Analysis of Cryptocurrency Regulation:

A Global Perspective

Aston University
BIRMINGHAM UK

THE CYBER SECURITY
INNOVATION RESEARCH CENTRE

Professor Vladlena Benson
Director
Cyber Security Innovation Centre,
Aston Business Social Science College

The Cyber Security Innovation (CSI) Centre at Aston, established in 2020, brings together stakeholders from industry, government and leading cyber security research institutions with the aim to deliver industry-aligned cyber security research outcomes. CSI members include globally-recognised researchers delivering outcomes that have impact and address real-world cyber security challenges through innovative solutions.

The CSI Director, Professor Vladlena Benson at Aston Business School is joined by Dr Donato Masi (Deputy Director) and the Senior Management team leading in research issues, increasing the scope of research operations, and developing strategic directions of research in coordination with the CSI industry and government stakeholders. The scope of the international Cyber Security & Innovation Centre is to effectively manage operations and build effective relationships across academia, industry and policy makers. The Cyber Security Innovation Centre at Aston Business School involves working with industry and government stakeholders. Innovation projects in this realm carried out by Aston academics improve cyber security posture of organisations from large to micro enterprises, involve regular communication and active engagement with policy making processes in the areas of Virtual Financial Assets (VFAs), AI, National Cyber security Strategy, National Infrastructure Security, Age Verification for the Digital Economy, Cybersecurity Insurance and Cyber Risk Management Instruments.

The Centre is addressing profoundly multifaceted challenge that is cyber security by linking academics in information security, corporate governance, risk management, linguistics, criminology, intelligence, law and psychology together with cyber security experts from industry and government. Our research activities ensure the protection of the global economies critical infrastructure, security of the connected supply

The Cyber Security Innovation centre forms a network of academic, business and government leaders:

- Providing expertise and leadership in cyber security regarding technology, governance, policies and human factors;
- Offering a platform for exchange between academics and practitioners from business and government;
- Conducting cross-cutting research across several disciplines in the field of privacy, victimisation, organisational resilience, cyber physical systems security, cyber security risk management, trusted artificial intelligence and human-centric security;
- Training the next generation of cyber security specialists as well as raising awareness among our leaders and developing the skills of the existing workforce.

The Cyber Security & Innovation Centre aims to have more forward-thinking industry, government and academic institutions (both in the UK and internationally) join the CSI.

UK Cyber Security Council,
Representative Workstream 6

Board Member,
UK Central ISACA

European Cybersecurity Framework,
ENISA

The Cyber Security Innovation
Research Centre

Contents

Introduction

This report explores the emerging regulatory developments of cryptocurrencies and presents a legal analysis of the approaches adopted by different countries. The global rise and evolution of cryptocurrencies has caused an increase in regulation to guide relevant activities.

This report will profile regulatory responses according to three criteria provided by the Global Compliance Report (2020). The first of these examines the exchange status of cryptocurrencies, exploring whether a jurisdiction has employed new regulations, expanded existing legislative parameters in response to identified grey areas, issued a ban, or remained non-committal thus far. The second looks at whether countries associate cryptocurrencies with legal tender and lastly, proposals for upcoming legislation within each country or region. These dimensions will help assess the legal position of cryptocurrencies in different territories and whether they reflect a strict or relaxed regulatory regime. The report further discusses the treatment of cryptocurrencies in relation to their legal status within financial and tax laws. While a consensus exists among policymakers that the high volatility of cryptocurrencies is of concern, the regulatory approach adopted nevertheless differs significantly across jurisdictions. Similarly, typical cryptocurrency features are associated with anonymity and decentralisation, which can facilitate illicit activities. Therefore, various preventative measures have been executed by regulators to mitigate financial crime, with particular attention to anti-money laundering (AML) and countering the financing of terrorism (CFT). Furthermore, the analysis illustrates imminent projects held by nation-states to assess the suitability and performance of different crypto technologies. These developments indicate a direction of travel from legal and financial institutions to increase innovative financial technology and the regulatory landscape of cryptocurrencies. This report analyses the degree of regulation in each region and whether the legal procedures reflect a stringent or lenient approach. The method used for this profiling compares legislative strategies, government rationales and policy frameworks that aim to effectively facilitate development.

Cryptocurrency has transformed the international payment ecosystem. Many associate the term '*cryptocurrency*' with the blockchain systems and distributed ledger technology (DLT). Although not all cryptocurrencies use blockchain, in general they rely on encryption and cryptography techniques to create a virtual currency with security, transparency and a decentralised nature as distinguishing features. In particular,

the absence of a central intermediary appears to be the most attractive feature since it prevents centralised intervention. Additional advantages include faster transfer of funds, minimal processing and transaction fees, confidentiality, and improved transparency. The success of cryptocurrency may stem chiefly from transparency, because it provides an alternative method to conventional payment systems. It provides a transparent record of the financial transactions of all actors trading in the cryptocurrency, thereby providing greater accessibility of information.

Although, cryptocurrency has been embraced with enthusiasm, its properties also create risks. *Tymoigne* (2015) highlights the fact that cryptocurrency is still an emerging technology and has high volatility. He maintains that cryptocurrencies cannot amount to durable electronic currencies until they become widely distributed and improve liquidity.[1] The lack of institutional support also poses higher risks for investors, as there is no formal legal entity accountable in cases of insolvency. Further limitations reveal cryptocurrencies can be used as a tool for money laundering, financing for terrorist organisations and other illicit activities. *Thapar* (2018) notes inherent properties of cryptocurrency like anonymity and decentralisation may be considered ambiguous. The platform allows users to create accounts anonymously and unlawfully convert cryptocurrencies into fiat currencies at low risk. Similarly, these properties can facilitate an easy transfer of payments for the purposes of terrorist financing.[2] Although both features appear attractive to participants, they provide opportunities for channelling illegitimate funds.[3] *Parashar* (2018) adds that decentralisation risks introducing a lack of control because the system is instructed by an algorithm and therefore tracing the movement of virtual currency will prove difficult for government bodies.[4] Hence, in order for cryptocurrencies to predominate in the global payments system, they must deliver increased value and overcome regulatory uncertainties. In recent years, development of crypto technology has required policymakers to provide clarity on the position of cryptocurrency in the financial sector. *Camoron* (2016) suggests government authorities will not allow the operation of cryptocurrencies within formal financial institutions without appropriate integration.[5] *Vora* (2015) asserts that cryptocurrencies and similar products are an indication of economic progress that offers a chance for existing systems of currency and statutory regulation to develop further. Cryptocurrency has significant potential to provide evolutionary changes for its economic agents. The technology can be used to alleviate existing disadvantages for impoverished people and achieve socially and financially inclusive outcomes. For example, according to data from the Global Findex Report 2017, 1.7 billion people worldwide still do not have access to a bank account. In this context, cryptocurrency can provide an alternative service to conventional financial institutions that has the potential to be inclusive. This technology can provide individuals with efficient, timely and transparent financial products and services. With the development of coordinated policies and strategies, aspects of cryptocurrency can be optimised - and risks controlled - to assist economic prosperity.[6]

A new addition to cryptocurrency terminology has been provided as part of recent regulatory changes in Malta. The Virtual Financial Assets Act 2018 (VFAA) (Chapter 590) classifies virtual assets as *"a virtual token; a virtual financial asset; electronic money or a financial instrument."* The virtual financial asset (VFA) has been described as a type of *"digital medium recordation that is used as a medium of exchange, unit of account, or store of value and does not constitute electronic money, a financial instrument; or a virtual token."* Therefore, this interpretation separates the different types of assets For instance, a virtual token is, *"a form of digital medium recordation whose utility, value or application is restricted solely to the acquisition of goods or services"*. This suggests these tokens have no utility, application or value outside the platform. Initial VFA Offerings (IVFAO) were described in Articles 3-12 of the VFAA. It is relevant to Initial Coin Offerings (ICO), defined as a process to offer VFA to the general public in order to raise funds. It is a category of funding using cryptocurrencies and is commonly referred to as a form of crowdfunding.

On the other hand, Malta's Banking Act 1994 (Chapter 371) defines electronic money as, *"the monetary value as represented by a claim on the issuer issuing such money which is:*

a) stored on an electronic device,

b) issued on receipt of funds of an amount of not less in value than the monetary value issued,

c) accepted as means of payment by undertakings other than the issuer".

Electronic money is recognised as legal tender and operates as a digital transfer mechanism backed by fiat currency, thereby distinguishing it from cryptocurrency. Furthermore, the definition of a financial instrument is detailed in the Second Schedule to the Investment Services Act 1995 (Chapter 370). Here, 'financial instrument' refers to securities that are transferable and flexible on the capital market and include:

a) shares in companies and other securities equivalent to shares in companies, partnerships or other entities, and depository receipts in respect of shares;

b) bonds or other forms of securitised debt, including depository receipts in respect of such securities;

c) any other securities giving the right to acquire or sell any such transferable securities or giving rise to a cash settlement determined by reference to transferable securities, currencies, interest rates or yields, commodities or other indices or measures.

It includes instruments that are managed on the money market, for example *"treasury bills, certificates of deposit and commercial papers and excluding instruments of payment"*. Essentially, financial instruments are legislated separately, granting property rights for particular instruments that fall within the scope of the schedule.

Nonetheless, the systemic risks posed by cryptocurrencies have grown as a concern for member states of the G20, a key objective of which is to maintain secure and sustainable growth of the global financial system.[7] G20 members include Argentina, Australia, Brazil, Canada, China, France, Germany, India, Indonesia, Italy, Japan, Mexico, Republic of Korea, Russia, Saudi Arabia, South Africa, Turkey, the United Kingdom, the United States and the European Union. This matter was assigned to the Financial Action Task Force (FATF), which has provided guidelines to mitigate the regulatory uncertainties emerging from cryptocurrencies. The rationale for introducing legal directives to regulate cryptocurrencies has been largely motivated by mitigating risks and preventing financial crime. Predominantly, FATF has focused on setting standards for AML/CFT in order to maintain the transparency and security of the international financial system.

FATF initially published a report, *Virtual Currencies: Key Definitions and Potential AML/CFT Risks* (June 2014) to present possible threats associated with new payment mechanisms emerging from cryptocurrencies. The report clarified common terminologies within the virtual currency domain, a task necessitated by the lack of lexis that adequately described different forms of virtual currency. The following report, *Guidance for a Risk-Based Approach to Virtual Currencies* (2015) established different methods that can avert ML/TF risks related to virtual currency payment products and services. By that time, it had become apparent that authorities worldwide were seeking to overcome regulatory challenges within the sector. Therefore, the terms set out by FATF were intended to assist regulators and governments to eliminate such risks.

Due to the ongoing development of the crypto sphere, FATF has since issued revised guidance on virtual currency activities.[8] The most recent edition, *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers* (June 2019), offers guidance on the application of suggested crypto policies for domestic implementation on a risk-based approach for AML/CFT. FATF has also incorporated broader terms such as, Virtual Assets (VA) and Virtual Asset Service Providers (VASPs) as this area attracts more international financial and regulatory interest. Alongside such reports, FATF issued an *Interpretive Note* (February 2019) as an amendment to **Recommendation 15** (October 2018).[9] This provides countries with a direction to implement a risk-based approach and, accordingly, to address ML/TF risks. Preventative measures to combat the threats posed by virtual currencies are presented.[10]

The new guidance has incorporated a catalogue of potential risks for authorities to identify and assess in accordance with ML/TF. For instance, immediate peer-to-peer transactions that are (to a great extent) anonymous lack the institutional intermediaries that act as conventional gatekeepers in the global AML/CFT regime. This fact has forced policymakers to try to bring cryptocurrencies under the authority of regulation.[11] An array of suggested preventative measures including stringent due diligence and supervisory requirements have been proposed. FATF emphasised the obligation for licencing and registration, while urging regulators to communicate with financial authorities to combat financial crime. Additionally, comprehensive record-keeping, suspicious transaction reporting, disciplinary and financial sanctions are some of the suggested interventions. In effect, VAs that enable pseudonymous transactions pose higher risks of ML/TF. Therefore, **Recommendation 10** advocates that countries adopt customer due diligence procedures. This process enables authorities to identify customer information, the beneficial owner and the nature of the business relationship. This requirement aids authorities in preventing potential fraudulent and illicit activities enabled by the anonymous and borderless features of cryptocurrencies. However, this recommendation directly conflicts with the nature of cryptocurrency and reduces the scope for anonymity, for both users and transactions. The aim of the guidance was to advocate accommodating policies that can adapt to a fast-changing digital environment without restricting innovation. Crypto platforms might, however, argue that the practical effect of enacting such a recommendation would be a decline in the market as the industry adjusted to regulatory principles that could restrict its facilities and limit the growth of technology.

What is evident is that while FATF has recognised the development of the crypto space, emerging new products and services increase the complexity of capital flows. Therefore, to provide clarity, the interpretive note to **Recommendation 15** directly relates to the treatment of VAs by financial regulators. The guidance provides relevant policies that support effective implementation and removes obscurity in the regulatory sector to enable individual countries to advance their cryptocurrency regulation. FATF outlines the significance of supervising and monitoring VASPs, information exchange and endorsing licencing or registration mechanisms to uphold AML/CFT measures.

Requirement 1 directs countries to establish cryptocurrencies into a category for the purpose of regulation, to organise virtual assets either as, *"property," "proceeds," "funds", "funds or other assets," or other "corresponding value"*, and employ relevant measures under the FATF Recommendations.[12] **Requirement 2** recommends VASPs be proactive in identifying and assessing risks. This refers to the above-mentioned requirements, namely that financial institutions should confirm the identity, region, and intention of each user to satisfy the AML/CFT agenda before pursuing a customer relationship.[13] Although such risks are inherent to cryptocurrency, these policies ought to function similarly to those within the traditional financial framework.[14] The use

of regulatory instruments can accommodate the cryptocurrency market within existing financial services and reduce risks of ML/TF.[15] Furthermore, this strategy appears progressive due to the significance placed on due diligence procedures, which will inevitably simplify the process and potentially reduce costs for financial institutions seeking to identify potential clients from a reliable source.[16] **Requirement 3** stipulates that a VASP should be licensed or registered in the jurisdiction in which it operates. Authorities should be able to apply relevant sanctions to VASPs that function exclusively. This strategy will offer support to national authorities when taking necessary legal measures to prevent financial crime within the VASP domain. The guidance further explains it can be detrimental for an offender to stand as the beneficiary or maintain a significant position within the functioning of a VASP.[17] **Requirement 4** establishes that financial institutions previously licensed or registered within a jurisdiction and authorised to interact with VASPs will not be subject to separate licensing or registration processes. However, those financial institutions will be responsible for the obligations detailed under FATF's recommendations.

Requirements 5 and 6 echo the importance of implementing supervision and monitoring strategies for the prevention of ML/TF. Given the distinctive features of cryptocurrency, the quality of due diligence may vary depending on the extent of risk involved. Therefore, financial institutions will have to conduct appropriate inspections and impose sanctions to ensure compliance of VASPs. It should be noted that some ardent crypto supporters have suggested this requirement could restrict the development of the VA domain, asserting that the intervention of legal and financial regulators could be damaging to the growth of cryptocurrency, as such bodies are inexperienced in regulating the technological space. Likewise, the inherent features of cryptocurrency, like anonymity and decentralisation, are ineligible for regulation unless obstructing the features themselves.[18]

Requirement 7 guides financial institutions to endorse transaction reporting and record-keeping for VASPs. They are required to execute customer due diligence checks on transactions that exceed a threshold of USD/EUR 1,000. In order for authorities to uphold a risk-based approach, it is vital they obtain accurate beneficiary information on transfers, as well as sufficient identification of holders, accounts and funds upon request. These factors will aid financial institutions to apply controls and detect potential ML/TF activities. Nonetheless, FATF's recommendations have placed considerable pressure on VASPs to accommodate due diligence requirements. The cryptocurrency sector has resultingly been burdened with the complexity of identifying pseudonymous data, for example. Further implications are related to transactions provided by VASPs. For instance, peer-to-peer networking within cryptocurrency transactions differ from conventional fiat currency transfers that are expedited by financial institutions. Alternatively, blockchain technology permits participants to transact with each other independently of an intermediary. Therefore, VASPs simply initiate networking between members through the platform. It will prove problematic for VASPs to replicate the administrative requirements of traditional intermediaries because they do not acquire the relevant information that authorities wish to access. Ultimately, **Requirement 8** supports international cooperation between authorities and swift information exchange between countries to counteract ML/TF and other illicit activities occurring from the crypto sphere. The inference to be drawn from this is that the application of FATF's requirements are compatible with a variety of different legal and regulatory systems. They provide a broad range of recommendations that allows for flexible implementation. Authorities are provided with a detailed explanation of the essential requirements to adequately combat the risks deriving from the crypto space. Therefore, countries are able to adopt satisfactory measures to achieve the objectives provided by FATF that simultaneously cohere with the legal system of their jurisdiction.[19] FATF has provided a framework for both financial institutions and policymakers to tackle the technical complexities of cryptocurrency. *Chohan* (2020), however, highlights that FATF has not considered other risks outside the scope of ML/TF that are detrimental to the virtual market. In essence, the guidance has not confronted additional legal topics in relation to VAs and VASPs, which may be summarised as including consumer protection, security and privacy, fraud, marketing and economic objectives.[20] While FATF's guidance is flexible and adaptable, studies suggest the guidance has not addressed the impact of local factors in each jurisdiction which will affect the implementation of its recommendations. This serves to demonstrate that financial and legal regulators are likely to adopt principles proposed by FATF in accordance with their national context.[21] Therefore, the AML/CFT framework is likely to be susceptible to the technological and social dimensions of a particular country. Essentially, legal frameworks regulating VA and VASPs will differ globally and reflect different perspectives. The Global Compliance Report outlines how policymakers have grappled with the development of cryptocurrencies. This has impacted the structure of the regulatory landscape and responses have not been uniform. For example, some jurisdictions have recognised the unique qualities of cryptocurrencies and, as a result, established new legal frameworks for a single, concise form of regulation. Others, meanwhile, have made efforts to accommodate the virtual space via extension of existing legislation. Countries that have taken the latter approach tend to regard cryptocurrencies as a type of commodity. At the most extreme end, some countries have banned the use of cryptocurrencies within their territory entirely, in an attempt to avert pressures on the financial ecosystem. Thus, the profile of each country below will illustrate the varying approaches adopted and implemented by different regions.

