul style="list-style-type: none"> <li>• Electronic money;</li> <li>• Financial instruments;</li> <li>• Virtual tokens: a form of <b>digital medium</b> recordation whose utility, value or application is restricted solely to the acquisition of goods or services, either solely within the DLT platform or in relation to which it was issued or within a limited network of DLT platforms: provided that the term "DLT platform" referred to in this definition shall exclude DLT exchanges: and provided further that a virtual token which is or may be converted into another DLT asset type shall be treated as the DLT asset type into which it is or may be converted. In essence, this definition captures pure utility tokens who, akin to 'vouchers';</li> <li>• Virtual financial assets: any form of digital medium recordation that is used as a digital medium of exchange, unit of account, or store of value and that is not: (a) electronic money; (b) a financial instrument; or (c) a virtual token.</li> </ul>
Mexico	Virtual Asset	A <b>representation of value electronically registered</b> and used among the public as a payment instrument in any type of legal transaction and which can only be transferred through electronic means.
People's Republic of China	Virtual Currency	<i>No official definition available</i>
Russia	Cryptocurrency	A type of digital financial asset created and accounted for in the distributed registry of digital transactions by participants in this registry in accordance with the rules of maintaining the registry of digital transactions.

<b>Singapore</b>	Virtual Currency	Any <b>digital representation of value</b> (other than an excluded digital representation of value) that is expressed as a unit; not denominated in any currency; not pegged by its issuer to any currency; is or is intended to be, a medium of exchange accepted by the public, or a section of the public; as payment for goods or services or for the discharge of a debt; can be transferred, stored or traded electronically; and satisfies such other characteristics as the MAS may prescribe.
<b>South Korea</b>	Virtual Currency	<b>Electronically transferable</b> token or information regarding such token, which a trade counterparty may recognise as a <b>means of exchange or a storage of value</b>
<b>Switzerland</b>	Virtual Currency	A <b>digital representation of value</b> which can be traded on the Internet and although it takes on the role of money - it can be used as a means of payment for real goods and services.
<b>Thailand</b>	Digital Asset	Encompasses cryptocurrency (1) and digital token (2): (1) an <b>electronic</b> 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. (2) an electronic data unit created on an electronic system or network for the purpose of: (a) specifying the right of a person to participate in an investment in any project or business; (b) 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.
<b>United Kingdom</b>	Cryptoasset	A cryptographically secured <b>digital representation of value</b> or contractual rights that uses some type of DLT and can be transferred, stored or traded electronically.
<b>USA</b>	Virtual Currency	A <b>digital representation of value</b> that functions as a medium of exchange, a unit of account, and/or a store of value.

# APPENDIX B: AUTHORISATION IN SELECTED JURISDICTIONS

				Distribution	Exchange	Storage	Payments
 Abu Dhabi	Securities law	Name of authorisation	Several licenses depending on activity				
		Mandated authority	FSRA				
	Bespoke response	Name of authorisation	Operating a Crypto Asset Business (OCAB) License				
		Mandated authority	FSRA				
 Australia	Securities law	Name of authorisation	Australian Financial Service (AFS) License				
		Mandated authority	ASIC				
	AML law	Name of authorisation	Digital Currency Exchange Provider				
		Mandated authority	AUSTRAC				
 Bermuda	Retrofitted regulation	Name of authorisation	Approval and Registration				
		Mandated authority	Ministry of Finance				
	Bespoke response	Name of authorisation	Digital Asset Business License				
		Mandated authority	BMA				
 Canada	Securities law	Name of authorisation	Several licenses depending on activity				
		Mandated authority	CAS				
	AML law	Name of authorisation	Money Service Business Registration				
		Mandated authority	FINTRAC				
 Estonia	Securities law	Name of authorisation	Several licenses depending on activity				
		Mandated authority	EFSA				
	AML law	Name of authorisation	License				
		Mandated authority	Estonian FIU				

				Distribution	Exchange	Storage	Payments
 <b>European Union</b>	Securities law	Name of authorisation	Several licenses depending on activity				
		Mandated authority	ESMA				
	AML law	Name of authorisation	Obligated Entities Registration				
		Mandated authority	National AML Regulator				
 <b>France</b>	Securities law	Name of authorisation	Several licenses depending on activity				
		Mandated authority	AMF				
	Bespoke response	Name of authorisation	Optional Visa				
		Mandated authority	AMF				
 <b>Germany</b>	Securities law	Name of authorisation	Several licenses depending on activity				
		Mandated authority	BaFin				
	Other existing regulations	Name of authorisation	Written authorisation for Financial Services				
		Mandated authority	BaFin				
 <b>Gibraltar</b>	Securities law	Name of authorisation	Several licenses depending on activity				
		Mandated authority	GFSC				
	Bespoke response	Name of authorisation	DLT Provider License				
		Mandated authority	GFSC				
 <b>Hong Kong</b>	Securities law	Name of authorisation	Several licenses depending on activity				
		Mandated authority	RBI				
	AML law	Name of authorisation	Registration				
		Mandated authority	Enforcement Directorate (ED)				
 <b>India</b>	Other existing regulations	Name of authorisation	Several licenses depending on activity				
		Mandated authority	RBI				
	AML law	Name of authorisation	Registration				
		Mandated authority	Enforcement Directorate (ED)				