VFA Profiling

1. Cayman Islands

- Not considered legal tender
- Legal, no explicit cryptocurrency regulations
- Upcoming legislation for virtual currency transactions
- Mutual Funds Law
- Securities Investment Business Law
- Companies Law
- Limited Liability Companies Law
- Money Services Law
- Proceeds of Crime Law
- Anti-Money Laundering Regulations

2. Jamaica

- Not considered legal tender
- Legal, no explicit cryptocurrency regulations
- Upcoming legislation from Jamaica Stock Exchange to enable live trading of digital assets
- Securities Act 1993
- Banking Services Act 2014
- Payment, Clearing and Settlement Act

3. Trinidad & Tobago

- Not considered legal tender
- Legal, unregulated
- Possible upcoming legislation
- N/A

4. St. Lucia

- Not considered legal tender
- Legal, no unregulated
- Possible upcoming legislation after successful Eastern Caribbean Central Bank pilot scheme
- N/A

5. Venezuela

- Not considered legal tender
- Legal, regulated
- No upcoming legislation
- Constitution
- Law of the Central Bank of Venezuela
- Constitutional Decree
- Law of the Financial Administration of the Public Sector
- Organic Law on Hydrocarbons
- Constitutional Decree on the Crypto Asset Integral System
- Organic Law on Organised Crime, Terrorism Financing and Proliferation of Mass Destruction Weapons

6. Ecuador

- Not considered legal tender
- Legal, unregulated
- No upcoming legislation
- Organic Monetary and Financial Code
- Resolution 005-2014-M of the Monetary and Financial Regulation and Policy Board
- Fundament al Monetary and Financial Code

7. Chile

- Not considered legal tender
- Legal, unregulated
- Upcoming legislation to regulate virtual currencies
- Law No. 19, 913 (Anti-Moneda Laundering Act)
- Law No.20, 393

8. Argentina

- Not considered legal tender
- Legal, unregulated
- No upcoming legislation
- Central Bank of the Argentine Republic and Financial Institutions
- Organic Charter and Gral Regime of the Central Bank of the Republic of Argentina
- Prevention of Money Laundering and Terrorism Financing Resolution 300/2014
- Law of Social Solidarity and Productive Reactivation within the Framework of the Public Emergency
- Laundering of Criminal Origin Assets – Pean Code Modification
- Regime for the Promotion of the Knowledge Economy

9. Nigeria

- Not considered legal tender
- Legal, unregulated
- Possible upcoming legislation
- Central Bank of Nigeria Anti-money Laundering and Combating the Financing of Terrorism in Banks and other Financial Institutions in Nigeria Regulations 2013
- The Nigerian Cybercrime (Prohibition, Prevention) Act 2015

10. Russia

- Not considered legal tender
- Legal, unregulated
- Upcoming legislation, expanding existing legislation
- Federal Law "On the Central Bank of the Russian Federation"
- The Russian Civil Code
- Federal Law No. 115-FZ "On Counteracting Legalisation (Laundering) of Illegal Income and Terrorism Financing"

11. China

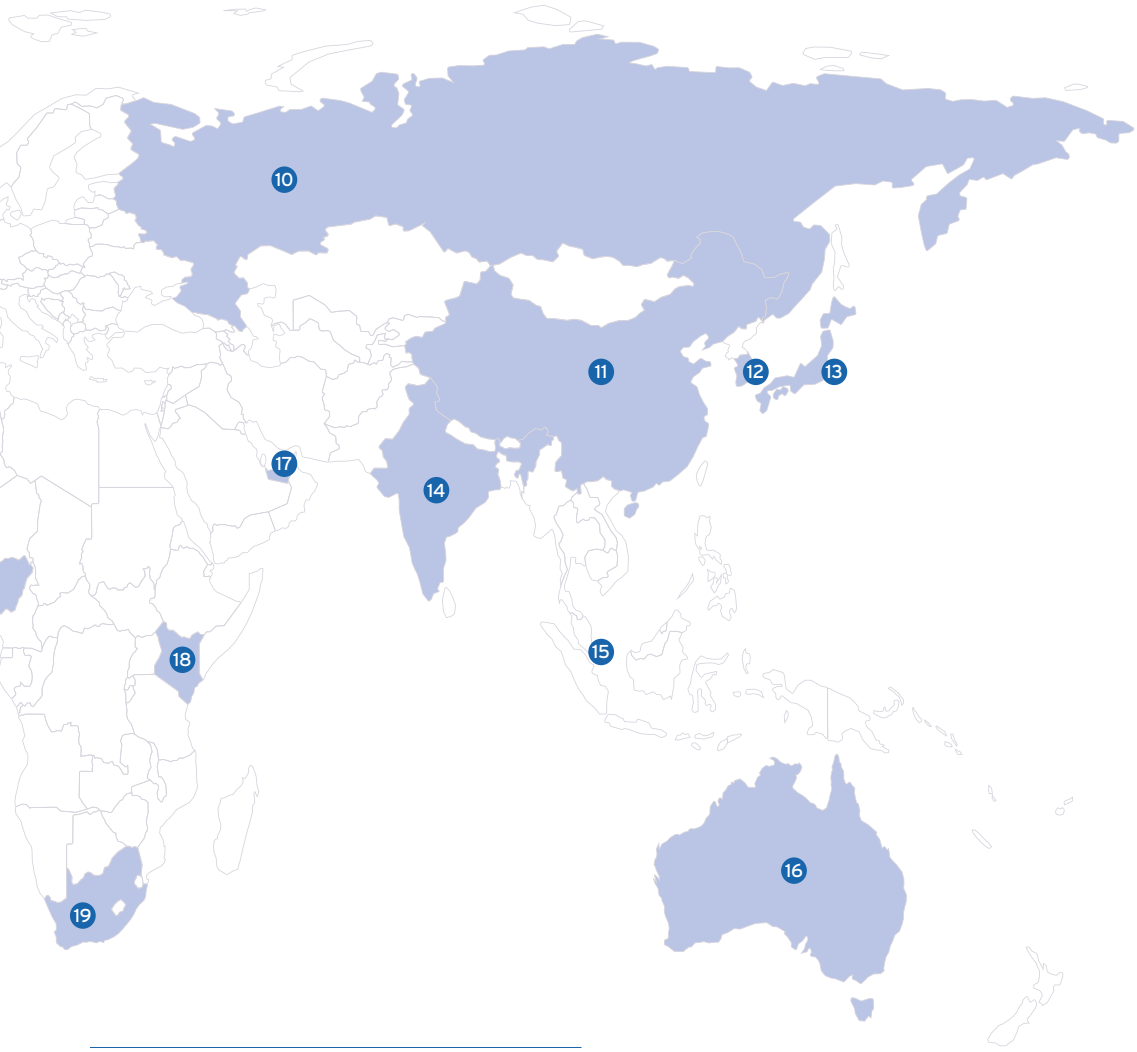
- Not considered legal tender
- Illegal, cryptocurrency exchanges banned
- No new upcoming legislation or removal of ban
- Blockchain Information Service Management Regulations

12. South Korea

- Not considered legal tender
- Legal, no legal framework regulating cryptocurrency
- Upcoming legislation to recategorize virtual currencies as digital assets
- Financial Investment Services and Capital Markets Act 2017
- Act on Reporting and Using Specified Financial Transaction Information

13. Japan

- Not considered legal tender
- Legal, regulated through existing legislation
- Upcoming legislation for cryptoasset derivative transactions
- Payment Services Act
- Prevention of Transfer of Criminal Proceeds
- Financial Instruments and Exchange Act



14. India

- Not considered legal tender
- Legal, no legal framework regulating cryptocurrency
- Upcoming legislation
- Prevention of Money-Laundering Act 2002
- Payment and Settlement Systems Act 2007
- Securities Contracts (Regulation) Act 1956
- Companies Act 2013
- Prevention of Money-Laundering Act 2002

15. Singapore

- Not considered legal tender
- Legal, cryptocurrency regulated through existing legal frameworks
- No new upcoming legislation
- Payment Services Act 2019
- Securities and Futures Act 2001
- Financial Advisers Act 2001
- Commodity Trading Act 1992
- Income Tax Act 1947
- Goods and Services Tax Act 1993

16. Australia

- Not considered legal tender
- Legal, cryptocurrency regulated through existing legal frameworks
- Upcoming legislation to strengthen regulatory controls.
- Corporations Act 2001
- Australian Securities and Investments Commission Act 2001
- Schedule 2 of the Competition and Consumer Act 2010
- Income Tax Assessment Act 1936
- Income Tax Assessment Act 1997
- Anti-Money Laundering and Counter-Terrorism Financing Amendment Act 2017

17. United Arab Emirates

- Not considered legal tender
- Legal, cryptocurrency regulated through existing legal frameworks
- Upcoming legislation to govern ICOs.
- Federal Law No. 4 of 2000, Concerning the Emirates Securities and Commodities Authority and Market
- Regulatory Law 2004
- Federal Law No. 20 of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism And Financing of Illegal Organisations
- Law No. 7 of 2014 on Combating Terrorism Offences

18. Kenya

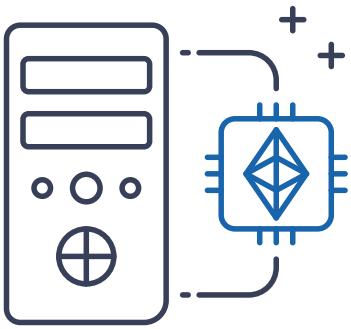
- Not considered legal tender
- Legal, unregulated
- Possible upcoming legislation
- Value Added Tax (VAT) (Digital Marketplace Supply) Regulations 2020

19. South Africa

- Not considered legal tender
- Legal, unregulated
- Possible upcoming legislation
- Financial Sector Regulation Act 9 of 2017
- Draft Taxation Laws Amendment Bill
- The Financial Intelligence Centre Act 28 of 2001

United Kingdom

In the United Kingdom (UK), cryptoassets are often considered an investment tool that are not considered legal tender and do not equate to fiat currencies. Perhaps as a consequence, authorities have not identified cryptocurrency as an imminent threat to the economic system in the UK and there are no stringent financial laws applicable to cryptocurrency.



Cryptocurrencies have been divided into regulated and unregulated instruments. The UK has not published first-hand legislation to regulate the crypto space, instead extendeding its existing directives to neutralise challenges. For cryptoassets to be regulated like the broader financial services sector in the UK, they must fall within the scope of the Financial Services and Markets Act 2000 (FSMA), or under the Payment Services Regulations 2017 (PSR) and the Electronic Money Regulations 2011 (EMR). The specified instruments listed in the Financial Services and Markets Act 2000 (Regulated Activities) Order 2001 (RAO) (RAO), outlines the regulated categories of cryptocurrency that are accountable to financial regulation in the UK.

Security tokens are a regulated instrument under the RAO and are mentioned in the Cryptoassets Taskforce Final Report, October 2018. The taskforce has determined such tokens amount to a specified investment, which may provide ownership rights and entitlement to settlements or upcoming shares. The Financial Conduct Authority (FCA) regulates security tokens as specified investments. Such tokens may be available for transferable securities or other financial instruments under the EU's Markets in Financial Instruments Directive II 2014 (MiFID II). Exchange tokens constitute unregulated cryptocurrencies and fall outside the scope of regulation. Therefore, activities on Bitcoin, Ether and Litecoin in relation to such tokens are currently unregulated. Such tokens are decentralised and operated on DLT, for the purpose of investment or as a means of exchange, and have no rights attached. Utility tokens generally utilise the DLT platform where tokens can be exchanged in return for goods or services. Therefore, instruments that do not constitute security tokens or e-money tokens are unregulated under UK legislation. However, instances involving unregulated cryptocurrencies as a means of business can potentially initiate a regulated action and require permissions from the FCA.[22]

The FCA issued separate Guidance on Cryptoassets, Consultation Paper CP 19/3 in January 2019 which delivers an account of the type of cryptoassets that will be regulated by the FCA, together with the responsibilities placed on institutions, and regulatory protections available to consumers. The guidance further demonstrates cryptoassets that fall outside the regulatory perimeter. Further guidance was issued relating to Feedback and Final Guidance to CP 19/3 in July 2019. This consultation document added clarity to the FCA's regulatory perimeter to help consumers understand the cryptoasset market and the eligible protections. Stable coins are a common type of cryptoasset which present a challenge to the financial regulatory sector. They are predominantly used as a means of exchange but differ from usual cryptocurrencies. The value of the stable coin is attached to a central asset which ought to enable a stable market value. However, this process can be achieved through different methods and the particular system used by a specific stable coin will determine its regulatory arrangement. For instance, a stable coin that is backed by a central issuer, and has a reference attached to an asset, the issuer holding the referenced asset will likely constitute a specified investment if holders of the stable coin have rights in relation to the referenced asset. However, if the relevant rights are not present it is possible to be unregulated under UK legislation. According to FATF, generally, stable coin holders and service providers are subject to FATF guidance and should not be left outside the scope of AML/CFT directives.[23]

Most recently, the FCA has published a new policy banning the sale of derivatives and exchange traded notes (ETNs) in relation to particular types of cryptoassets to retail consumers. The FCA has concluded such commodities are inappropriate for retail consumers because of potentially unfavourable consequences. These are that such commodities cannot be accurately valued by retail consumers because of the

The FCA issued separate Guidance on Cryptoassets, Consultation Paper CP 19/3 in January 2019 which identifies the types of cryptoassets that will be regulated by the FCA, together with the responsibilities placed on institutions, and regulatory protections available to consumers.

inherent characteristics of such assets; financial crime; high volatility in cryptoasset prices; premature technology; and insufficient grounds for investment by retail consumers. The reasons highlighted above suggest retail consumers are likely to suffer losses as a result of investment. Moreover, the FCA has previously made a distinction between unregulated transferable cryptoassets and regulated specified investments. In order to prevent the consequences outlined, the FCA banned the sale, marketing and distribution of derivatives and ETNs that include unregulated transferable cryptoassets by businesses acting in, or from, the UK. An estimate produced by the FCA suggests the ban will help retail consumers save £53m, therefore the purpose of this ban is to preserve consumer protection. The ban will be enforced from 6 January 2021. In the meantime, consumers have been cautioned to be aware of fraudulent crypto-related activities. In the Policy Statement (PS) PS20/10, the FCA outlines its final position and stipulates all relevant policies that will take effect on 6 January 2021.

The new policies will affect businesses issuing, creating, or marketing products that reference cryptoassets; businesses distributing products that reference cryptoassets which include brokers, investment platforms and financial advisors; trading platforms; retail consumers; and relevant stakeholders which are regulated and unregulated. The FCA highlighted a number of reasons for its conclusion explained in PS20/10. For example, retail consumers cannot reliably value cryptoassets since they have no intrinsic value and their valuations can therefore fluctuate substantially. The lack of reliability poses a high risk of unpredicted losses. The price fluctuation across exchanges shows differences in cryptoasset prices between exchanges over a 14-day period. Also, the high correlation between different cryptoassets suggests cryptoasset prices reflect speculation rather than economic forces within the technology sector. The FCA has also determined that crypto derivatives do not constitute a legitimate investment need, despite some consultation respondents suggesting potential uses for crypto derivatives such as hedging, where investors use crypto derivatives to hedge against volatility. The FCA notes that this advantage does not compensate for the prospective harms, whereas the ban will provide significant consumer protections.

In July 2019 the CP19/22 mentions that the (then) existing regulations do not adequately tackle the harms caused by crypto derivatives. Thus, the FCA felt the prohibition will mitigate the potential consequences. Further, the FCA considered the relevant provisions in Article 42 of Markets in Financial Instruments and Amending Regulation (MiFIR) and Article 21 (2) of the Delegated Regulation of MiFIR and concluded that the marketing, distribution and sale of crypto derivatives still exposed retail consumers to significant harm. The FCA extended the ban to all derivatives and ETNs that reference unregulated transferable cryptoassets because all forms present potential harm to retail consumers. They also determined that crypto ETNs hold comparable risks, together with the restricted amount of products available on EU trading platforms. This demonstrated the proportionality of the prohibition. Nevertheless, some arguments were made by respondents that existing regulations are competent to address the apparent harms. The FCA stated that existing regulations address the direct risk of regulated products but not the indirect harm from the underlying assets which regulated products reference. Meanwhile, the existing regulations support the distribution of products rather than their suitability for retail consumers. Additionally, the FCA has recognised that prohibition may drive investors to trade in unregulated cryptoassets or trade crypto derivatives outside the UK. However, the FCA believes the prohibition will protect the majority of consumers and act as a caution to those engaged in these products.

While cryptocurrency shares comparisons of fiat currency and property, the risk profile differs substantially from traditional assets. To simply incorporate cryptocurrency into the existing regulatory frameworks can be problematic, as the guidelines will be directing two different financial mechanisms Therefore, despite the UK having an initial lead on cryptocurrency activity, focused cryptocurrency regulations will deliver greater assistance to both VA users and VASPs.[24] Nonetheless, it is clear the UK's financial and judicial systems are capable of constructing thorough regulation to remain at the forefront of global regulatory efforts

The Fifth EU Money Laundering Directive (5MLD) came into force in January 2020, and has been integrated into the Money Laundering and Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations.

post-Brexit. Meanwhile, some crypto users are requesting separate regulations for the protection of participants and businesses, in particular, a regulatory framework that can ensure opportunities through impartial policies for consumers and service providers. It is clear that financial institutions will need to work closely with regulators and VASPs in order to maximise the economic opportunities. Nonetheless, FCA guidelines alongside FATF's recommendations offer a valuable contribution towards the transformation of the regulatory space within cryptocurrency. Regulators have taken a progressive approach to the rapid growth of cryptocurrencies, irrespective of cautions issued by the FCA and the UK has refrained from imposing general prohibitions and bans. Additional clarity applied to the categorisation of VFAs within the existing legislative perimeter would nevertheless be useful for participants that require regulation as a matter of urgency. Essentially, the UK has taken proportionate steps to enable growth in the crypto world while developers continue to explore the possibilities for sectoral growth.

There are no bespoke tax laws regulating cryptocurrencies in the UK. However, the authorities have expanded existing tax laws. HM Revenue and Customs (HMRC), the UK's tax authority, issued a policy paper *Cryptoassets for individuals* in December 2018. The document established that the tax treatment of cryptoassets will vary depending on the use and characterization of the token and not its definition. Section 275 and 275A of the Taxation of Chargeable Gains Act 1992 provides statutory definition on whether a particular type of asset will be subject to taxation in the UK. Individuals that occupy cryptoassets for *"personal investment will be liable to pay Capital Gains Tax when they dispose their cryptoassets"*. Likewise, individuals will be subject to pay Income Tax and National Insurance Contributions under the Income Tax Act 2007, on cryptoassets which they receive from *"their employer as a form of non-cash payment or, mining, transaction confirmation or airdrops"*.

The PSR and EMR provide a regulatory framework for payment services in the UK. These regulations are only applicable to individuals employing payment services or electronic money, as defined in the PSR and EMR. However, it is important to note that payment services specified in the PSR include the use of funds, whereas cryptocurrencies do not constitute funds. Therefore, it is very unlikely for exclusively cryptocurrency products to amount to a payment service. Nevertheless, it is important to consider the exemptions, for instance stable coins that have been designed as e-money would in fact fall within the perimeter of the PSR and EMR. Conversely, where fiat currencies are involved there will be funds, so further analysis would need to be conducted to determine whether payment services are being provided and, if so, the precise application of the regulatory regime established by the PSR and EMR. Equally, where fiat currencies are included the funds will have been established in such a way that this will initiate further analysis to determine whether payment services are being provided and the relevant application of the PSR and EMR can take effect.

The UK understands the dynamics of cryptocurrencies with the risks of ML/TF, and shares similar concerns identified by FATF. The Fifth EU Money Laundering Directive (5MLD) came into force January 2020, and has been integrated into the Money Laundering and Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017. The changes put forward by the 5MLD are focused on delivering additional powers from previous AML/CFT directives. For example, the provisions provide increased access to beneficiary and ownership information.[25] The directive confronts anonymity by employing firm customer due diligence checks. Thus, participants entering a transaction through virtual exchange cannot remain anonymous. Authorities are required to use financial intelligence units to monitor registered cryptocurrency users and verify identities and addresses. Simultaneously, these mechanisms will align the proposals in the 5MLD to FATF's recommendations, steering towards a global approach for confronting ML/TF. Alongside these provisions' firms are expected to register with local financial authorities to comply with the AML/CFT regime. Essentially, previous directives have been amended to create new requirements that can adjust to the growth of technology.

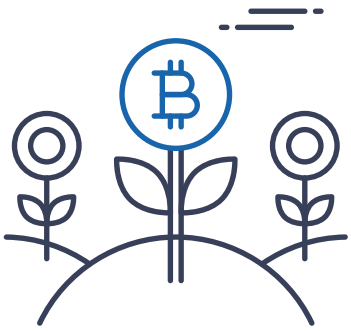
Although, the 5MLD has made significant efforts to safeguard financial transactions, the definition of virtual currencies features legal uncertainty. For instance, it states virtual currencies *"must be accepted by the natural or legal persons as a means of exchange"*. This provision invites further clarification as the directive does not explain what is intended by the requirement. Any use of a virtual currency will action an exchange; goods or services can be accepted in exchange for other tokens or against fiat currencies. Therefore, the text does not outline the specificities of a virtual currency that can be used as a means of exchange. *Haffke et al* highlighted that the implications of this wide interpretation could potentially extend powers of the AML/CFT regulation to accommodate transactions within the private sector. Consequently, this will instigate unwarranted scrutiny and reduce boundaries of regulation. This demonstrates the 5MLD requires a narrow interpretation. Furthermore, the term *"means of exchange"* commonly refers to the role of money, however the unique characteristics of cryptocurrencies mean the purpose is primarily transitional within trade rather than a medium of exchange. Therefore, certain tokens that act as transitional assets within trade will amount to a virtual currency provided by the definition of 5MLD. Conversely, other tokens that are used for investment purposes that do not act as a transitional asset will be left outside the legal structure of 5MLD. Consequently, the definition requires refinement and should reflect a more focused description of virtual currencies.[26]

Moreover, the directive clearly holds *'custodian wallet providers'* and *'virtual currency exchanges'* accountable to the stipulations under 5MLD. The inference to be drawn from this is that the 5MLD has overlooked crucial members within the cryptocurrency market. For instance, miners have the required skills and capacity to initiate openings for invaders to exploit and facilitate conditions for ML/TF. As key actors, they have the potential to join investments through the mining industry, which can be later sold for fiat currencies. This is an attractive opportunity for offenders to replicate to convert funds into cash holdings. Likewise, mining cryptocurrencies in the UK is legal, as no tailored legislation exists to regulate such activity. Therefore, miners should be included in the scope of regulation to enhance the AML/CFT rule. Furthermore, whether an individual is subject to licensing requirements for activities related to cryptocurrencies in the UK will be contingent on their definition under the FSMA and some activities involving cryptocurrencies will require approval from the FCA.

Nevertheless, in November 2018 the FCA formed a new department for regulators to assess various strategies in accordance to innovation in the financial sector. The FCA's 'regulatory sandbox' has permitted businesses that are competent in the eligibility criteria to sample proposals for an innovative financial system, alongside genuine consumers. The FCA's agenda has influenced a global sandbox for regulators to effectively develop propositions between jurisdictions. The UK has taken a lead through this project, creating a platform for regulators to network with financial firms for effective policymaking initiatives. The FCA has also offered further cooperation to businesses that will be requesting permissions from it, to enable them to function in this innovative industry. It is clear the existing laws surrounding cryptocurrencies in the UK are not well defined. However, these activities suggest the government is working towards tightening policies and expanding the remit of regulation.

European Union

The EU approved the Fifth Money Laundering Directive (5MLD), in April 2018 which brought cryptocurrency and fiat currency exchanges in line with the EU Anti-Money Laundering and Counter Terrorist Financing legislation (AML/CFT).



Inherent characteristics of cryptocurrency, such as anonymity and quick transferability, are easy to exploit, and provide innovative methods to execute financial crimes. The EU approved the Fifth Money Laundering Directive (5MLD), in April 2018 which brought cryptocurrency and fiat currency exchanges in line with the EU Anti-Money Laundering and Counter Terrorist Financing legislation (AML/CFT).[27] The EU has also outlined potential challenges to the monetary system and the control of currencies by the European Central Bank (ECB) with particular regard to the increased popularity and practice of cryptocurrencies resembling the functions of fiat currency and medium of exchange. Cryptocurrency could provide an improved system in comparison with traditional banking and offer a decentralised approach with more transparency, security, efficiency, and reduced bureaucracy.
The EU is enthusiastic about blockchain technology and has plans to implement new technologies across various sectors. Authorities have advised that regulators should not be concerned about pre-emptive legislation or innovation being stifled due to the emergence of cryptocurrency and blockchain. Virtual currency is not considered legal tender by the EU and its legal status varies between jurisdictions.

In December 2013, the European Banking Authority (EBA) issued a *'Warning to Consumers on Virtual Currencies'*. The warning made clear the risks associated with holding, purchasing, and trading in virtual currencies. Notably, the EBA highlighted that the majority of exchange platforms are unregulated and vulnerable to bankruptcy and hackings. Moreover, there are no protections for refund rights under EU law when using virtual currencies as a means of payment for goods or services, or when making transfers from traditional banks, making it unlikely that unauthorised withdrawals or credits from the digital wallet could be reversed. The EBA also stated that virtual currencies are highly volatile due to the absence of a central authority or institutional capital underpinning a currency. The fluctuation of prices could therefore enable short term investments while simultaneously causing significant losses and instability. This demonstrates the clear differences between exchange platforms and financial institutions. For example, if an exchange platform loses assets or collapses, there are no legal protections or guarantees. Furthermore, global regulators have expressed concerns regarding virtual currency and its capacity to enable money laundering and the financing of terrorism. Virtual transactions are extremely difficult to trace due to consumer anonymity thereby providing opportunistic users with an platform to carry out illicit activities.

The EBA published a report on the impacts and risks associated with virtual currencies in July 2014. The *'EBA Opinion on Virtual Currencies'* defines virtual currency as *"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."* The report documents several benefits of using virtual currencies. First, the absence of financial intermediaries provides lower costs for virtual currency transactions due to the lack of regulatory requirements. Exchange fees are also not applicable to virtual currency conversions. This clearly offers cost saving alternatives and provides competition for exchange services and traditional banks. Nonetheless, this cost reducing benefit in less effective for countries within the Single Euro Payments Area (SEPA). The SEPA is the EU's payment integration initiative which simplifies bank transfers in euros. Virtual currency provides commercial competition to conventional payment services and their established business agents. The decentralised nature of virtual currency means that innovative developments are possible. The EBA's report also lists different risks for consumers: fraudulent activities; losses when exchanging virtual currency

against fiat currency; fluctuations in the value of virtual currency; and unexpected tax requirements. The report proposed a regulatory framework including features of customer due diligence (CDD), accountability, and transparency in price formulation.

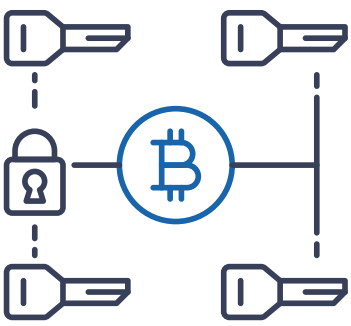
In October 2012, the ECB published a report *'Virtual Currency Schemes'* which defined and classified virtual currency and shed light on the benefits and risks arising from its use. In February 2015, *'Virtual Currency Schemes – A Further Analysis'* (a collaboration between the central banks of the Eurosystem), was published which provides greater detail on the initial 2012 report. In particular, the 2015 report addresses the legal ambiguity of virtual currencies. For example, the lack of regulations restricts legal protection for consumers which in turn exacerbates the risks. The absence of legal responsibility and regulated activities can have an impact on legitimacy and initiate unforeseen complications with contracts, thereby creating additional costs. Some jurisdictions have introduced regulations and implemented strategies to mitigate risk. However, the report suggests that these approaches have not eliminated actual risks but have instead compelled practices to circumvent such risks. Most losses occur due to fraudulent activities made possible as a result of anonymity and bankruptcy due to lack of compensation mechanisms. Moreover, because bricks and mortar financial institutions are monitored, consumers imagine that virtual currency schemes are regulated in a similar way. The report found that comparisons between virtual currency and electronic payments fuelled confusion as many consumers assumed that the same procedures were used for virtual currency. It is clear that key issues need to be addressed in order to reduce illicit activities.

The 5MLD came into force on 10 January 2020 and made requirements of users of virtual currencies. A list of specific users was identified who are accountable under the scope of the Directive. These users include the following: virtual currency and custodian wallet providers; art traders (if the value of transactions exceeds EUR 10,000); some auditing services; external accountants and tax advisors; and estate agents acting as intermediaries for property letting (if the value exceeds EUR 10,000). The 5MLD requires firms to ensure their existing structure replicates the new controlled framework. The directive also applies Customer Due Diligence (CDD) measures on non-reloadable electronic payment instruments that maintain a monthly transaction limit of EUR 150. Remote payment transactions with an amount of EUR 50 or higher are also subject to CDD. Therefore, this provision requires electronic money licence holders to implement the new policy changes. Member states and international organisations are also obliged to keep an up-to-date lists of prominent public functions and politically exposed persons. CDD and Enhanced Due Diligence (EDD) are both common features of the 5MLD. Identification and verification of consumers are crucial and should be supported with reliable and legitimate documentation. EDD measures are required for high risk countries. However, individual firms are able to determine their unique criteria and procedures, and an electronic identification system must be implemented. Last, firms should share information and electronic data with Financial Intelligence Units (FIU) and other relevant authorities in order to report suspicious transactions and fraudulent activities.

The Sixth Anti-Money Laundering Directive (6AMLD), known as Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law, came into effect on 3 December 2020 and must be implemented by institutions before 3 June 2021. This revised law strengthens provisions from previous directives and grants authorities more power to prevent money laundering and terrorist financing activities. The 6AMLD also provides stricter, punitive measures for offenders. The 6AMLD significantly harmonises the definition of money laundering across member states in order to remove ambiguities between domestic legislations. For example, a synchronised list of the 22 predicate offences (including cybercrime) is documented in the 6AMLD. Firms will have to adjust their policies to adapt to the new risks while updating internal strategies to mitigate any offences. Furthermore, the scope of the regulation has been extended to include *"aiding and abetting"* which includes anyone who takes part in these offences. At present, the 5MLD holds individuals accountable for money laundering whereas the 6AMLD extends criminal liability to legal entities such as corporations. This extension provides a global effort to mitigate illicit activities and helps relevant bodies focus their attention on companies that fail to comply with AML/CFT regulations. Furthermore, the 6AMLD specifies a four year minimum prison sentence for money laundering offences and judges have been granted the power to execute monetary penalties and prevent offenders from accessing public funding. In essence, EU member states should criminalise other predicate offences such as terrorism, drug trafficking, human trafficking, sexual exploitation, and corruption, in an attempt to centralise legal proceedings within a single jurisdiction. The 6AMLD also provides guidance for prosecutions which includes the victim's country of origin, the nationality of the offender, and the jurisdiction in which the offence took place. In summary, the 6AMLD has widened the regulatory scope with member states to combat money laundering and terrorist financing. The Directive (EU) 2018/1673 focuses on the particularities of these crimes and their sanctions while deploying a stricter monitoring and supervision initiative.

Malta

Malta is the first jurisdiction to adopt an innovative approach to the regulation of cryptocurrencies. Three pieces of legislation were put in place in July 2018: Malta Digital Innovation Authority Act (MDIA); Innovative Technology Arrangements and Services Act (ITAS); and Virtual Financial Assets Act (VFAA).



Malta is the first jurisdiction to adopt an innovative approach to the regulation of cryptocurrencies. Maltese authorities have recognised the economic potential of DLT (Distributed Ledger Technology) and appointed the Parliamentary Secretariat for Financial Services, Digital Economy and Innovation, and Malta Financial Services Authority (MFSA) to devise an organised regulatory framework for cryptocurrencies. Malta is recognised as the central hub for the gaming and cryptocurrency industry. The main driver for the Maltese government was to add legal certainty for investors in a well-regulated environment. Consequently, authorities were determined to create an effective legislative framework that collectively enabled the technical characteristics of blockchain activity to succeed. Because the enactments seek to create an approach to materialise opportunities it is likely that users of cryptocurrency in Malta will take the lead in the blockchain industry as legal certainty and protective measures enhance marketability.

Three pieces of legislation were enacted in July 2018: Malta Digital Innovation Authority Act (MDIA); Innovative Technology Arrangements and Services Act (ITAS); and Virtual Financial Assets Act (VFAA). The MDIA grants powers both to regulate and stimulate the development of innovative technologies. 'Innovative technology services' have been classified under the Second Schedule of the ITAS Act as: *"the review or audit services referred to in this Act with reference to innovative technology arrangements provided by system auditors; the technical administration services referred to in this Act with reference to innovative technology arrangements provided by technical administrators."*. The authority itself is responsible for promoting innovation and mediating between relevant institutions and authorities. The role of the MDIA is to ensure that standards and procedures are accordingly followed for the protection of service providers and consumers in order to maintain the integrity of the financial system. The MDIA's main objectives are to facilitate practices in line with the legal criteria and enforce the implementation of standards. This strategy will secure the stability of the blockchain market and ensure legal certainty of relevant activities in Malta. Therefore, it is clear that Malta has attempted to stabilise cryptocurrency regulations by simultaneously prioritising consumer protection and promoting the development of new technologies.

Cryptocurrencies will be regulated either by Malta's existing financial legislature or the VFAA, depending on the type of asset involved. The financial regulatory framework also includes the Markets in Financial Instruments Directive II, which is EU legislation that regulates institutions offering a service related to financial instruments.[28] The Second Schedule of the Investment Services Act and the Financial Institutions Act both provide further details on financial instruments. The financial instrument includes devices which are transferable in the marketplace:

a) *shares in companies and other securities equivalent to shares in companies, partnerships or other entities, and depository receipts in respect of shares;*

b) *bonds or other forms of securitised debt, including depository receipts in respect of such securities;*

c) *any other securities giving the right to acquire or sell any such transferable securities or giving rise to a cash settlement determined by reference to transferable securities, currencies, interest rates or yields, commodities or other indices or measures.*

It also includes instruments that are managed on the financial market, for example, *"treasury bills, certificates of deposit and commercial papers and excluding instruments of payment"*. The VFAA introduces a regulatory system that classifies DLT assets and relevant services

in their own right. The four categories of DLT include: electronic money; financial instruments; virtual tokens; and virtual financial assets. Other services include Initial Virtual Financial Asset Offerings (IVFAO) and Virtual Financial Asset Exchanges (VFAE).

The MFSA adopted the Financial Instrument Test (July 2018) to establish into which regulation a DLT asset fits. The test is used to classify DLT assets and is conducted on a case by case basis by VFA Agents – designated gatekeepers to the MFSA – to ensure regulations are adhered to in relation to IVFAO and VFA exchanges. The supervisory body is expected to act as an intermediary by reporting suspicious transactions and tracking transfers. VFA Agents are credible sources to help eradicate the manifest risks and are accountable to the MFSA. The test is applicable in following instances:

a) *issuers offering DLT Assets to the public in or from within Malta,*

b) *Persons providing any service and/ or performing any activity, within the context of either the VFA Act or traditional financial services legislation, in relation to DLT Assets whose classification has not been determined for any reason whatsoever, including inter alia because the offering of the said DLT Asset was conducted abroad.*

The purpose of the test is to qualify the DLT asset either as *(i) electronic money as defined under the Third Schedule to the Financial Institutions Act, (ii) a financial instrument as defined under the Second Schedule to the Investment Services Act, (iii) a VFA or a virtual token as defined under the VFAA*. If the DLT asset is a virtual token it is considered outside of the scope of the regulation because a virtual token does not have a value beyond its given platform. Notably, virtual tokens generally reflect utility tokens. Secondly, the test will determine whether the DLT asset amounts to a financial instrument under the MiFID II and the Investment Services Act. Security tokens are generally regulated under local financial legislation. The final stage concludes that if the DLT asset has not been classified in the previous categories then the financial instrument will fall within the scope of the VFAA. This test is convenient as it distinguishes between the different types of DLT assets available. In instances where the DLT asset is defined as a VFA, the service provider will be subject to the conditions stipulated in the VFAA. Namely, issuers of a IVFAO (Initial Virtual Financial Asset Offering) must register a white paper with the MFSA and adhere to the provisions noted in the First Schedule of the VFAA. The white paper must contain key information about the nature of the issuer, the VFA offered to the public, and a summary of essential information in relation to the offering.

According to the Global Legal Insights Report, Blockchain & Cryptocurrency Regulation 2020, Malta currently has no direct tax legislation applicable to cryptocurrencies; however, general tax principles apply to transactions involving cryptocurrencies across the Value Added Tax Act (Chapter 406) and the Duty on Documents and Transfer Act (Chapter 364). In November 2018, the Commissioner for Revenue issued *Guidelines for the VAT Treatment of transactions or arrangements involving DLT assets*. The guidelines make a clear distinction between coins and tokens, with coins referred to as assets using DLT as a means of payment, a medium of exchange and a store of value which do not resemble securities. Tokens are divided into financial tokens and utility tokens. Financial tokens are those assets using DLT which resemble securities, equities, or some form of financial instrument; on the other hand, utility tokens are assets using DLT where the value of the token is limited exclusively to the purchase of goods or services. For each transaction, the following considerations must be taken into account: the nature of the transaction, the position of the parties, and any other special circumstances.[29] The establishment of a distinct legal framework has placed Malta in the lead of the regulatory space for cryptocurrencies. However, confirming the legal status of cryptocurrency in its early stages of development can cause regulations to collapse if they are unable to adapt to the changes. The upcoming innovation in Malta could be restricted even though the government is aiming for a flexible approach which puts technology first. These new regulations could limit economic prosperity to the present conditions and it may be difficult to adjust to the global economic challenges ahead. However, based on its current track record Malta has been able to provide competent legislation around the growth of cryptocurrencies.

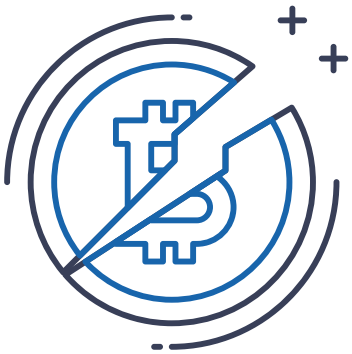
Malta's AML/CFT regime derives from the Prevention of Money Laundering Act (Chapter 373) (PMLA) and the Prevention of Money Laundering and Funding Terrorism Regulations (Subsidiary Legislation 373.01) (PMLFTR). Both pieces of legislation have made amendments to incorporate the Fifth EU Money Laundering Directive (5MLD) which came into force January 2020. Individuals partaking in a relevant financial business or activity will be subject to the stipulations under PMLA and PMLFTR. Regulation 2 of the PMLFTR states, *"subject person" means any legal or natural person carrying out either relevant financial business or relevant activity.* The PMLA provides the foundation for basic legal principles, administering protocols for assessment, and prosecution of ML/TF offences. It grants powers and procedures for the Financial Intelligence and Analysis Unit (FIAU) to carry out regulatory provisions on subjects during the course of their commercial activities. For example, VFA issuers, licence holder, and agents will be obliged to abide by the FIAU's guidance. For the purposes of an IVFAO, a white paper including a report of the AML/CFT procedures must be registered with the MFSA. It is mandatory for subject persons to carry out risk assessments and customer due diligence procedures throughout their dealings. On te other hand, the PMLFTR includes several amendments, while expanding the list of subject persons

The MFSA aims to produce a long term strategy to accelerate growth in innovation and ensure consumer protection.

and enhancing the stipulations regulating corporate organisations. A range of supervisory, monitoring, and disciplinary powers are also granted to ensure consumer protection. In regards to ownership and licensing, the Second Schedule of the VFAA requires service providers 'in or from within' Malta to obtain a licence. The statement *'in or from within Malta'* has not been given clarification but can be interpreted to mean the service providing a VFA from an entity within Malta, or services provided to members in Malta. Exemptions may be available under the Virtual Financial Asset Regulation (Subsidiary Legislation 590.01), where service providers may be exempt from obtaining a licence. For example, individuals dealing on their own account and in their own name rather than providing a service.

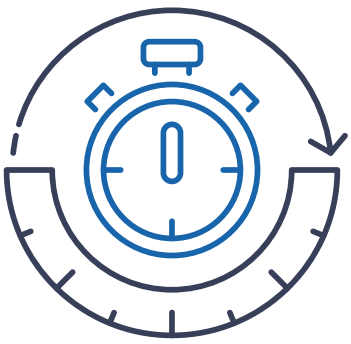
Although Malta is not a member of the Financial Action Task Force (FATF), it participates in MONEYVAL, a committee contributing to the evaluation of AML/CFT measures. Following the consultation document The Fifth Round Mutual Evaluation Report (July 2019), the assessment team voiced their concerns that national authorities did not entirely recognise the risks of ML/TF. A series of amendments to the PMLFTR came into force in May 2020, following a discussion issued by the FIAU in April 2020 reflecting concerns from the Fifth Round Mutual Evaluation Report. The changes issued by the Legal Notice 214 of 2020, sought to add clarification to the legal frameworks navigating AML/CFT. Regulation 15(3) and Regulation 15(7) were amended to adjust the time frame for reporting suspicious transactions to the FIAU, as the previous 5 working day strategy was not adequately prompt. Regulation 21(2) highlights that penalties issued by the FIAU should be balanced and active. Regulation 21(7) grants more powers to the FIAU to execute sanctions on individuals. Regulation 8(5) has been altered to reflect strict identification requirements where transactions are prohibited from processing until verification procedures have been executed: such instances should be reported to the FIAU immediately. Changes to Regulation 11(3) specify that subject persons are required to obtain adequate information about the institution in question, including the nature of the business, status, and quality of the organisation. Regulation 11(6)(b) states that if beneficiaries or beneficial owners are politically exposed persons, the subject person must file an admission to the FIAU. Last, Regulation 12(2)(b) advises that subject persons should not rely on intermediaries or third parties from regions that signify a high risk of ML/TF.[30]

Malta has launched an array of regulatory testing. The Malta Gaming Authority Sandbox (March 2018) released guidance on the use of virtual currency within the gaming environment, with the aim of examining the adoption of DLT in the gaming and gambling sector. Furthermore, the MFSA Vision 2021 (January 2019) and Fintech Regulatory Sandbox are both attempts to strengthen the organisation of this innovative financial sector. Vision 2021 containssix key areas including regulation; ecosystem architecture; international links; knowledge; and security. The MFSA aims to produce a long term strategy to accelerate growth in innovation and ensure consumer protection. The MFSA has arranged support for initiatives in active financial institutions whereby institutions have been permitted – under supervision – to test innovative products and services in order to assess the capacity of innovative financial archetypes for both investors and the financial sector as a whole. Fintech's Regulatory Sandbox aims to assist the regulatory viability of innovative financial products to expand on mechanisms that will help the MFSA to achieve market integrity and eliminate risks.