				Distribution	Exchange	Storage	Payments
 <b>Israel</b>	Securities law	Name of authorisation	Several licenses depending on activity				
		Mandated authority	ISA				
	Bespoke response	Name of authorisation	Financial Asset Services License (basic or expanded)				
		Mandated authority	Ministry of Finance				
 <b>Japan</b>	Securities law	Name of authorisation	Several licenses depending on activity				
		Mandated authority	FSA				
	AML law	Name of authorisation	Specified Business Operator				
		Mandated authority	FSA				
	Retrofitted regulation	Name of authorisation	Virtual Currency Exchange Registration				
		Mandated authority	JVCEA and FSA				
 <b>Malta</b>	Securities law	Name of authorisation	Several licenses depending on activity				
		Mandated authority	MFSA				
	Bespoke response	Name of authorisation	Virtual Financial Asset (VFA) Service Provider License				
		Mandated authority	MDIA, MFSA				
 <b>Mexico</b>	Bespoke response	Name of authorisation	Financial Technology Institution License				
		Mandated authority	CNBV and Central Bank of Mexico				
 <b>China</b>	AML law	Name of authorisation	Registration				
		Mandated authority	State Council				
 <b>Russia</b>	Bespoke response	Name of authorisation	Several licenses depending on activity				
		Mandated authority	Central Bank of Russia				
 <b>Singapore</b>	Securities law	Name of authorisation	Several licenses depending on activity				
		Mandated authority	MAS				
	Bespoke response	Name of authorisation	Payment Institution License				
		Mandated authority	MAS				

				Distribution	Exchange	Storage	Payments
 <b>South Korea</b>	Securities law	Name of authorisation	Several licenses depending on activity				
		Mandated authority	FSC				
	AML law	Name of authorisation	Registration				
		Mandated authority	FIU, FSS				
 <b>Switzerland</b>	Securities law	Name of authorisation	Several licenses depending on activity				
		Mandated authority	FINMA				
	AML law	Name of authorisation	Financial Intermediary License				
		Mandated authority	FINMA				
 <b>Thailand</b>	Bespoke response	Name of authorisation	ICO portal or Digital Asset Business				
		Mandated authority	SEC, Ministry of Finance				
 <b>United Kingdom</b>	Securities law	Name of authorisation	Several licenses depending on activity				
		Mandated authority	FCA				
	Other existing regulations	Name of authorisation	Payment Service Provider or E-money License				
		Mandated authority	FCA, PSR				
	AML law	Name of authorisation	Registration				
		Mandated authority	OPBAS, FCA				
 <b>United States</b>	Securities law	Name of authorisation	Several licenses depending on activity				
		Mandated authority	SEC				
	Other existing regulations	Name of authorisation	Registration				
		Mandated authority	CFTC, FTC, IRS				
	AML law	Name of authorisation	Money Service Business (MSB) License				
		Mandated authority	FINCEN				

# APPENDIX C: GLOSSARY

---

**Blockchain:** see *DLT System*.

**Cryptoassets:** umbrella term commonly used to refer to digital tokens issued on a DLT system. There are different views on the boundaries of the definition:

- **Broad view:** encompasses all types of digital tokens issued and transferred via both open and permissionless as well as closed enterprise DLT systems.
- **Intermediate view:** includes all types of digital tokens issued and transferred via permissionless DLT systems with open access and public transaction history. The tokens do not necessarily need to perform an essential function for the underlying network to operate properly.
- **Narrow view:** exclusively refers to digital tokens issued and transferred via open, permissionless DLT systems that play an essential role in the functioning of the underlying distributed ledger or application. There is no formal issuer; instead, a network of nodes creates new units according to a transparent and pre-defined schedule specified by an intangible software protocol. The token is inextricably linked to the underlying network by acting as an indispensable economic coordination mechanism without which the network would cease to function.

**Cryptoasset exchanges:** venues enabling users to buy and sell cryptoassets for other assets. They serve as the on-off ramps to the cryptoasset ecosystem.

- **Centralised:** exchange operator is in full control of order matching, clearing and settlement, and custody.
- **Peer-to-peer (P2P):** non-custodial exchange with DLT-based clearing and settlement. The exchange operator connects buyers with sellers (central “matching”).
- **Decentralised (“DEX”):** trust-minimised exchange that does not require a central operator; all processes are executed directly via the DLT system.

**Cryptoasset custody:** refers to the secure storage of cryptographic keys that are required to unlock and move funds.

- **Custodial:** service provider controls keys and is in full control of customer funds.
- **Non-custodial:** customer controls keys and thus remains in full control; can unilaterally move funds without service provider approval.
- **Hybrid:** setting in which neither the service provider nor the customer can unilaterally move funds; approval of both parties is required to unlock funds.