Poland

The growth of the cryptocurrency industry is relatively contingent on the legal principles provided by individual jurisdictions. At present, the Polish legal system does not prohibit exchanges in cryptocurrencies and they are therefore considered legal. However, Poland does not consider cryptocurrencies as legal tender.



Polish regulators have taken a relaxed approach and have no specific legislation regulating cryptocurrencies apart from what is contained in the Act of 1 March 2018 on Counteracting Money Laundering and Terrorist Financing (AML Act). The act provides a definition for virtual currencies as *"a digital image of values other than:*

a) a legal tender issued by NBP, foreign central banks or other public administration bodies,

b) an international unit of account established by an international organisation and accepted by individual countries belonging to this organisation or cooperating with it,

c) electronic money within the meaning of the Act of 19 August 2011 on Payment Services,

d) a financial instrument within the meaning of the Act of 29 July 2005 on Trading in Financial Instruments, e) a promissory note or a cheque; and which is exchangeable in business transactions to legal tender and accepted as the means of exchange as well as can be electronically stored or transferred, or can be subject to electronic trade." Although this definition does not categorise cryptocurrencies, it clearly distinguishes them from other types of financial exchanges.

The *"Statement by Narodowy Bank Polski (NBP) and the Polish Financial Supervision Authority (KNF) on virtual currencies"* was published in July 2017. The joint statement confirmed that virtual currencies are not issued by the central bank of Poland (NBP) and do not equate to fiat currencies. The statement also emphasises that virtual currencies are not regulated within the parameters of existing legislation, notably the Act of 19 August 2011 on Payment Services and the Act of 29 July 2005 on Trading in Financial Instruments. It was suggested that deeper exploration of emerging technologies was required before legal frameworks could be produced and financial markets could be revealed. Furthermore, the purpose of the statement was to express the risks associated with virtual currencies. For example, the paper gives examples of risks in relation to potential loss of funds due to theft and fraud. It also highlights that virtual currencies are not widely accepted or supported by the Central Bank. The paper clarifies institutions like the Office of Competition and Consumer Protection and the KNF do not have the powers to intervene in such circumstances, leaving investors to carry out their own criminal inquiries. Last, the statement lays out the risk of high price volatility of virtual currencies which can prompt significant price changes. The NBP and KNF have advised against trading in virtual currencies due to the associated risks and negative impact on investors and financial institutions. If persons do engage with virtual currencies they should be cautious and aware of money laundering and financing terrorism schemes. Any engagement should constitute a detailed examination of the legal implications and consumer outcomes. The statement ends with the necessity to distinguish between virtual currencies and distributed ledger technology (DLT) given that the authorities promote the development of blockchain activities.

Poland has not established specific legislation for the taxation of cryptocurrency. In September 2018, KPMG produced an article *'Tax Alert'* which explained the tax processes around cryptocurrencies in Poland. In August 2018, the Ministry of Finance proposed a Bill to amend the Personal Income Tax Act (PIT), Corporate Income Tax Act (CIT), and the Tax Ordinance Act (TO) (among other tax related regulations), because of the absence of adequate guidelines for the properties of cryptocurrency exchanges in existing legislation. The following amendments were enacted in January 2019. For the purpose of PIT, revenue from cryptocurrency trade is now included in capital gains, regardless of whether the tax payer acquires the revenue through business activities or not. Importantly, this reduced the taxation on revenues from

Poland has incorporated the European Union's Fifth Anti-Money Laundering Directive (5AMLD) into the Act of 1 March 2018 on Counteracting Money Laundering and Financing of Terrorism (AML Act).

cryptocurrency trading from rates of 32% to a flat tax rate of 19%. Likewise for CIT, the income from the cryptocurrency trade is also included in capital gains. Furthermore, taxpayers must record and equate revenue from cryptocurrency exchanges with real money. The amendment also proposed that cryptocurrency exchanges for other cryptocurrencies will be tax neutral, irrespective of the tax method. Furthermore, Poland does not violate any of the rules provided by European law, and upholds the ruling made by the Court of Justice of the European Union which means cryptocurrency exchanges and fiat currencies are exempt from VAT.

Poland has incorporated the European Union's Fifth Anti-Money Laundering Directive (5AMLD) into the Act of 1 March 2018 on Counteracting Money Laundering and Financing of Terrorism (AML Act). The Directive addresses methods to combat anti-money laundering and the financing of terrorism (AML/CFT) within the cryptocurrency market. Poland's AML Act has implemented stricter customer due diligence procedures, particularly against high risk countries. Also, cryptocurrency entities such as custodian wallet providers have been classified as *'obliged entities'* subject to registration or licensing requirements. The Polish AML Act reaffirms this through *'obligated institutions'* and now extends to businesses that engage in exchange services between virtual currencies and fiat currencies by way of the Directive. The AML Act provides a wider criteria for obligated institutions in comparison to the Directive and extends to businesses that facilitate:

a) exchange between virtual currencies and means of payment;

b) exchange between virtual currencies;

c) intermediation in the exchange referred to in letter a or b;

d) operating accounts referred to in paragraph 2(17)(e). In spite of this, the AML Act will have to adopt stricter financial security measures; for example, enhanced customer due diligence checks and reporting procedures to the Financial Intelligence Unit. This also includes record keeping and executing programs to mitigate ML/FT. The Directive also requires Member States to enforce registration or licensing obligations for businesses that engage in cryptocurrency services. However, cryptocurrencies are largely unregulated in Poland and this registration process does not exist. Furthermore, cryptocurrency does not constitute a payment service and consequently will not trigger a financial licence. Thus, Poland has not incorporated this provision and cryptocurrency entities are not obliged to register or obtain a licence. The 5AMLD requires Member States to generate a public register of the beneficial owners which must be regularly updated; Poland's Central Register of Ultimate Beneficiaries was initiated in October 2019.[31]

Poland is now motivated to regulate the crypto space and one example of upcoming legislation is built on the Sixth Anti-Money Laundering Directive (6AMLD). The Comply Advantage Report 2020 issues a paper on, *"The Sixth Anti-Money Laundering Directive: What You Need to Know"* detailing the changes involved from the transformation of the 5AMLD. The changes will be enacted by Member States on 3 December 2020 and must be employed by financial institutions by 3 June 2021. The 6AMLD reflects on its aims to deliver mitigating provisions to combat ML/TF and principles have been reconsidered in order to strengthen existing regulations. The 6AMLD prioritises the adoption of a unified definition across all EU Member States in an effort to avoid ambiguities within local legislation. The updated Directive will also harmonise enforcement strategies and provide a list of 22 'predicate offences' that should be treated as ML. The list includes tax evasion, environmental crimes, and extends to other cyber-related offences. Subsequently, changes within the Directive will prompt financial institutions to reorganise policies and procedures to facilitate the new risk system. Furthermore, 6AMLD extends criminal accountability under the definition of ML and adds *'aiding and abetting'* into the scope of criminal activity. Individuals who assist with ML activities will therefore be held liable for their conduct, while authorities should recognise actions of aiding and abetting to mitigate illicit activities. Furthermore, the 6AMLD redefines the penalties for offenders: for example, the minimum sentence of imprisonment

The "*Statement by Narodowy Bank Polski (NBP) and the Polish Financial Supervision Authority (KNF) on virtual currencies*" was published in July 2017. The joint statement confirmed that virtual currencies are not issued by the central bank of Poland (NBP) and do not equate to fiat currencies.

has been changed from one year to four years. Judges have also been granted powers to issue monetary fines and prevent persons from retrieving public funding. The purpose of such amendments is to create consistency between AML/CFT regulations across all EU regions. When dual criminality has occurred (when an offence has taken place in one jurisdiction and the proceeds of crime are situated in a different location) the 6AMLD proposes information exchange between countries to allow prosecutions in more than one place. Jurisdictions will also work collectively to integrate legal proceedings within a selected jurisdiction.

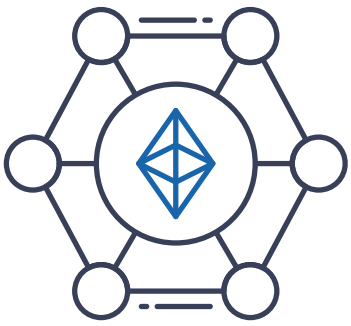
Poland has initiated the *'Special Task Force for Financial Innovation in Poland'* in collaboration with the KNF, Ministry of Finance, and the Ministry of Economic Development to respond to emerging technologies in the fintech market. The aim of the task force is to explore the regulatory dimensions of financial innovation and create a legal framework to prevent illicit activities. The report, issued in 2017, highlighted key concerns within the sector. For example, a lack of strategy and financial support for financial innovation and the lack of legal certainty were specified as issues. The objective of the task force was to initiate appropriate action to remove identified barriers and increase legal certainty. The group has worked towards establishing stability and transparency in the market and the regulatory landscape. The report reflects Poland's ambition to be at the forefront of financial innovation; however, authorities must establish operational solutions from an organisational perspective in order to create effective policies which support fintech departments. Moreover, the *'KNF Innovation Hub'* was produced to offer support to the development of fintech institutions. The program helps companies enter the financial market while upholding the integrity of the financial system and protecting consumers. The system distinguishes between different fintech institutions from start-ups entering the financial market offering a modern technological product or service to long established entities providing an innovative product or service: both will be accountable to the KNF. Consequently, this agenda shows a positive movement towards the regulation of the cryptocurrency market in Poland. Although activity from legislative bodies has been slow, new developments are on the horizon as risks have been identified and measures have been executed.

Lithuania

In 2017, the Bank of Lithuania implemented a similar definition of virtual currency used by the European Banking Authority (EBA). It defined virtual currency as, *"ungoverned and unregulated digital money, which may be used as a means of payment, but is issued into circulation and guaranteed by an institution other than the central bank"* which means that virtual currencies can have different purposes.

For example, these currencies can be used as a means of payment, savings, or investments (including securities and commodities). Virtual currencies are not considered legal tender in Lithuania. In 2018, the Ministry of Finance of Lithuania issued guidelines on initial coin offerings (ICOs), 'ICO Guidelines' in an attempt to provide legal certainty and transparency for the regulatory and taxation sectors. The guidance demonstrates that ICOs are not regulated by exclusive legislation and instead, depending on the characteristics and features of the coins/tokens, may be subject to existing Law on Securities of the Republic of Lithuania or financial legislation, under the scrutiny of the Bank of Lithuania. The applicable legislation will be determined by the rights attached and the conditions applied to the ICOs. The guidelines highlight service providers intending to offer or sell tokens which reflect the characteristics of securities or other regulated financial services under the supervision of the Bank of Lithuania. Nevertheless, a Financial Market Participant (FMP) can provide a service in relation to virtual currencies so long as there is a clear distinction in the services supplied by the FMP. It is therefore fundamental for FMPs to ensure their regulated financial services (including names, domains and other commercial attributes) are not connected to the services associated with virtual currencies. Furthermore, FMPs are obliged to fulfil the requirements around anti-money laundering and countering the financing of terrorism (AML/CFT).

With regard to the taxation of virtual currencies, the State Tax Inspectorate published a consultation paper *"Virtual Currency and ICO Taxation in Lithuania"* in January 2019. The paper illustrates that the tax treatment of virtual currencies is determined by the purpose of the currency itself. The Law on Corporate Income Tax stipulates that through the substance and economic activity of the transactions, a virtual currency is recognised as assets which can be used as a means of payment for goods and services or held for sale. For VAT purposes, a virtual currency should be treated as a regular currency such as euros or dollars. Taxable transactions are applicable to selling, purchasing, payment using virtual currencies for purchased or sold goods or services, and mining. However, there is no legislation determining the exchange rate of virtual currencies against fiat currency and therefore, relevant market information and data may be used to determine the exchange rate. For the purposes of Corporate Income Tax the production of virtual currency is not taxable but any profit gained from selling the virtual currency is taxable. With personal income tax virtual currencies are treated as property and income gained from the sale of virtual currency is taxable. Significantly, virtual currency or any other digital assets involved should not be treated as personal income; the taxation of personal income arises during the sale of virtual currencies. From 1 January 2018, individual income will be based on the amount of income received from the sale and purchase of virtual currencies at a personal income tax rate of 15%.



For the purposes of Corporate Income Tax mining of virtual currency is not taxable but any profit gained from selling the virtual currency is taxable. With personal income tax virtual currencies are treated as property and income gained from the sale of virtual currency is taxable.

It is clear that Lithuanian authorities will be working towards future legislation in order to establish a stable regulatory framework for virtual currencies.

As noted above, FMPs must comply with AML/CFT protocols and procedures to manage the risks associated with virtual currencies. The nature and characteristics of the virtual currency in question will determine the relevant applicable legislation. The *ICO Guidelines* make a distinction between two types of ICOs in light of their purpose. Namely, *"ICOs that do not grant profits or government rights"*, state that if an ICO has rights attached to use goods or services, the application of the Civil Code of the Republic of Lithuania would take effect. If an ICO is used as a payment instrument or considered a charity, the Law on the Prevention of Money Laundering and Terrorist Financing would apply.[32] On the other hand, *"ICOs that grant profits or governing rights"* demonstrates that ICOs which issue coins reflecting the characteristics and attributes of securities will be subject to the Law on Securities. The guidance also specifies that if ICOs are used in crowdfunding the Laws on Crowdfunding will be apply. Moreover, the Law on Markets and Financial Instruments is the relevant legislation to use if an ICO is used as a financial instrument or engages in secondary trading. Therefore the purpose and nature of the ICOs may trigger various existing legislations to be consulted in Lithuania. At present, the ICO Guidelines suggest regulators are currently updating the AML/CFT legislation in order make adaptations for virtual currencies. Therefore, until revisions have been made, the guidelines suggest that FMPs involved with cryptocurrency setups should follow the existing AML/CFT legislation.

It is clear that Lithuanian authorities will be working towards future legislation in order to establish a stable regulatory framework for virtual currencies. The Bank of Lithuania has been actively working towards a digital, blockchain based collector coin known as 'LBcoin'.[33] It was released on 23 July 2020 to commemorate the country's Act of Independence. The Central Bank has emphasised the rapid growth of financial technologies and this represents a strategic move towards innovation. LBcoin allows residents of Lithuania and financial institutions to explore the technologies in a regulated environment. It also allows the Bank of Lithuania to understand how the issuance of a digital currency from a central bank can open up new avenues for the community as a whole.

Switzerland

The Swiss government has taken a progressive approach towards virtual currency, and both the Federal government and the Swiss Financial Market Supervisory Authority (FINMA) acknowledge the valuable impact that blockchain technology could have on the economy. Authorities are keen to welcome emerging technologies and take the global lead in this industry and consequently virtual currencies are legal in Switzerland, although they do not constitute legal tender.

In December 2018 the Swiss Federal Council issued a report on the relevant legal framework for blockchain and distributed ledger technology (DLT). The report highlighted that the nation's current legal framework provides a sufficient foundation for the regulation of new technologies. Nonetheless, authorities have recognised areas of improvement in relation to the financial market. The Swiss Federal Council has also initiated consultations for refining the framework conditions of blockchain and DLT. The DLT Draft Law, *'To Adapt Federal Law to Developments in the Technology of Distributed Electronic Registers'*, was issued in March 2019. Swiss law does not currently provide a definition for virtual currency although the federal government has provided a definition in its *'Federal Council Report on Virtual Currencies in Response to the Schwaab (13.3687) and Weibel (13.4070) Postulates'* issued in June 2014 and is here described as *"a virtual representation of a 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 – it is not accepted as legal tender anywhere (...) Virtual currencies exist only as a digital code and therefore do not have a physical counterpart for example in the form of coins or notes. Given their tradability, virtual currencies should be classified as an asset."* FINMA used the same definition in the revision of the Anti-Money Laundering Regulations. In February 2018, FINMA provided *'Guidelines for Enquiries Regarding the Regulatory Framework for ICOs'* (ICO Guidelines). This report presented three categories of tokens and their classifications. The same description of virtual currency was used by the Federal Council in its report on delivering the DLT Draft Law. For example, 'payment tokens' can be used like money to obtain goods or services; these tokens have no rights attached to them to make claims against an issuer or a third party. In essence, payment tokens are recognised as intangible assets and represent cryptocurrencies similar to bitcoin. On the other hand, 'utility tokens' are used to provide digital access to an application or service through DLT. Furthermore, 'asset tokens' represent assets in a debt or equity financing claim against the issuer. According to FINMA, asset tokens also allow physical assets to be traded with blockchain technology. However, FINMA has highlighted the possibility that some tokens fall outside the scope of these three categories and that another category ('hybrid tokens') can comprise elements of two types of tokens.

Virtual currency activities are permitted in Switzerland and are contingent on the approval of the DLT Draft Law but there are no statutory frameworks which explicitly regulate virtual currency. The DLT Draft Law has introduced the concept of 'DLT rights' which proposes that rights are attached to tokens, financial instruments, shares, and derivatives. DLT rights advocates the tokenisation of rights through a legal framework for an electronic registration of rights. For example, contractual claims and membership rights fall within the scope of DLT rights. Asset tokens therefore have the necessary elements to constitute a DLT right; however, payment tokens for which claims cannot be made against the issuer would not qualify for DLT rights. With regard to the sale or tradability of virtual currencies such transactions will be regulated if the token qualifies as a security under the Financial Markets Infrastructure Act (FMIA). Article 2 of FMIA stipulates that securities constitute *"standardised certificated and uncertificated securities, derivatives and intermediated securities, which are suitable for mass trading"*. Apart from in the ICO Guidelines where FINMA suggested that virtual currencies would not generally be treated as securities, there are no clear laws to indicate whether tokens are securities. Therefore, each token will be determined on a case-by-case basis in line with the existing guidance provided by FINMA.

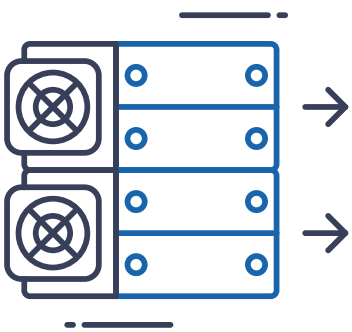
FINMA does not consider virtual currency to constitute securities because virtual currency holders do not have any rights upon

the issuer or third party. Virtual currency is used as a means of exchange and does not constitute a financial instrument under the Financial Services Act (FinSA). Utility tokens are not considered as securities by FINMA because they do not possess the full economic properties of an investment. Asset tokens can be treated as securities if it satisfies the definition provided in Article 2 of FMIA. Nevertheless, tokens that constitute securities can activate Swiss securities dealer licence requirements under the Federal Stock Exchanges and Securities Trading Act (SESTA), Swiss trading platform regulations under FMIA, and Swiss prospectus requirements. Individuals trading in security tokens on behalf of clients for business purposes may be required to obtain a securities dealer licence. Cases where asset tokens are issued which are connected to shares need to be administered by a regulated securities dealer.[34] The DLT Draft Law presents a new licensing category named DLT Trading Venue under the FMIA. The DLT Trading Venue will be licensed and authorised to offer services in the trading, clearing, settlement, and custody of DLT securities. At present, the DLT Trading Venue licence requirements reflect the existing requirements for trading venues. However, the Swiss government and the FMIA intend to deliver specific policies for DLT Trading Venue in relation to DLT securities.

In August 2019, the Federal Tax Administrator (FTA) published a paper on the tax treatment of cryptocurrencies for wealth, personal, and corporate income tax. The FTA provides end of year conversion rates for cryptocurrencies into Swiss francs. There are different tax authorities in the region some of whom consider cryptocurrency to be assets, similar to bank deposits, and are correspondingly subject to wealth taxes. If the FTA does not offer an end of year market value, the cryptocurrency must declare the end of year price of the trading platform where transactions were processed. It is common that individuals are relieved from capital gains income tax on cryptocurrency assets. However, when cryptocurrencies form an asset which contributes to the business assets, the capital gains will be subject to income tax. Consequently, FTA is working towards developing a framework for the tax treatment of cryptocurrency in line with the growth of this technology.

The primary legislation governing anti-money laundering and countering the financing of terrorism (AML/CFT) is the Anti-Money Laundering Act (AMLA) and the Anti-Money Laundering Ordinance (AMLO). The AMLA can be applied to financial intermediaries, supervisors, and persons that accept, hold, or deposit assets on the behalf of others in a business capacity under Article 2 (3) AMLA. The AMLA includes a list of activities that are considered financial intermediation which – for ICOs and Initial Token Offerings – specifies that when the issuance of means of payment are not to be used exclusively with the issuer, transmission services, money exchange services and financial intermediation services. In the context of the AMLA, a financial intermediary will have to be associated with an authorised AML self-regulatory organisation (SRO). Additionally, a financial intermediary must comply with the requirements stipulated under the AMLA, including the Customer Due Diligence (CDD) and Know Your Customer (KYC) procedures. All suspicious transactions must be reported to the Money Laundering Reporting Office to mitigate terrorist financing. FINMA clarifies its ICO Guidelines by stipulating that and states contingent on the classification of tokens within an ICO, can qualify as a financial intermediary action. The issuance of utility tokens that maintain elements of a payment function on a particular platform, where the utility tokens to pay for services used on that platform qualifies as a means of payment and constitutes a financial intermediary action. However, this is not the case if the utility token does not have any payment functions.

In summary, Switzerland is working towards adopting a detailed DLT Bill which will initiate DLT Rights as a new category representing rights that can be registered and exercised against the issuer or third party. The aim of DLT rights is to create the digital equivalent of certificated securities. The rights that can be issued as certificated securities can be issued as DLT rights. For example, *"(i) fungible contractual claims (e.g., debt claims); (ii) non-fungible contractual claims (e.g., rights arising from a licence agreement); (iii) membership rights that can be issued as certificated securities (e.g., rights of shareholders of joint-stock corporations); and (iv) rights in rem that can be issued as certificated securities (e.g., mortgage certificates)."* Nonetheless, DLT rights are not applicable on cryptocurrencies or similar tokens that do not represent any rights against the issuer or third party, or property rights and transportable assets.



The Americas

United States

Cryptocurrency regulations are not wholly consistent across the United States (US) for those making transactions in virtual currencies. Virtual currency transactions are generally regulated across the US jurisdiction if the sale can qualify as securities or satisfy money transmission requirements.

Various state governments have enacted legislation to regulate cryptocurrencies and have either endorsed positive regulations relieving cryptocurrency from security laws, or have issued warnings restricting investment in cryptocurrencies. Dominant regulatory systems adopted by the US States include the New York 'BitLicense' and the 'Blue-sky laws', which pertain to dealings in digital asset securities. On the other hand, federal security laws are applicable to digital assets that constitute a security risk, meaning that entities must satisfy the relevant requirements under the Securities Act 1933 (SA). Cryptoassets which constitute a commodity are subject to the Commodity Exchange Act (CEA). To regulate this space the federal government has enlisted the assistance of the following authorities: Securities and Exchange Commission (SEC); Commodity Futures Trading Commission (CFTC); Federal Trade Commission (FTC); Financial Crimes Enforcement Network (FinCEN); Office of Foreign Asset Control (OFAC); US Treasury Department; Internal Revenue Service (IRS); and the federal banking regulators. Although federal policymakers are exploring fintech in greater depth, there has been no explicit legislation created to exclusively regulate virtual currency. Regulators have recognised the dangers of pre-emptive legislation and have opted for an approach focused on technological developments. According to the Comply Advantage Report 2020, virtual currencies are not treated as legal tender in the US; however, dealings in certain jurisdictions in 2013 were considered as money transmitters since tokens are *"other value that substitutes for currency"*.

Federal security laws are applicable to digital assets that constitute securities and the SEC is the primary regulator of the sale of such securities. Section 2 of the SA stipulates that an investment contract amounts to a security, which was defined in the US Supreme Court judgement of Securities and Exchange Commission v. W. J. Howey Co (1946). The definition established the 'Howey Test' which determines whether a transaction amounts to an investment contract, *"an investment of money in a collective enterprise with a reasonable expectation of profits derived from the entrepreneurial or managerial efforts of others."* Therefore, in order to regulate virtual currencies or digital assets in compliance with securities legislation the digital asset needs to constitute an investment contract. The SEC examines the substance of the transaction rather than its form in order to determine the nature of the digital asset. Transactions that constitute securities will be subject to disclosure and registration provisions stipulated in Sections 4 and 5 of the SA. However, market professionals could avoid certain aspects of the Howey Test in an attempt to escape securities legislation: for example, this may apply in situations where there is no return on investment and instead the coin/token holder intends to use the tokens as a means of purchasing goods or services. Furthermore, if the holder's anticipation of profits did not depend on the efforts of others and instead relied on their own effort to generate a return on investment, this caveat may also be applicable. The SEC has addressed this issue through the *'Chairman's Testimony on Virtual Currencies: The Roles of the SEC and CFTC'* published in February 2018. This clarified the position of ICOs in the context of federal securities laws that simply labelling or structuring a token to reflect 'utility' characteristics does not make it exempt from securities regulations. Consequently, tokens featuring promotions that highlight the potential profits from the efforts of others stimulates properties of securities.

In June 2018, the Director of Corporation Finance made a speech entitled, *'Digital Asset Transactions: When Howey Met Gary (Plastic)'*. In the speech the Director addressed the question of whether digital assets that were initially offered as securities could later be sold as non-securities. When rights are attached to the digital asset it provides the holder with an economic interest in the enterprise which cannot be later

Regulators have recognised the dangers of pre-emptive legislation and have opted for an approach focused on technological developments. According to the Comply Advantage Report 2020, virtual currencies are not treated as legal tender in the US; however, dealings in certain jurisdictions in 2013 were considered as money transmitters since tokens are *"other value that substitutes for currency"*.

sold as a non-security. In such situations merely labelling the transaction as an Initial Coin Offering (ICO) will not mean it is not applicable to securities regulations since the *"economic substance of a transaction determines the analysis, not the label"*. However, if there is no central enterprise for investment, or the digital asset is used for purchasing goods or services through the network it was created on, it could later be sold as a non-security.

In April 2019, the SEC published a public statement on 'Framework for 'Investment Contract' Analysis of Digital Assets'. The statement highlighted the SEC's Strategic Hub for Innovation and Financial Technology (FinHub) and created a framework to determine whether a digital asset constitutes an investment contract and thereby a security. This framework provides a useful guide to determine whether dealings of digital assets fall within the scope of the securities definition under US federal law; it does not represent a complete legal summary. The framework provides a detailed structure of the application of the Howey Test and other relevant considerations such as the economic reality of the transaction. This helps authorities decide if the digital asset is being sold and offered for the holder's use or consumption. The framework also illustrates features and characteristics of 'use' or 'consumption' that potentially renders the Howey Test unfulfilled. For instance, holders of a digital asset can immediately use it for its intended function, the digital asset's structure is designed to fulfil the requirements of its users rather than to instigate speculation on its value. Therefore, the digital asset can only be used on the given network and traded within the amount that resembles a purchaser's expected use. Furthermore, the increase in value for a digital asset is restricted. For example, the creation of the digital asset maintains a constant value or eventually reduces so that it cannot be used as an investment for a lengthy duration. Also, digital assets that are associated with virtual currency can be directly used as payments in various circumstances or used as a substitute for fiat currency. Subsequently, digital assets that emphasise these characteristics are unlikely to constitute an investment contract. Ultimately, the framework clarifies features for market participants to consider when determining the nature of a digital asset. The highlighted factors are not determinative and should be used as additional guidance. The framework does not replace existing legal requirements or previous statements provided by the SEC.

The SEC also published its first 'no-action letter', *'Response of the Division of Corporation Finance'*, in April 2019. The letter explained that the SEC would not conduct enforcement actions against the sale of TurnKey's Jet Inc. (TJK) digital tokens. The SEC confirmed that TJK's tokens did not constitute securities and provided a number of points reflecting on elements of the Framework for Investment Contract Analysis of Digital Assets. Importantly, no-action letters are only applicable to the addressees and are not binding on others, particularly because the letter contains a concise list of facts.[35] Nevertheless, where a digital asset amounts to a security the issuer must register the security with the SEC unless exempted. Section 3 of the SA demonstrates the exemptions available and remains more lenient on the sale of securities to accredited investors. Furthermore, alongside federal security laws, the majority of the US States have other regulations that are applicable to digital assets. These regulations are known as 'Blue-sky laws' which provide structure and supervision of offers and sales of securities and differ between states. The exemption from certain requirements under federal security laws does not prevent the application of Blue-sky State laws provided by the National Securities Markets Improvement Act 1996.[36]

There are other requirements that need to be considered when a token constitutes a security. The SEC's Division of Trading and Markets and Division of Enforcement issued a *'Joint Staff Statement on Broker-Dealer Custody of Digital Asset Securities'* in July 2019 which discusses the need for market participants to ensure that registration requirements have been satisfied as imposed by the Securities Exchange Act (1934) (SEA) when trading in virtual currencies. Market participants should also acknowledge the classification of broker-dealers and Alternative Trading Systems (ATS). According to Section 15(a)(1) of the SEA, issuers that meet the definition of 'broker-dealer' (when conducting relevant digital asset securities activity) should be licensed with the SEC and

a registered member of the Financial Industry Regulatory Authority (FINRA) in order to facilitate the trade of securities. A securities broker is defined under the SEA as: *"any person engaged in the business of effecting transactions in securities for the account of others."* The Act also provides exemptions for this definition which are available to banks that are involved only in certain securities.

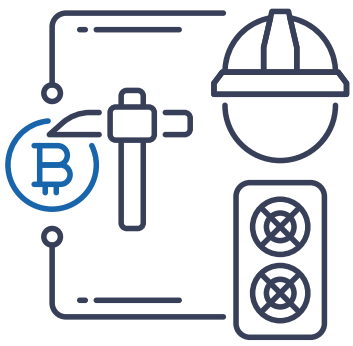
Many US states have adopted a wide array of regulatory approaches and have used the Uniform Regulation of Virtual Currency Business Act (URVCBA) for guidance. The URVCBA provides a statutory outline for the regulation of companies involved in virtual currency business activity. The act defines virtual currency as a digital representation of value that can be used as a medium of exchange, unit of account, or store of value but does not constitute legal tender. The URVCBA also stipulates any engagement with virtual currency business activity will require a licence. The Act defines virtual currency business activity as:

(a) exchanging, transferring, or storing virtual currency or engaging in virtual-currency administration, whether directly or through an agreement with a virtual-currency control-services vendor;

(b) holding electronic precious metals or electronic certificates representing interests in precious metals on behalf of another person or issuing shares or electronic certificates representing interests in precious metals; or

(c) exchanging one or more digital representations of value used within one or more online games, game platforms, or family of games for: (i) virtual currency offered by or on behalf of the same publisher from which the original digital representation of value was received; or (ii) legal tender or bank credit outside the online game, game platform, or family of games offered by or on behalf of the same publisher from which the original digital representation of value was received. The URVCBA also triggers additional requirements that uphold sufficient anti-money laundering and countering the financing of terrorism (AML/CFT) procedures in an attempt to avoid fraudulent and illicit activities.

The Bank Secrecy Act (BSA) is the central federal statutory framework regulating financial institutions to comply with AML/CFT procedures. Most federal authorities adhere to the provisions stipulated in the act; however, certain financial institutions that are not federally regulated are also required to register with FinCEN, uphold an AML/CFT risk-based approach, and maintain information sharing with FinCEN. In March 2013, FinCEN published *'Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies'* which included guidance to clarify the applicability of the regulations provided by the BSA to participants *"creating, obtaining, distributing, exchanging, accepting, or transmitting virtual currencies"*. FinCEN specified that a Money Service Business (MSB) should include a virtual currency exchange and nominate an administrator of a centralised source of a virtual currency who has the powers to issue and exchange the virtual currency, unless exempted. Any MSB that is a money transmitter must carry out a wide ranging risk assessment to devise AML strategies. For example, the MSB must include written policies and procedures to uphold compliance and allocate an officer for supervision and monitoring. The MSB must provide training for reporting, detecting suspicious transactions, and record keeping. Nationals who are included on the Specially Designated Nationals and Blocked Entities List (SDN List) from the US Treasury Department Office of Foreign Assets Control (OFAC) are not to be traded with by any US persons or entities. The OFAC also requires persons from the US jurisdiction to block assets of individuals and corporations which are engaged in transactions with blocked nationals, corporations that act on the behalf of such nationals, and individuals who act as agents for such nationals. Failure to comply with these stipulations allows the OFAC to impose civil and criminal penalties as stated in the 'Economic Sanctions Enforcement Guidelines in November 2009'. Arizona was the first US state to assemble a regulatory sandbox to explore fintech, blockchain, and virtual currency industries in greater detail. The sandbox provides regulatory relief for participating institutions which will allow them to develop new products and services with real market results. The program provides innovators with two years to test their products and engage with a maximum of 10,000 clients before having to apply for an official licence.



Canada

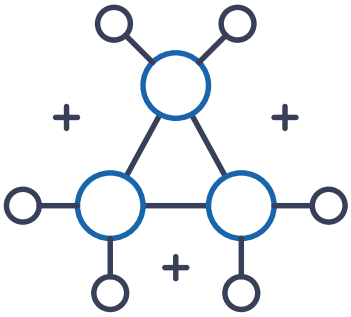
Canadian authorities' established cryptocurrencies are not treated as legal tender. Canada has not created new legal frameworks to govern the crypto space but has carefully expanded their existing securities legislation to accommodate cryptocurrencies. Canada's securities regulation is governed through legislation by the provincial governments and consequently each province has individual policies.

However, the provincial regulations have been largely harmonised across the country through national instruments. The Canadian Securities Administrators (CSA) organisation represents all the authorised securities regulators throughout the territories in Canada. Securities legislation can be used to administer various types of transactions and usually covers the distribution of securities. Securities regulation helps to manage the trading of securities through a catalogue of requirements including registration and information exchange. The federal government has made efforts, together with a selection of provincial authorities, to generate a co-operative securities regulatory system which is applicable nationwide. Draft legislation, Pan-Canadian Securities Regulation SCC 48, was published in 2018; however, a date for enforcement is yet to be confirmed.[37]

Canada's National Instrument 45-106 (NI 45-106) regulates the requirements for a prospectus and exemptions for the distribution of securities. The prospectus is a disclosure document detailing obligations for the protection of investors. Members involved in the distribution of securities are obliged to register with their local securities regulator and carry out other reporting procedures. Section 2.3(1) of NI 45-106 stipulates that businesses dealing in securities can trade with *'accredited investors'* when obtaining an entire security and that they will be exempt from the prospectus requirement.[37] Retail investors who do not fulfil the criteria for accredited investors can rely on the '*Offering Memorandum*' (OM) prospectus exemption. The prospectus includes information relating to the offering in question such as the final offering of the securities, its price, and background information on the business involved.

The CSA produced a staff notice *"CC Offerings"* (SN 46-307) in August 2017. This notice provided guidance on the application of existing securities legislation against cryptocurrency offerings. It delivers guidance on the direction financial technology (fintech) businesses should take when assessing whether Initial Coin Offerings (ICO) or Initial Token Offerings (ITO) are a distribution of securities. Although coins/tokens are not referred to as shares or bonds, they may still constitute a security under the definition provided by the securities legislation for the provinces of Canada. The notice states that each ICO/ITO has unique properties and should be assessed independently. When deciding whether a coin/token amounts to a security for the purposes of securities regulation, the CSA have referred to the *Investment Contract Test* which was formulated on the findings of *Pacific Coast Coin Exchange v Ontario (Securities Commission)*[38]. The four-part test requires consideration of the financial veracities of a transaction in order to determine whether the ICO/ITO constitutes an investment contract. The test contains the following criteria: *a) an investment of money, b) in a common enterprise, c) with the expectation of profit, d) to come significantly from the efforts of others.* The Supreme Court of Canada has instructed regulators to reflect on substance over form when assessing an application. In those cases where the test is unsatisfactory, regulators are required to consider the scope of the objectives and processes of the securities legislation. The CSA staff notice stipulates that the same test applies to all issuers trading in securities for ICOs/ITOs across Canada. The CSA also highlighted the following factors for determining whether an individual is trading in securities for commercial purposes: facilitating numerous investors; using the internet to increase the number of potential investors; publicly advertising the sale of coins/tokens; and receiving huge capital from various investors. The CSA's staff notice also emphasised concerns associated with cryptocurrency investment funds. The term *'investment funds'* in the provisions for securities law is described as the arrangement of investing in cryptocurrencies. The CSA encourage fintech businesses to evaluate several considerations when establishing

The CSA issued the notice *"Securities Law Implications for Offerings of Tokens"* (SN 46-308), in June 2018 which clarified the treatment of 'utility tokens' which are multifunctional and allow holders to trade using blockchain technology.



a cryptocurrency investment fund. For example, the OM prospectus exemption is not effective throughout all the Canadian provinces. In particular, the involvement of retail investors in the investment fund would prompt prospectus requirements. Although no cryptocurrency exchanges have been registered with securities regulators in Canada to date, a range of strict due diligence checks and registration must be activated on cryptocurrency exchanges when an investment fund is used to trade in cryptocurrencies. The CSA explain ways in which cryptocurrency exchanges can have an effect on staff's evaluation of ICOs/ITOs and cryptocurrency investment funds. The CSA have flagged the importance of the valuation of cryptocurrencies in investment funds and has laid out criteria to consider when determining the valuation:

'How will cryptocurrencies in the investment fund's portfolio be valued?

How will securities of the investment fund be valued? Will one or multiple cryptocurrency exchange(s) be used; and how will such exchange(s) be selected?

Will there be an independent audit of the investment fund's valuation?' For protection purposes the securities regulation of Canada largely requires the assets of the investment fund to be held by a single custodian who satisfies the requirements.

Additional guidance demonstrates how the CSA Regulatory Sandbox (CSA's 2016–2019 Business Plan) can help fintech businesses meet the requirements of securities law. The CSA offer support to both start-ups and established businesses that test the impact of the technology within the real market against regulatory frameworks. This provides a platform for organisations to trial their services in real time within the national marketplace but without being held to the requirements of securities law. The aim of the experiment is to assist both innovation and the scope of regulations and to determine existing implications for both the development of the technology and investor protection. The CSA are aware of the rapid growth in technology and seek to reform the regulatory structure to cater for those changes. Authorised firms are subject to registration and other regulatory obligations in the sandbox environment. Members of the Regulatory Sandbox are subject to sharing relevant data from their services for monitoring purposes.

The CSA issued another staff notice, *"Securities Law Implications for Offerings of Tokens"* (SN 46-308), in June 2018. The notice clarified the treatment of *'utility tokens'* which are multifunctional and allow holders to trade using blockchain technology. The guidance covers offerings of tokens, particularly when the offering of a token does not resemble that of securities. The guidance stipulates that the offering of a token may constitute a distribution of securities if it includes an investment contract. An ICO/ITO can also amount to distribution of securities if the offering can be compared

The CSA created a regulatory sandbox to support fintech businesses to trial innovative products and services and to find an equilibrium between consumer protection and innovation.

with the requirements and purpose of the securities legislation, even if it is not included in the list of *'enumerated categories'*. The outcome will be determined by Canadian securities regulators on a case by case basis depending on the substance of the ICO itself. Moreover, the CSA and Investment Industry Regulatory Organisation of Canada issued a joint consultation paper *"Proposed Framework for Crypto-Assets Trading Platform"* (Consultation Paper 21-402), in March 2019. The purpose of the consultation paper was to request feedback from a range of faculties (including the fintech sector, economic agents, and investors), to develop changes in requirements to accommodate firms engaging in securities law. The paper sought to establish unique properties and risks of platforms that have not been adopted in the existing regulations and to work towards creating a clearer regulatory framework. The paper specifies that securities legislation is applicable to cryptoassets that form commodities as the investor's contractual right to the cryptoasset can amount to securities or derivatives and are therefore subject to the regulatory requirements of securities law.[39]

The *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA) was developed to counter money laundering (ML) and terrorist financing (TF) activities in Canada. The statutory provisions address cryptocurrencies in detail and implement reporting requirements, prosecutions to combat illicit activities, and measures such as record keeping and client identification. The act authorised the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) to monitor and prevent ML/TF in cryptocurrency relations. FINTRAC is an independent organisation which collects appropriate information for law enforcement groups. FINTRAC issued general guidance in June 2016 *("Guideline: Methods to Ascertain the Identity of Individual Clients")* to provide information on reporting procedures and methods used to ascertain the identity of the client. Amendments to PCMLTFA were enforced in June 2020, and these define 'virtual currency' as

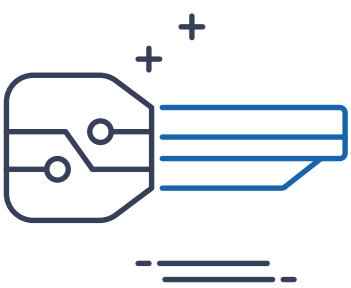
a) *"a digital representation of value that can be used for payment or investment purposes that is not a fiat currency and that can be readily exchanged for funds or for another virtual currency that can be readily exchanged for funds" or*

b) *"a private key of a cryptographic system that enables a person or entity to have access to a digital representation of value referred to in point (a)"*. The amendment also stipulates that cryptocurrency platforms should be catalogued as Money Services Businesses (MSB) so that they comply with the regulatory requirements outlined in the legislation. Such measures include: implementing a compliance regime and registering with FINTRAC; keeping efficient records; and practising strict due diligence checks for suspicious transaction reporting. Likewise, the import or export of fiat currencies or financial instruments of $10,000 or more must be reported to FINTRAC. These measures were introduced to provide greater regulatory clarity and to strengthen the supervisory requirements of the regulation. To mitigate ML/TF the amendments focus on individuals or entities (for example, virtual currency service providers or MSBs) involved in servicing the trade of cryptocurrencies.