**Developer:** actor that writes and reviews code that underlies the technological building blocks of a DLT system and its connected system(s). A developer can be professionally employed or participating as volunteer contributor.

**Distributed Ledger Technology (DLT) System:** a system of electronic records that (i) enables a network of independent participants to establish a consensus around (ii) the authoritative ordering of cryptographically-validated (‘signed’) transactions. These records are made (iii) persistent by replicating the data across multiple nodes, and (iv) tamper-evident by linking them by cryptographic hashes. (v) The shared result of the reconciliation/consensus process - the ‘ledger’ - serves as the authoritative version for these records.

There are three different types of DLT systems:

- **Open, public and permissionless:** complex socio-economic consensus systems that rely on a combination of game theory and clever economic incentive design in order to reach agreement over the state of the system. Access is unrestricted and open to anyone.
- **Closed, private and permissioned:** multi-party consensus systems that rely on access control and contractual agreements between known, vetted participants in order to achieve distributed consensus. A gatekeeper is responsible for member onboarding. They are generally deployed in a controlled enterprise environment.
- **Hybrid:** consensus systems that share characteristics of both permissionless and permissioned DLT systems.

**Locus of execution:** refers to the system on which a given process is executed.

- **On-chain:** interactions, actions, and processes that occur directly within the DLT system (e.g. peer-to-peer Bitcoin transaction).
- **Off-chain:** interactions, actions, and processes that occur outside of the DLT system boundaries (e.g. Bitcoin Lightning network transaction).

**Multi-signature:** cryptographic technique that enables the creation of transactions that require a minimum threshold of private keys ( $m$  out of  $n$ , with  $m < n$ ) to sign off. Also colloquially called “multi-sig”, the technique allows the creation of complex custody settings where no party can unilaterally move funds.

**Node:** a network participant that runs a software client designed to communicate with peers over a shared communication channel.

**Over-the-counter (OTC):** OTC desks enable users to engage in bilateral trades outside of formal trading venues in order to avoid moving the market too much.

**Privacy coins:** a type of cryptoassets specifically designed to support specific cryptographic techniques (e.g. zero-knowledge proofs, ring signatures) to enhance user privacy.

**Public key cryptography:** authentication and asymmetric encryption system that uses a pair of mathematically-related keys (public and private). The public key is used to encrypt a message before sending it. Only the corresponding private key can subsequently decrypt the message. In the context of cryptoassets, the public key acts as an identity (e.g. bank account number) whereas the private key can be considered a password to the bank account.

**Record producer:** actor that produces and submits sets of candidate records (e.g. blocks) for potential inclusion into the DLT system’s global ledger. Record producers in open, permissionless DLT systems are often referred to as *miners* or *stakers*, whereas closed and permissioned DLT systems make use of so-called *validators* or *consensus nodes*.

**Stablecoin:** cryptoassets designed to maintain price stability, either in relation to a pegged asset or a basket of goods (“purchasing power”).

- **Asset-backed:** stablecoin backed by collateral in the form of an asset or basket of assets. These can either be (off-chain) conventional assets (e.g. fiat currency, gold), or cryptoassets (on-chain).
- **Algorithmic:** smart contract programmed to regulate issuance and redemption of the stablecoin to match supply and demand, and hence reduce price volatility.

**Token:** cryptographically-secured representation of a set of rights conferred to token holders. Regulators generally classify them into four categories, mainly according to the nature of the rights provided:

- **Payment/exchange tokens** or **cryptocurrencies**: a means of value exchange.
- **Utility tokens**: granting access to a digital platform or service.
- **Security tokens**: an investment instrument.
- **Hybrid tokens**: share characteristics of multiple categories.

**Token creation:** tokens can, in theory, be created by any individual or entity that has been granted access to a given DLT system. There are three major mechanisms to create a token:

- **Pre-mine:** an entity creates all token units in one batch as a one-time event.
- **Continuous mining:** record producers create new units on a continuous and regular basis according to a transparent, pre-specified procedure specified by the protocol that governs the network or application ruleset.
- **Hybrid:** some entity pre-mines a specific proportion of the total final token supply; the remaining token units are then “minted” through continuous mining after network or application launch.

**Token distribution:** once created, a token can be distributed *via* five main channels:

- **Airdrop:** new token units are distributed to holders of an existing other token, generally under specific conditions.
- **Fork:** a new token is created as a result of an incompatible rule change in the underlying DLT system that causes the network to split. Existing token holders receive the new token on a 1-1 basis.
- **Mining:** newly minted units are distributed ad-hoc to record producers that satisfy the necessary conditions specified by the protocol (e.g. find a valid proof-of-work).
- **Pre-sale:** private round offering of pre-mined token units, often at substantial discounts. The network/application may not be operational yet.
- **Initial Coin Offering:** public (or private) offering of pre-mined token units. The network/application may not be operational yet.