The CSA created a regulatory sandbox to support fintech businesses to trial innovative products and services and to find an equilibrium between consumer protection and innovation. Furthermore, the Bank of Canada published the announcement *'Bank of Canada partners with the Bank for International Settlements to launch innovation centre'* in June 2020. The aim of this collaboration is to assist fintech innovation within the central banking sector. Another initiative, Project Jasper, is explored how the private and public sectors can renovate the wholesale payments system using DLT. Payments Canada, the Monetary Authority of Singapore (MAS), and the Bank of England worked together to create a faster and more cost-effective, cross-border currency settlement system. The paper, entitled *'Jasper-Ubin Design Paper: Enabling Cross-Border High Value Transfer Using Distributed Ledger Technology'*, showcases collaboration between Canada's Project Jasper and Singapore's Project Ubin.

Mexico

Regulators in Mexico have recognised the growth of the cryptocurrency market in its jurisdiction and as a result of this policy makers have established a regulatory framework to govern its operations. The fundamental purpose of the policies is to mitigate potential illicit activities deriving from the use of virtual currencies and to strengthen the financial framework. Although the use of virtual currencies is legal in Mexico, they do not constitute legal tender.



The Law to Regulate Financial Technology Institutions 2018 (The Fintech Law) contributes towards several provisions of cryptocurrency in relation to credit institutions. Article 30 of the Fintech Law defines digital assets as *"the representation of value registered electronically and used among the public as a means of payment for all types of legal acts is considered a virtual asset, the transfer of which can only be carried out through electronic means. In no case shall the currency of legal tender in national territory, foreign currency or any other asset denominated in legal tender or in foreign currency be understood as a virtual asset."* Financial authorities that regulate fintech entities in Mexico are the Central Bank of Mexico (Banxico), the Ministry of Finance and Public Credit (SHCP), the National Banking and Securities Commission (CNVB), and Financial Consumer Protection Commission (CONDUSEF). Due to the enactment of certain regulations Mexico is likely to advance technological innovations in a consistent and confident manner.

Virtual currencies in Mexico are regulated by the Fintech Law, which was issued by the Federal Executive branch in March 2018 and aims to separate cryptocurrency from the traditional financial system. This law regulates institutions that provide crowdfunding and e-money services. Crowdfunding institutions provide a platform for people to make investments through electronic means; whereas e-money service institutions provide facilities to issue, transfer, and administer e-money. Both institutions are capable of operating in virtual currency. Article 16 of the Fintech Law stipulates that clients of collective financing institutions may carry out certain functions among themselves and through their institutions. For example, collective financing institutions connect investors to investees through electronic or digital means; investors may use one of the following schemes: *"(i) Collective debt financing, in order for investors to grant loans, credits, mutual or any other financing causing a direct or contingent liability to the applicants; (ii) Collective capital financing, in order for investors to buy or acquire securities representing the capital stock of legal entities acting as applicants; and (iii) Collective financing of co-ownership or royalties, in order for investors and applicants to enter into joint ventures or any other type of agreement by which the investor acquires an aliquot or participation in a present or future asset or income, profits, royalties or losses that are obtained from the performance of one or more activities or projects of an applicant."* Article 23 of the Fintech Law provides a description of what constitutes electronic payment funds: *"a) A monetary value equivalent to a specified amount of money, in national currency or, with prior authorization from Banco de México, foreign currency; or b) A determined number of units of a virtual asset determined by Banco de México, in accordance with the provisions of Chapter III of Title II of this Law; (i) They correspond to a payment obligation in charge of their issuer, for the same amount of money or units of virtual assets referred to in section I of this article; (ii) Are issued against the receipt of the amount of money or virtual assets referred to in section I of this article, with the purpose of paying, transferring or withdrawing said funds, totally or partially, by means of the instruction that, for that purpose, give the respective holder of the electronic payment funds; and (iii) Are accepted by a third party as receipt of the respective amount of money or virtual assets."* Furthermore, fintech institutions in Mexico are monitored by the Interinstitutional Committee comprising the CNBV, Banxico and the Ministry of Finance. Crowdfunding or e-money companies are required to obtain a licence issued by the CNVB and approved by the Interinstitutional Committee.

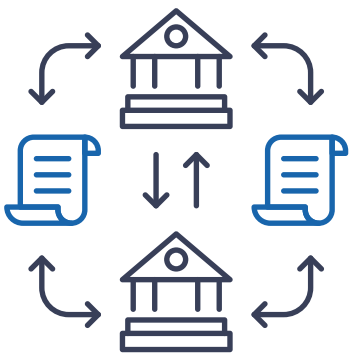
The Fintech Law also refers to 'Innovative Models'. Innovative models include entities which use technological instruments to provide financial services which are distinguishable from the methods outlined by the Fintech Law. Entities which do not constitute financial institutions may be

Although virtual currencies are not treated as legal tender in Mexico, licensed fintech companies can operate in certain cryptocurrencies that have been permitted by Banxico.

granted a two year, temporary authorisation. Within this time period entities must obtain a definitive authorisation, whilst remaining compliant to the conditions provided by financial institutions. Authorities have used innovative models to facilitate and regulate virtual currency related activities which are detached from the traditional financial system. The process requires approval through registration which is in line with the Fintech Law. The enactment of the Fintech Law has activated some changes in areas of financial law, in particular the Securities Market Law in March 2018. The Securities Law regulates the development of securities, transactions and its trading system but excludes those securities dealt with in the Fintech Law. Bitcoin and similar tokens are not regulated by the Securities Law. Furthermore, there is currently no existing tax regime that is applicable to virtual currencies in Mexico. Tax authorities are working towards a tax structure but no regulations have been established.

Although virtual currencies are not treated as legal tender in Mexico, licensed fintech companies can operate in certain cryptocurrencies that have been permitted by Banxico. In March 2019, Banxico published the Circular 4/2019 which stipulated that fintech institutions are not authorised to provide services of exchange, transfer, or safeguard cryptocurrencies. At present, it is only permissible for fintech companies and financial institutions to engage with cryptocurrencies on their own account. In addition to the Fintech Law, companies that associate with virtual currencies are prohibited from providing misleading information and must adopt policies to circumvent false advertisement. For customer protection, companies must notify their clients of the risks involved in such transactions. Fintech companies must declare on their platforms and communication systems that the federal government does not support the companies' responsibilities but that they are regulated and authorised by the Mexican financial authorities. Fintech institutions must also specify in their commercial name whether they provide crowdfunding or e-money services. Since the Fintech Law does not provide guidance on advisory facilities, such services may obtain authorisation from financial authorities through registration.

With regard to Mexico's anti-money laundering and countering the financing of terrorism (AML/CFT) regime, the Federal Law for the Prevention and Identification of Transactions with Resources of Illicit Origin (AML Law) was amended in March 2018. The amendment includes the offer and exchange of virtual assets through electronic or digital platforms by entities or persons other than financial institutions. The amendment also refers to 'vulnerable activity', which under the AML Law indicates a higher risk of money laundering and terrorist financing. Operations related to virtual assets are therefore subject to greater inspections by the Financial Intelligence Unit of the Ministry of Finance (FIU). A wide array of requirements is imposed on those engaged in 'vulnerable activities' by the AML Law. For example, companies that provide such services must adhere to enhanced customer due diligence procedures, regular record keeping, safeguard relevant documents (for at least five years), and report suspicious transactions. The companies must implement strong AML policies and introduce Know-Your-Customer (KYC) practices to their clients. Companies are also obliged to register with the FIU for reporting purposes, particularly for transactions exceeding MXN 54,496.05, equivalent to USD 2,2725 (2019). Additionally, the Ministry of Finance has the power to regulate frequent audits on organisations that engage in vulnerable activities to assess the observance of AML/CFT protocols and procedures. Companies who fail to comply with the AML Law can incur penalties and criminal sanctions if the company enables illegal activities.



Costa Rica

Costa Rica has largely embraced cryptocurrency and blockchain technology in its jurisdiction. For example, the Inter-American Development Bank identified 25 new financial technology (fintech) start-ups in Costa Rica in 2019. This suggests the government is moving towards the development of financial innovation and is exploring the crypto sphere. However, there are no extended legislation or separate regulations for the fintech sector in Costa Rica.

Virtual currencies have not been classified as securities and are not subject to financial regulations in Costa Rica. The scope of such regulations may include certain digital assets, based on their characteristics and nature. It is difficult to predict whether regulators will introduce new regulations or expand existing laws. The current tax treatment of virtual currencies is uncertain and the use of virtual currency or digital assets is not subject to income tax, capital gains tax, or VAT.

The Central Bank of Costa Rica (BCCR) and the Maximum Deconcentration Bodies (ODM) released *'Position of the BCCR and its (ODM) with respect to cryptocurrencies'* in October 2017. They declared a joint warning to the wider public regarding the risks of digital assets and cryptocurrencies. If any financial entity or consumer engages in the commercialisation or acquisition of virtual currencies, the entity or individual will be responsible for their own risk. The warning demonstrated that if such operations take place outside the scope of banking regulations they are not authorised by the BCCR. The statement also reaffirmed *Articles 42-51 of the Organic Law of the Central Bank* (OLCB) which established the colón as the only recognised currency in Costa Rica. Virtual currencies are therefore not considered legal tender in this region. The BCCR and ODM also emphasised that they do not regulate or administer cryptocurrencies and that these should not to be traded through the National Electronic Payment System (SINPE). The statement explained that cryptocurrencies are not issued by any foreign central bank and therefore cannot constitute foreign currency. Consequently, cryptocurrencies are not applicable to the provisions of Article 48 and 49 of the OLCB which allow open currency convertibility. Although there is a lack of explicit legislation, cryptocurrency is legal in Costa Rica and its use is dependent upon other regulations such as anti-money laundering requirements. This can be seen as an opportunity for innovation but also presents a lack of clarity and uncertainty for investors.

Despite the warnings provided by the BCCR, Costa Rica is open to corporate ventures, particularly within the tourism industry.

Anti-money laundering and countering the financing of terrorism (AML/CFT) initiatives have been strongly monitored in Costa Rica in recent years. The US Department of Justice held a Costa Rican based business 'Liberty Reserve' accountable in May 2013, for operating an unregistered money transmitter business and laundering 6 billion USD.[40] Liberty Reserve was created specifically to avoid regulations and assist illicit activities. The online money remittance service used its own virtual currency, known as 'liberty dollars', to allow users to preserve their anonymity on the platform. A significant lack of official monitoring of money laundering, together with an absence of identification and verification checks, helped the business reach high levels of criminal activity in several jurisdictions. However, Costa Rica is subject to the recommendations put forward by the Financial Action Task Force of Latin America (GAFILAT). These include Know-Your-Customer (KYC) and strong due diligence requirements which are regularly scrutinised by the General Superintendency of Financial Institution (SUGEF). GAFILAT helps the region to develop a legal system that actively prevents such offences. In situations where these offences take place the authorities are prepared to investigate suspicious transactions and implement a reporting method for these crimes.

Costa Rica has shown some enthusiasm to deliver a secure experience to those handling virtual currencies, despite the lack of legislation. Although Costa Rica is not currently operating a regulatory sandbox the 'Costa Rica Whitepaper, Blockchain as a Service ICO and the CR Coin System' (2020) delivers an insight into the 'CR Coin'. This coin will be the first digital asset to be used within the decentralised ecosystem in Costa Rica which caters for more secure, digital payments.[41] It can therefore be inferred that authorities and regulators are likely to implement regulations in order to manage the use of such coins and help develop innovation with legal certainty.

Cuba

Virtual currencies are not regulated in Cuba and are not considered legal tender. Cuban authorities have not confirmed the legal status of cryptocurrencies. Although the use of cryptocurrencies has not been made illegal, the absence of regulations creates consumer uncertainty. However, there is still a growing popularity for the use of cryptocurrencies, particularly due to Cuba's current economic climate.

The use of two currencies in Cuba – the Cuban Peso (CUP), and the Convertible Peso (CUC) – has caused extremely low national domestic peso prices for basic essentials and services. The CUC is predominantly used for non-essential items and its employment generates alterations in the country's financial system, which restricts development. The Cuban government announced prospective measures for a process of economic reform in order to enhance standard of living and to unite their dual currency system. Cuba's President Miguel Diaz-Canel delivered a speech *'Cuba Briefing 1 July 2019'*, which laid out a series of possible new measures to provide fundamental changes to the existing economic regime. The process of unification of both currencies may result in inflation, resulting is a less wealthy population. Recent government initiatives indicate that gradual reform is being planned. Cuba is considering significant policy changes to control the possible consequences of cryptocurrencies. In addition to this, virtual currency has been considered to help stimulate economic development in Cuba. The speech confirms that *"work has begun on the study of the possibility of using cryptocurrency"*.There has been no indication of any crypto-lead operations actively taking place and it is unclear whether authorities will produce their own cryptocurrencies or use existing ones. Some Cuban crypto entrepreneurs have expressed concerns about the initiative and have questioned whether Cuban citizens will be able to transfer cryptocurrencies into fiat currencies as the majority of people do not have access to a bank account.

Cuba is associated with the Financial Action Task Force of Latin America (GAFILAT) and is subject to various recommendations to mitigate anti-money laundering and counter the financing of terrorism (AML/CFT). The United States government also issued the Cuban Assets Control Regulations to prompt Cuban authorities to accommodate international AML/CFT requirements.[42] Since 2013, Cuba has made a significant improvement towards their AML/CFT regime by increasing transparency within the financial sector and in communications with international authorities. GAFILAT's report *'Technical Analysis of FATF Recommendations – Re rating of Cuba 2017'* laid out the development of Cuba's efforts to reform their AML/CFT system which indicates that Cuba is – for the most part – compliant with its recommendations. Consequently, Cuban crypto operations will have to align with the stipulated requirements such as customer due diligence, Know-Your-Customer (KYC), and suspicious transaction reporting procedures.

More regulatory frameworks will be required – depending on the progress of cryptocurrencies in Cuba – to legitimise these operations. There are some developments in cryptocurrency businesses; for example, *'Fusyona'* and *'CubaCripto'* are two small, Cuban start-up cryptocurrency companies. They have no connection with the Central Bank of Cuba (BCC) and have not been given any regulatory approval. It is clear that Cuba is undergoing a national dilemma and different approaches are being evaluated. It is possible that future legislation will regulate virtual currencies.

Brazil

Virtual currencies are not regulated by specific legislation in Brazil and are not considered legal tender. Authorities have acknowledged the rapid growth of cryptocurrencies and have attempted to address some issues.

For example, the Brazilian Central Bank (BCB) issued a paper *'Policy Statement Nr. 25,306, of February 2014'* stating that the 'Real' is the only legal tender accepted by the Brazilian jurisdiction and that the use of cryptocurrency was not supported by the government. The paper also included a warning to consumers about the various risks associated with virtual currencies. The statement ends positively and declares the BCB will be exploring the development of such instruments in order to implement the appropriate regulatory actions where required. The Securities and Exchange Commission of Brazil (CVM) issued *'CVM Statement on Initial Coin Offering'* in 2017. The statement details concerns about the use of ICOs and mentions that ICOs could be subject to pre-registration with the CVM if the cryptocurrency in question reflects similar characteristics to, or features of, securities. Importantly, the CVM banned possession of cryptocurrency in Brazilian investment funds because cryptocurrency does not fall within the definition of financial assets under the existing legislation (Law no. 6.385 of December 7, 1976). In November 2017, the Central Bank of Brazil warned the public of the speculative risk of digital currencies in COMMUNIQUÉ 31,379 OF November 16, 2017. Nevertheless, there are no statutory provisions restricting persons from trading in cryptocurrencies or purchasing goods or services, so long as there is an agreement between the participants involved.

As mentioned above, there is currently no specific legislation regulating the creation or trade of virtual currencies. However, there are two bills of law which are being considered in the House of Representatives. The first bill of law (PL2303 dated July 7, 2015) proposed to incorporate cryptocurrency into the definition of 'payment schemes'. The BCB defines 'payment schemes' as the principles that govern certain payment services to the public (credit and debit cards would be such examples). This bill states that if cryptocurrency is included in the definition of payment schemes then it would be subject to the legislation and supervision of the BCB. However, after consideration in the House of Representatives the bill was overthrown as cryptocurrency was not accepted as a means of payment. Subsequently, new changes were proposed to allow the issuance of cryptocurrency and prevent regulators creating pre-emptive legislation that could possibly hinder innovation. The second bill of law (PL2060 dated April 4, 2019), defines cryptocurrency and makes a distinction between securities. The bill also endorses the use, issuance, and transfer of cryptocurrency. Both bills have not been approved, are still being considered, and may encounter amendments where required.

There is no specific legislation which regulates the sale of cryptocurrency in Brazil. Nonetheless, if certain features or characteristics of cryptocurrency align with securities, such instruments can come under the scope of the Securities Law (Law 6.385/76). In situations where virtual currency or digital assets constitute securities, Initial Coin Offerings (ICOs) will have to pre-register with CVM. Although the CVM does not regulate ICOs, such instruments may be subject to policies regulating securities offerings. The CVM has also expressed an opinion that ICOs should be considered securities or *"collective investment agreements"*, which are securities that include participation and remuneration rights. The CVM claims that there is confidence in the securities system via registration and authorisation procedures.[43] In 2016, the Brazilian Federal tax bureau considered cryptocurrencies as financial assets and therefore subject to taxation. Taxpayers are required to declare cryptocurrency in their tax returns and pay income tax on capital gains from the use of cryptocurrency. For income tax purposes, cryptocurrencies must be declared as other assets and will be taxed, provided that the total value of the cryptocurrency disposed exceeds BRL 35,000.00.

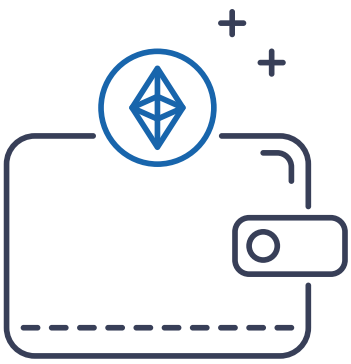
With regard to Brazil's anti-money laundering and countering the financing of terrorism (AML/CFT) regime, a series of obligations instructs individuals or entities involved in virtual currency dealings in various markets to keep detailed records and report suspicious transactions.

With regard to Brazil's anti-money laundering and countering the financing of terrorism (AML/CFT) regime, a series of obligations instructs individuals or entities involved in virtual currency dealings in various markets to keep detailed records and report suspicious transactions. This structured criteria was established by the Financial Activities Control Council (COAF). COAF is a federal government agency that manages and enforces AML requirements within the jurisdiction. At present, there are no statutory frameworks imposed by the Brazilian legal system which specifically delegate the prevention of money laundering or terrorist financing (ML/TF). Nevertheless, the enactment of the Anti-Money Laundering Law, which outlines the definitions, requirements, and sanctions, creates the foundation for a local legal framework in order to mitigate such crimes in Brazil. Furthermore, in May 2019, the Brazilian Federal tax authorities will have access to information that will help recognise suspicious transactions due to the new reporting obligations provided by Normative Instruction No. 1,888/19. These reporting obligations extend to Brazilian legal entities and individuals transacting with virtual currencies without using any exchange or exchanges located outside of Brazil. Anybody who fails to comply with the obligations are subject to fines between BRL 100.00 and BRL 1,500.00 per month of delay in payment.

There are no advancements for cryptocurrency or blockchain technology led by the Brazilian government. However, the Central Bank of Brazil is exploring distributed ledger technology within the financial system and working towards developing preliminary systems. In May 2019, the Central Bank of Brazil also launched the initiative 'Financial and Technological Innovation Lab (Lift)' which offers support to projects that are initiating technological innovations within the financial arena. Most projects are heavily concentrated on the development of blockchain activity.

Bolivia

The use of virtual currencies in Bolivia is prohibited. The Central Bank of Bolivia (BCB) has emphasised that the use of any currency which has not been authorised by the monetary authority is also prohibited. In *'Resolucion De Directorio N'' 044/2014'* (Resolution Nº 044/2014 published in May 2014), the BCB clarified that virtual currencies are unregulated and the prohibition stands for monetary denominations within the remit of the national payment system.



Virtual currencies are therefore not considered legal tender in Bolivia. The BCB also reiterated the prohibition in *'Comunicado'* (April 2017), and warned the public about the apparent risks and potential losses from the use of virtual currencies. Furthermore, the Financial Regulatory Authority in Bolivia known as Autoridad de Supervisión del Sistema Financiero (ASFI) is the regulatory body for the financial services industry in Bolivia. In May 2017, the AFSI issued a press release titled *'Asfi Recuerda A La Población Que En El País Esta Prohibido El Uso Y Circulación De Monedas Virtuales'*. The announcement declared that sixty people were held in detention by the Special Fight Against Crime Force for taking part in virtual currency related training with the intention of making investments. The press release sought to remind the public that such activity in Bolivia is illegal, and has been recognised as a pyramid scheme. The appeal was made by the Executive Director General of the ASFI, who referring to the BCB Resolution Nº 044/2014, stated that the circulation of any virtual currency must be reported. The use of virtual currency in Bolivia comes with a high risk of fraudulent activities that can affect both the nation's monetary systems and finances of individuals. There was also an indication that the ASFI, together with judicial authorities, could enforce the relevant law on persons implementing virtual currency related businesses in the jurisdiction. The appeal requested Bolivians to be cautious with their savings and to protect the economy by rejecting any virtual currency activities and reporting directly to the ASFI. The press release also indicated that the ASFI were in the process of constructing a draft law that would incorporate pyramid schemes into the penal code. This will mitigate fraudulent activities and implement procedures that will reprimand those who choose to participate in such activities.

In Bolivia, anti-money laundering and countering the financing of terrorism (AML/CFT) initiatives have been implemented through 'Laundering of Illicit Gains' in the Penal Code (CP) by Law 1768 of March 10, 1997. There is no direct reference to virtual currencies in this legislation. Bolivia remains susceptible to money laundering and terrorist financing through the use of virtual currencies. However, Bolivia has implemented various regulations to tighten AML/CFT directives through Know-Your-Customer (KYC) and the criminalisation of illicit activities. The KYC procedures require valid photo identification and relevant user identification information. Financial intermediaries are required to register relevant information on their systems irrespective of the transaction amount, whereas private banks must adhere to international KYC standards. Bolivia's Financial Investigative Unit (UIF), alongside BCB's banking regulations, have effected reporting regulations for transactions above USD 3,000. In 2017, the Bolivian National Customs signed a Customs Mutual Assistance Agreement (CMAA) that permits international cooperation and sharing information on money laundering. In the *'Bureau of International Narcotics and Law Enforcement Affairs, International Narcotics Control Strategy Report'* issued by the United States Department of State in March 2020, it is stated that Bolivia is included in the 'Major Money Laundering Jurisdictions in 2019' in the United States Money Laundering Report. The report demonstrates that the UIF lacks resources and a stable regulatory framework to effectively combat money laundering and terrorist financing. Although Bolivian authorities have banned the use of virtual currencies, the report demonstrates that the Bolivian justice system is corrupt and therefore political interventions are restricted. The report highlighted that, with improved supervision and regulation, authorities will be better equipped to counteract financial crime and address deficiencies in the virtual currency sector. Bolivia is also a member of the Financial Action Task Force of Latin America (GAFILAT) and has improved on AML/CFT compliance by implementing the proposed recommendations. At present, it is not clear whether Bolivian authorities will lift the ban on virtual currencies and what regulations future legislation may contain.

Venezuela

The Venezuelan government has taken a wide-ranging approach to virtual currencies. Authorities have significantly promoted the use of virtual currencies for both commercial and non-profit purposes together with the creation of the country's own cryptocurrency, 'petro'.

Simultaneously, the government has also kerbed cryptocurrency miners and warned players from engaging in foreign exchange transactions. In essence, the petro has been popularised to the extent that it is now used to provide wages, taxes, and public offering prices. However, Article 318 of the Constitution establishes that the bolivar is the national currency of Venezuela, and has been authorised by Article 106 of the Law of the Central Bank of Venezuela. Virtual currencies do not constitute legal tender in Venezuela and only the bolivar should be treated as fiat currency; however, the Constitutional Assembly has effectively endorsed the use of virtual currencies in April 2018 by publishing the Constitutional Decree. This decree regulates virtual currencies while Article 9 provides the requirement to promote, protect, and guarantee the use of virtual currencies as a means of payment in both public and private spheres. The extent of Venezuela's promotional strategy is questionable as the objectives require changes beyond the current legal powers. For example, Article 9 of the Constitutional Decree enacts an obligation to promote the use of virtual currencies which may produce various incentives in the process, yet the use of virtual currencies cannot be guaranteed given that the bolivar is the one and only recognised legal tender.

The petro was initially launched in December 2017 by a Presidential Decree. In April 2018, the Constitutional Assembly issued the Consultation Decree, supported by the backing of Venezuela's oil reserves. However, the qualification of the petro has led to some controversy. Although the petro is a cryptocurrency, it potentially qualifies as an unconventional government debt under Article 80 of the Law of the Financial Administration of the Public Sector. This has been confirmed in the United States Department of the Treasury FAQs on Venezuela's related sanctions. It was suggested that currencies with such characteristics indicate an extension of credit to the Venezuelan government. However, this could lead to the violation of the Venezuelan Constitution. The law states that a public debt comprises the issuance of securities and the granting of guarantees; the Petro potentially satisfies both classifications. For example, the Petro qualifies as securities since it is guaranteed by the issuer and grants the holder certain rights, allowing it to fall within the remit of the definition provided by Article 80 of the Law of the Financial Administration of the Public Sector. This has been supported by the National Assembly of Venezuela in the *'Agreement on the Implementation of Petro'* (March 2018). The statement expressed that the issuance of a national cryptocurrency associated with government debt is illegal without congressional approval and the enactment of law under the National Constitution. Furthermore, the government initiated the backing of the Petro with oil reserves. This has raised legal concerns under Article 12 of the Constitution and Article 3 of the Organic Law on Hydrocarbons which proscribe the impediment of oil reserves. The Law of Financial Administration of the Public Sector also prohibits public assets being used to guarantee public debt transactions.

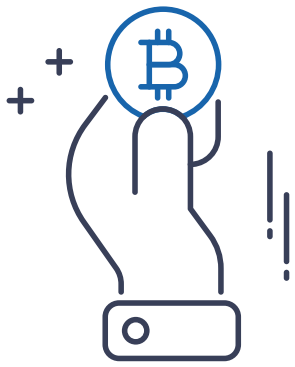
The government has introduced various arrangements in order to promote the use of the Petro. For example, *'Petro zones'* have been created which are designated zones for the purpose of mining and dealing with virtual currencies. The Venezuelan government is also beginning to incorporate crypto assets to achieve a prosperous economy, and has effected different tax approaches. Authorities have also encouraged the development of the cryptocurrency space in relation to blockchain technology, virtual exchanges and digital wallets. Notwithstanding the optimistic efforts regarding virtual currencies, there is clear evidence of conflicting applications. In 2017, there were several arrests of bitcoin miners for illegal consumption of electricity; the Vice President of Venezuela cautioned participants with imprisonment for speculating in cryptocurrency in June 2018. This has derived from the rise of the parallel foreign currency market, where virtual currencies have been

used to escape the exchange controls regime, which has consequently affected attitudes towards virtual currencies. Nevertheless, the Executive's outlook had changed by July 2018 and had become more accepting of the parallel market concerning exchange controls. In August 2018, the Constitutional Assembly issued a Constitutional Decree through the Official Gazette No. 41.452 repealing the penalties associated with the exchange system. The Venezuelan government maintained a tolerant and flexible attitude towards exchanges, including cryptocurrency transactions.

Venezuela has enacted explicit legislation to regulate cryptocurrencies and assigned the National Superintendency of Cryptocurrencies (SUNACRIP) as the regulating body. The regulations maintain both direct and indirect obligations and have not been clearly specified. Article 30 of the Constitutional Decree on the Crypto Asset Integral System imposes registration requirements on all entities and individuals engaging in crypto activities. Article 28 obligates participants to acquire a licence; however, Article 11, from the same decree, also authorises SUNACRIP to permit crypto asset related activities. Although authorisation has not been stipulated as a prerequisite, the obligation to acquire authorisation is implied through the provision. Primarily, the mining of cryptocurrencies was prohibited due to excessive power consumption; however, in September 2020, SUNACRIP legalised cryptocurrency mining through the Official Gazette No. 41.955. The decree requires all entities and persons to obtain licences from the agency in order to legally mine cryptocurrencies. The decree actions the process towards the creation of a National Digital Mining Pool (NDMP), which will effectively organise all miners who are operating in Venezuela. The new regulations encourage cryptocurrency miners to join the NDMP irrespective of the electricity usage. In order for miners to comply with the regulations, the decree highlights that such operations will be under scrutiny and supervision from relevant bodies, including the creation and importation of mining equipment. The decree also specifies that miners operating outside the pool will be subject to sanctions and penalties.[44] Furthermore, the Constitutional Decree proposes limitations that breach the constitution. For example, Article 156 (32) of the Constitution restricts legislation to national authorities; Article 187(1) stipulates that the National Assembly legislate affairs (including commercial activities), according to the national authorities known as *reserva legal*. Therefore, the regulation of virtual currencies constitutes a commercial matter within the *reserva legal* and – for validity – must be enacted through law by the National Assembly. Therefore, regulations established through the Constitutional Decree are unconstitutional and annulled.

Virtual currency activities are nonetheless regulated by the decrees enacted by the Constitutional Assembly which were published in the Official Gazette in January 2019. SUNACRIP introduced the Integral Registry of Crypto Assets Services (RISEC) through a resolution which requires all individuals and businesses interested in crypto related activities to register with them. The resolution provides a definition of users, specifies the procedure for registration, and the relevant documentation required. SUNACRIP has also published a resolution that is applicable to everyone engaging in receipt and transfer of personal remittances in virtual currencies in Venezuela. The resolution also specifies a threshold on the amount of crypto assets that can be transferred each month, which is equivalent to 10 petro. In accordance with the Constitution Decree published in January 2019, monetary penalties, sanctions, and imprisonment will be applicable to persons participating in illicit activities and crypto related activities without authorisation. Moreover, securities legislation may also be applicable to certain virtual currencies depending on their characteristics and structure. In particular, the petro may qualify as securities. Article 46 of the Capital Markets Law stipulates that the National Superintendents of Securities will determine whether an asset can constitute a security. If a virtual currency satisfied the criteria of securities, the Capital Markets Law would apply. With regard to taxation, regulators have not determined a specific tax treatment for virtual currency and general rules will be affected.

The Organic Law on Organised Crime, Terrorism Financing and Proliferation of Mass Destruction Weapons is the primary regulation in Venezuela controlling anti-money laundering and countering the financing of terrorism (AML/CFT) directives. Venezuela has also adopted recommendations proposed by the Financial Action Task Force (FATF) and is a participating member of the Caribbean Financial Action Task Force (CFATF). All suspicious transactions must be reported to SUNACRIP and failure to notify authorities can lead to deregistration and penalties. At present, Venezuela seems minded to promote the use of virtual currencies but there has been no indication of upcoming legislation. However, authorities have created two environments for the development of the cryptocurrency and new technologies.



Argentina

Virtual currencies were well received in Argentina, primarily in an attempt to protect the economy against inflation and foreign exchange limitations. Although virtual currencies are legal, there is no regulatory framework applicable to the exchange, issuance or practice of such currencies.

The Argentinian government has implemented guidelines relating to taxation, anti-money laundering, and countering the financing of terrorism (AML/CFT). Authorities have adopted a relaxed approach and are gradually working towards the development of cryptocurrencies in the financial market. However, virtual currencies do not constitute legal tender in Argentina, which is specified in Article 18 of the Central Bank of the Argentine Republic and Financial Institutions (Law 25,780) and refers to Article 1 of Organic Charter and Gral Regime of the Central Bank of the Republic of Argentina (Law 24,144). The law clarifies that *"The Bank is exclusively in charge of the issuance of notes and coins of the Argentine Nation and no other body of the national government, nor the provincial governments, nor the municipalities, banks or any other authorities, may issue notes or coins, metal or other instruments that could be circulated as currency."* Nevertheless, the Financial Information Unit (UIF) has provided a definition for virtual currencies, such as bitcoin, in Article 2 of the Prevention of Money Laundering and Terrorism Financing Resolution 300/2014. Virtual currencies are described as the *"digital representation of value that can be the object of digital commerce and whose functions are to constitute a medium of exchange, and/or a unit of account, and/or a reserve of value, but they are not legal tender, nor are they issued, nor are they guaranteed by any country or jurisdiction"*. The Argentina Civil and Commercial Code (CCCN) stipulates that persons and legal entities have rights over both tangible and intangible assets that constitute their property. Virtual currencies are intangible assets comprising a form of property. It is clear that virtual currencies are not considered legal tender and that only the Argentinian peso can be treated as fiat currency. Virtual currency can be used as a means of payment, but is not supported by the Central Bank of Argentine (BCRA), nor guaranteed by the government. This was reinforced in the *'Press Communication'* issued by the BCRA in May 2014.

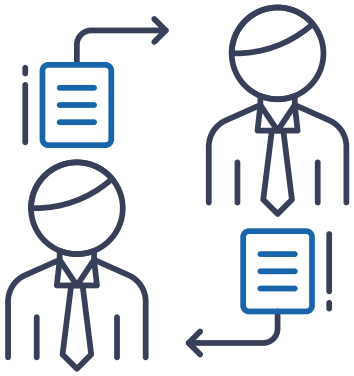
There are no detailed regulations governing the sale of virtual currencies which are not classified as securities or commodities under Argentinian law. Since securities in Argentina are recognised instruments that include credit rights to issuers, virtual currencies are outside of the scope of the securities legislation. Virtual currency operations lack a central authority. In December 2017, the Argentinian Securities and Exchange Commission (CNV) issued a warning (*'Ofertas Iniciales de Monedas Virtuales o Tokens'*) against ICOs and virtual tokens. The warning was directed at investors and highlighted the risks associated with virtual currencies and Initial Coin Offerings (ICOs). The document illustrated that the associated technology is still premature and that the absence of regulations could mean a greater likelihood of fraud coupled with price volatility and potential liquidity risks. The CNV also confirmed capital market regulations will not be applicable to ICOs; however, the CNV has the powers to regulate ICOs subject to their structure and characteristics. The CNV does not act as the primary regulators of ICOs but the announcement provided an explanation of fraud and suspicious activities related to ICOs which can be reported to the CNV.

With regard to taxation, Argentina enacted tax reform through Decree No. 824/2019 which amended the Law of Social Solidarity and Productive Reactivation within the Framework of the Public Emergency (Law No. 27,541), in December 2019. After approval of the Tax Reform Law, it will impose tax on financial income generated by the commercialisation of digital currencies.[45] In spite of this, there is no clear definition or understanding of digital currencies provided by the Tax Reform Law or the Income Tax Law (ITL). The definition used by the UIF Resolution 300/2014 of virtual currencies should therefore be applied, which would bring virtual currencies within the remit of the reformed tax laws. The ITL has stated that if the issuer of virtual currencies is located or domiciled in Argentina, the asset in question will constitute an Argentinian

The Argentinian Congress passed the Regime for the Promotion of the Knowledge Economy (Law No. 27.506) in June 2019 which offers a new tax regime that will assist new technologies.

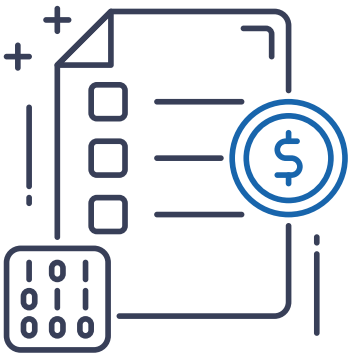
source but if the issuer is established outside of Argentina the income will be considered foreign.[46] All legal entities, whether based in Argentina or elsewhere, will be subject to a schedular tax rate of 15%. Resident legal entities will be subject to income tax on gains derived from the sale or ownership of digital assets at a rate of 30%. Given that virtual currencies are classified as intangible assets, such exchanges should not be affected by value added tax (VAT).[47] Furthermore, the Argentinian Congress passed the Regime for the Promotion of the Knowledge Economy (Law No. 27.506) in June 2019 which offers a new tax regime that will assist new technologies. The regime will be in force between January 2020 and December 2029. Article 2 (a) of Law No. 27.506 lists several categories where the legislation aims to *"create, design, develop, produce and implement or adapt products and services and their associated technical documentation"*. Contingent on its application, distributed ledger technology (DLT) may fall within various categories listed under this regime and exposed to the benefits thereof.

Virtual currencies are generally not regulated in Argentina. The one exception to this is UIF's Resolution 300/2014. This policy requires suspected fraudulent activities to be reported to the UIF under the Laundering of Criminal Origin Assets – Pean Code Modification (AML Law) Law No. 25.246 and Law No. 27.430. The AML Law states that those obligated to make these reports include the following: financial entities; broker-dealers; insurance firms; and government registries and agencies. These persons are also subject to Know-Your-Customer (KYC) procedures in order to adhere to anti-money laundering and countering the financing of terrorism (AML/CFT) initiatives. The UIF Resolution 300/2014 also requires obligated subjects under the AML Law to report all transactions using virtual currencies, irrespective of values handled. Argentina is a member of the Financial Action Task Force of Latin America (GALIFAT) and has acknowledged the recommendations proposed by the Financial Action Task Force (FATF). As a result, the UIF has warned obligated persons about the risks associated with virtual currency transactions and that those involved are required to closely monitor operations. There is no government led sandbox to explore the regulatory developments of virtual currencies in Argentina. Excluding tax and AML/CFT regulations, authorities are making observations and waiting for technologies to progress in order to avoid pre-emptive legislation. It is also significant that BCRA has created research groups for blockchain technology and cryptocurrency in order to enable regulatory developments for the financial technology sector.



Chile

The Chilean government has not granted virtual currencies a legal status and persons transacting in cryptocurrencies are not subject to regulation provided by the financial authority. Virtual currencies are not backed by the Central Bank of Chile (BCC) and do not constitute legal tender.



At present, there is no regulatory framework applicable for virtual currencies. The Chilean Minister of Finance referred to a draft bill to regulate financial technology (fintech) and virtual currencies in April 2019; however, no such bill has to date been approved or discussed in more detail by the Chilean government. Nonetheless, the use of virtual currencies has not been prohibited and can be employed at the user's own risk.

In April 2018, the Financial Stability Council (CEF) issued a press release entitled, *'The Financial Stability Council warns the public about the risks associated with the acquisition and holding of so-called cryptocurrencies'*. The CEF is chaired by the Minister of Finance. The President of the Commission for the Financial Market, the Superintendent of Banks and Financial Institutions, the Superintendent of Pensions, and the President of the Central Bank of Chile also sit at this council. The press release indicates that virtual currencies do not pose a significant risk for the Chilean financial system but warns the public about the risks associated with its use. The appeal clarified that the BCC and other financial authorities do not encourage the use of virtual assets. Those acquiring or investing in such assets should be aware that the value of such assets originates only from the dependence of its users. Importantly, there are no statutory instruments regulating virtual currencies in the jurisdiction; there is consequently no legal recourse available to individuals, issuers, nor intermediaries. The lack of centralisation, backing and supervision wholly distinguishes virtual currencies from legal tender and its financial system. Furthermore, the Commission for the Financial Market (CMF) has confirmed that virtual currencies do not constitute securities under the existing legislation. The CEF has expanded on the risks associated with virtual currency and assets, particularly focusing on their high volatility. High volatility allows investment in such assets to create potential profits as well as substantial losses in a short period of time. Consumers can expect to be exposed to robust price variations, lack of backing from traditional assets, and subsequent losses from fraudulent activities.

Although there is no legal framework applicable to virtual currencies the CEF press release informs service providers, issuers, and consumers that they must comply with the following applicable regulations: anti-money laundering and countering the financing of terrorism (AML/CFT) directives; taxation; foreign exchange regulations; and instructions from the BCC. Virtual currency users are accordingly still subject to legal provisions and will be held liable. As the Council highlighted, the caution was only directed to the risks related to virtual currencies, and not all fintech developments. For example, blockchain technology and distributed ledgers are encouraged for innovation. Ultimately, the statement stressed that the CEF will continue to study and observe changes in the industry in relation to the national financial framework. Policy makers will also consider appropriate regulations to enable the growth of fintech developments and innovation in order to increase competition and contribute to the market.

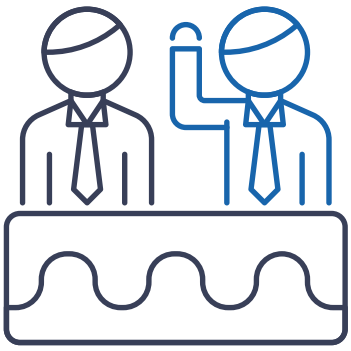
Law No. 19, 913 (Anti-Moneda Laundering Act) lays out the general regulations for anti-money laundering and countering the financing of terrorism (AML/CFT) objectives in Chile. The AML Act imposes procedures on banks and similar entities to report to the Financial Analysis Unit (UAF) for suspicious transactions, cash transactions exceeding USD 10,000, and to provide relevant documentation for inspection when requested. The Law also provides Know-Your-Customer (KYC) and identification procedures for traditional banking systems. Similarly, Law No. 20, 393 extends the criminal liability of corporations for money laundering or terrorist financing and other fraudulent behaviour. It is noteworthy that there has been no direct reference to virtual currencies in these laws. No update on progress has been given on alleged accounts of a bill to regulate virtual currencies.

Ecuador

Ecuador established a nationally recognised central digital currency known as *Sistema de Dinero Electrónico* (SDE) (which translates as electronic money system), in 2014.

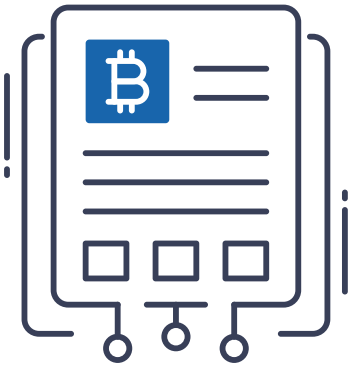
In January 2018, the Central Bank of Ecuador (BCE) put forward its position on the use of bitcoin and similar cryptocurrencies in the *'Official Communication on the use of the Bitcoin'*. The BCE declared that bitcoin is not to be treated as legal tender and does not constitute an authorised payment method, as specified under Article 94 of the Organic Monetary and Financial Code. Bitcoin and similar cryptocurrencies are not backed by an authority since they are usually employed as speculative investments. The BCE also stipulated that transactions involving bitcoin are not regulated or monitored by any national authority and that investors engaged in such activity are exposed to financial risk. The BCE clarifies that the sale and purchase of virtual currencies, similar to bitcoin, are not prohibited. This can be inferred by the fact that there is no regulation governing virtual currencies in Ecuador and its use is lawfully permissible (although not advisable, for the reasons provided above). Nevertheless, Ecuador established a nationally recognised central digital currency known as *Sistema de Dinero Electrónico* (SDE) (which translates as electronic money system), in 2014. This digital currency functions alongside the existing national currency (the US dollar). The initiative behind the program was to generate financial inclusion and enhance economic growth in Ecuador. Authorities have also drawn a stark contrast between the SDE and bitcoin, emphasising that only the SDE is backed by financial institutions.

The SDE was established through Resolution 005-2014-M of the Monetary and Financial Regulation and Policy Board (The Resolution), in 2014, which governs Ecuador's digital currency. The Monetary Policy Board and Financial Regulation bring the following four entities together: the Banking Board; the Board of Market Regulation of Securities; the Regulation Board of the Popular Economy and Solidarity; and the Central Bank Board. This initiative was constructed to provide residents with opportunities and access to financial services. The electronic payment system was established to allow individuals to trade flexibly and to offer businesses in remote areas access to appropriate and timely financial products. This payment method also operates through the liquid assets held by the BCE, which makes the availability of foreign exchange in the economy imperative. The SDE also helps towards reducing the costs of handling for, and the profitability of, financial institutions. The BCE is the regulatory authority for digital currency and creates all electronic payment accounts. The BCE is also obliged to register the final daily balance of electronic money for liability purposes. The electronic payment system can be used by nationals, residents, and legal entities domiciled in Ecuador, and can only be exchanged through electronic devices. Individuals holding digital currency can make exchanges for fiat currencies at face value; holders can also send and receive transfers to and from their accounts in the



The BCE is the regulatory authority for digital currency and creates all electronic payment accounts. The BCE is also obliged to register the final daily balance of electronic money for liability purposes. The electronic payment system can be used by nationals, residents, and legal entities domiciled in Ecuador, and can only be exchanged through electronic devices.

The primary legislation governing anti-money laundering and countering the financing of terrorism (AML/CFT) in Ecuador is the Law on the Prevention and Eradication of Money Laundering (September 2016). This legislation extends to non-financial organisations and imposes an obligation to report suspicious transactions involving USD 10,000 or above within four days.



National Financial System. The objective is to increase control and easily identify counterfeiting, together with improved transparency from financial institutions.

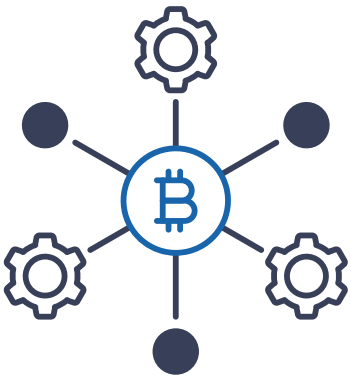
Later, in July 2015, the BCE issued the *'Central Bank of Ecuador Official Statement'*. The statement clarified that the purpose of the resolution was to enable all Ecuadorian financial entities to be able to engage with electronic money services. Importantly, financial institutions must only offer this service to persons as a means of payment. Individuals are not obligated to use this service and it is available on a voluntary basis. Similarly, banks as legal entities are not required to issue or collect payments in the digital form. The statement strictly emphasised Article 94 of the Fundamental Monetary and Financial Code which stipulates that *"Under no circumstances whatsoever can the State compel any natural person or legal entity to receive currency other than the United States Dollar"*. The Ecuadorian government and the BCE are both determined to support the digitalisation of the dollarization money scheme. The statement also refers to Article 3 of the Resolution which specifies that the BCE can only provide electronic money in exchange for US dollars. The Administrative Resolution No. BCE-0122-2014 (dated September 2014), cited that electronic money must be backed by assets with the same level of liquidity as those of the international reserves. It also prohibits the exchange for any other type of securities issued by public or private entities. Article 101 of the Fundamental Monetary and Financial Code was also referred to, which expressly states that only the BEC may circulate electronic money that is backed by liquid assets. Actions carried out by the BCE must be centred on the directions provided by the Monetary and Financial Policy and Regulation Board.

The primary legislation governing anti-money laundering and countering the financing of terrorism (AML/CFT) in Ecuador is the Law on the Prevention and Eradication of Money Laundering (September 2016). This legislation extends to non-financial organisations and imposes an obligation to report suspicious transactions involving USD 10,000 or above within four days. There are no specific AML/CFT regulations or legislation which explicitly address virtual currencies. There has been no indication as to whether Ecuador will issue legislation or relevant regulations concerning virtual currency.

East Asia

China

China has recognised the significance of blockchain technology and advocates proposals for blockchain operations in a range of areas, including the financial industry. While China appreciates the benefits of blockchain activity, cryptocurrencies are largely disapproved of.



The *"Notice on Preventing Bitcoin Risks"* issued in 2013 by various Chinese regulatory authorities, demonstrates the risks of cryptocurrencies on the financial sector. The notice confirms a ban on bitcoin transactions because cryptocurrencies do not constitute legal tender in China. The notice states that financial institutions should not trade or accept bitcoins as a payment tool, nor act as an intermediaryfor financial services relating to bitcoin. The *"Public Notice on Preventing Risks of Fundraising through Coin Offerings"* was issued in 2017 by the People's Bank of China (PBC) in collaboration with other organisations. The notice addressed the disruption to the financial order due to the rise of both speculation in cryptocurrencies and illegal financial activities. The notice established that any virtual currencies used in coin offerings are not supported by the financial authority and do not hold the properties of fiat currencies, meaning that they cannot be distributed in the financial market. The notice declared that the public should be aware of the risks deriving from coin offerings and be able to recognise illegal financial activities. The Internet Finance Association provided further guidance in *"Announcement on Preventing Initial Coin Offerings (ICO) Risks"* in 2017. The document highlights the explicit financial risks of using cryptocurrency; for example, money laundering (ML), terrorist financing (TF), illegal fund raising, and other financial criminal activities. The announcement banned ICOs and cryptocurrency exchanges in China. When cryptocurrencies became widespread in 2017, authorities lost control of censorship and capital flight, primarily due to inexperienced investors encountering speculative ICOs from illegitimate resources. Therefore, to prevent economic disaster authorities banned the use of ICOs and classified them as unlawful public fundraising. China had also prohibited cryptocurrencies exchanges including trading platforms delivering exchange services and the sale of tokens or services in relation to virtual currencies. However, it is evident that the notice and announcement do not restrict individuals from holding or dealing in cryptocurrencies. Instead, cryptocurrencies are not recognised as currency and financial institutions are prohibited from supplying services related to cryptocurrencies. This suggests cryptocurrencies are largely unregulated in China because no regulations specify how bitcoin or cryptocurrencies should be treated.

On the other hand, Chinese authorities support the advancement of blockchain technology and have consequently regulated blockchain facilities with care. The Cybersecurity Administration of China published the Blockchain Information Service Management Regulations (BISMR), in 2019 which provides a legal structure for the regulation of blockchain services. *"Blockchain information service providers"* include: *(1) entities and nodes that provide blockchain-based information services to the public*; and *(2) institutions and organizations that provide technical support to such entities*. It is clear that regulators have avoided any implications of anonymity under BISMR with the legislation stipulating the importance of retaining information for supervision purposes. Businesses providing blockchain services must therefore register with regulators and carry out efficient due diligence checks to identify the users involved. Blockchain businesses are also responsible for reporting exploitation of services and monitoring users to prevent illegal activities. The legislation expressly prohibits both service providers and users from abusing services for unlawful ends which would disturb the economic order or breach the rights of others.

Although cryptocurrencies exchanges are banned in China, there are still possibilities for individuals to engage in related services, particularly because China still authorises the mining of cryptocurrencies. There is not a ban on users owning or transferring cryptocurrencies. The legal status of bitcoin has not been confirmed by legislation or policy statements; however, it has

Although ICOs and cryptocurrency exchanges are banned, the PBC has been involved in the development of a central bank digital currency.

been discussed in a judicial hearing from Hangzhou Internet Court in July 2019. The hearing constituted a discussion on the legal parameters of bitcoin in the context of Chinese property law. The plaintiff could not access bitcoins or withdraw the money as the service which had sold the bitcoins had subsequently closed. The court's decision implied that bitcoin reflected the necessary legal requirements to amount to virtual property because it is *"valuable, scarce and disposable"*. Each court decision in China holds an independent interpretation of law and there is no legal precedence to assist with future cases. Although cryptocurrency regulations may shine a light on grey areas in the law, authorities have emphasised that cryptocurrencies are not to replace the national currency (renminbi – RMB). The RMB is the only recognised legal tender in China and individuals can only make valid exchanges using this currency. Therefore, cryptocurrencies are not directly regulated, but instead cryptocurrency dealings are regulated. Furthermore, ICOs are deemed illegal under the Internet Finance Association's announcement because the structure of ICOs is very similar to the sales of securities. Although Chinese securities law does not regulate ICOs, the ICO embodies an unlicensed form of securities offering. There are no bespoke tax laws regarding cryptocurrencies. As a general rule, any form of income is taxable; however, this is not the case for cryptocurrencies due to the prohibition of cryptocurrency services imposed on the financial sector.

On the issue of anti-money laundering (AML) and countering the finance of terrorism (CFT), China has established strong capital controls to restrict the amount of capital outflow to other countries. China's State Administration of Foreign Exchange (SAFE) thoroughly inspects the remittances and expenditure in and from China. Individuals are restricted to moving an annual limit of USD 50,000 outside of China. Cryptocurrencies manifestly pose a significant risk for capital control, for example, by making capital transfers outside of China without correspondence with Chinese financial institutions or obtaining approval from SAFE. Consequently, the notices outlined above indicate that financial institutions should carefully monitor trans border cryptocurrency activities while taking ML/TF risks into account. China is also a member of the Financial Action Task Force (FATF). The majority of the AML/CFT objectives derives from the recommendations proposed by FATF. The *"Anti-Money Laundering and Countering Terrorist Financing Measures Mutual Evaluation Report"* was produced by FATF for the People's Republic of China in April 2019 and explores the country's understanding and identification of ML/TF risks in the financial sector. FATF outlined that the PBC has been able to issue appropriate risk warnings to the public detailing the threat of ML/TF from cryptocurrencies; however, the PBC has not adopted an inclusive strategy to address more recent developments. The National Internet Finance Association of China was able to highlight a series of cautions about Fintech products, predominantly ICOs and cryptocurrencies. Nonetheless, the issues in question refer to the misuse of technology and distinguish between lawful and unlawful activities as opposed to emphasising measures to mitigate ML/TF risks.

There is no indication that China will relax regulations or remove the ban on cryptocurrency exchanges, yet the growing interest in the blockchain area indicates that China is working towards a new unregulated space which may require regulations. The PBC has been involved in the development of a new central bank digital currency, with the aim to maintain control over monetary sovereignty. It is working towards the concept of a virtual currency which would be issued by the state and constitute a valid currency.

Although ICOs and cryptocurrency exchanges are banned, the PBC has been involved in the development of a central bank digital currency. Authorities wish to maintain control over money, including virtual currencies. In order for virtual currencies to function in China, they must be established and distributed by the state. The PBC, together with government agencies, encourage the use of blockchain technology to revitalise financial services. Blockchain technology has received a positive response and has been encouraged in artificial intelligence. China is insistent that the growth of blockchain technology occurs without the use of tokens, in order to mitigate illegal fundraising and financial crime.

Japan

Cryptocurrency has had a positive response in Japan. Japan was the first country to provide a legal definition of the term 'virtual currency' and introduced the registration of entities as 'virtual currency exchange service providers'.

Japanese authorities subsequently put forward a bill to amend the Payment Services Act (PSA) and the Act on Prevention of Transfer of Criminal Proceeds (APTCP) which was approved in April 2017 by the National Diet of Japan. This act was based on the recommendations proposed by the Financial Action Task Force (FATF) report, *'Guidance for a Risk-based Approach to Virtual Currency'*, published in June 2015. The report advised the implementation of a registration or licensing procedure which would enable compliance with anti-money laundering and countering the financing of terrorism (AML/CFT) regulations. Despite the increasing popularity of virtual currencies, cryptocurrency is not treated as legal tender and is not supported by the Central Bank of Japan (BOJ). Consequently, the BOJ published the working paper, *'Digital Innovation, Data Revolution and Central Bank Digital Currency'*, in February 2019. The paper makes clear that the BOJ does not – at present – intend to issue its own digital currency due to the wider consequences that could impact payment efficiency and damage the existing monetary transmission mechanism. However, the paper indicates that the BOJ will consider expanding digital information technology in accordance with fiat currencies in the near future. Later, in January 2018, the prominent cryptocurrency exchange ('Coin check Inc.'), endured a loss of USD 530 million due to a cyber-attack. Following this (in March 2018), the Financial Services Agency of Japan (FSA) created a Study Group on Virtual Currency Exchange Business to explore the regulatory landscape in relation to exchange services. The Study Group produced the *'Report from Study Group on Virtual Currency Exchange Services'* in December 2018. The report summarises the risks and implications associated with the use of virtual currency and its potential to breach AML/CFT regulations. The report also provides details of regulations for virtual services concerning exchange services, derivative trading, and investment-type ICOs. In March 2019, the report played a substantial role in the revision of the PSA, in their proposed legal framework to regulate virtual currencies. Simultaneously, the bill proposed revisions to the Financial Instruments and Exchange Act (FIEA) to clarify the categorisation and regulations of virtual currency.

The bill to revise regulations on virtual currencies and ICOs in Japan included changes to the PSA and the FIEA. The PSA revisions proposed that the term 'cryptoasset' should be used instead of 'virtual currency' because 'cryptoasset' is internationally recognised and virtual currency is a broad category representing a range of instruments. The bill's aim is to regulate custody services, which includes the sale, purchase, and exchanges of cryptoassets, which were not governed prior to the amendment. With regard to revisions to the FIEA, the bill introduced the idea of 'Electronically Recorded Transferable Rights' (ERTR), and proposed applicable regulations.[48] The FIEA regulates traditional securities; however, securities issued using an electronic data processing system (for example, blockchain), have higher liquidity risks than traditional securities. Therefore, the FIEA Revisions recommended new regulations for securities which are transferable through the electronic data processing systems. Such securities have also been divided into three categories: 1) securities which are transferable through electronic data processing systems; 2) contractual rights, namely beneficiary interests and interests in collective investment schemes which have customarily been considered as securities and are transferable through electronic data processing systems; 3) contractual rights including trust beneficiary interests and interests in collective investment schemes, where negotiability is limited.[49] If the token rights satisfy the definition provided by the Interest of Collective Investment Schemes and ERTRs, such token rights will be included in the disclosure regulations of commercial dealings and monitored by the Cabinet Office Ordinance (COO).[50] Virtual currency derivatives were not initially applicable to financial regulations in Japan.

In accordance with Japanese legislation, virtual currency is not recognised as a security unless the characteristics of a particular token are subject to the FIEA. The PSA provides a definition for virtual currency and requires entities providing an exchange service to be registered with the FSA.

However, the bill introduced regulations managing cryptoasset derivative transactions and unfair acts in cryptoasset, or cryptoasset derivative, transactions. Such transactions are now subject to regulations under the FIEA. The bill was approved in May 2019 by the National Diet of Japan and came into force in May 2020.

In accordance with Japanese legislation, virtual currency is not recognised as a security unless the characteristics of a particular token are subject to the FIEA. The PSA provides a definition for virtual currency and requires entities providing an exchange service to be registered with the FSA. Entities that fail to register will be held accountable through criminal proceedings and penalties, thus both definitions of virtual currency and virtual currency exchange service provider hold significance. Under Article 2 (5) of the PSA, the term 'virtual currency' means: *"(i) property value (limited to that which is recorded on an electronic device or any other object by electronic means, and excluding the Japanese currency, foreign currencies, and Currency-Denominated Assets; the same applies in the following item) which can be used in relation to unspecified persons for the purpose of paying consideration for the purchase or leasing of goods or the receipt of provision of services and can also be purchased from and sold to unspecified persons acting as counterparties, and which can be transferred by means of an electronic data processing system; and (ii) property value which can be mutually exchanged with what is set forth in the preceding item with unspecified persons acting as counterparties, and which can be transferred by means of an electronic data processing system."* The revised PSA replaced the term 'virtual currency' to 'cryptoasset' but the definition remains the same. The PSA also explained the term 'virtual currency exchange services' and stated that for the terms of a virtual exchange service to be met the following conditions in the course of trade should be present: *"(i) purchase and sale of a Virtual Currency or exchange with another Virtual Currency; (ii) intermediary, brokerage or agency services for the act set forth in the preceding item; and (iii) management of users' money or Virtual Currency, carried out by persons in connection with their acts set forth in the preceding two items."*

The custody services of cryptoassets share similar risks with exchange services. Such risks include bankruptcy, money laundering, terrorist financing, and fraudulent activities. The PSA revisions attempt to address these issues by stating that managing cryptoassets for others would establish an exchange service. Consequently, the cryptoasset custody service would constitute an exchange service regardless of whether it involves any of the acts listed under virtual currency exchange services. Article 63 (2) of the PSA stipulates that all exchange providers must be registered. Article 63 (2) of the PSA demonstrates that the process of application for registration includes the submission of a written application for registration containing the following: *"(i) trade name and address; (ii) amount of capital; (iii) name and location of*

the business office pertaining to the virtual currency exchanges service; and (iv) name of director and company auditor". Subsequently, the FSA requires applicants to complete a checklist of 400 questions to ensure they can securely carry out the exchange service. As a result, the register containing the list of exchange service providers is made accessible to the public. The exchange provider is required to implement various measures in order to protect users, safeguard information and introduce disclosure requirements.

The sale, purchase, and exchange of virtual currencies are not within the remit of conventional securities as defined under the FIEA. Tokens satisfy the definition of virtual currency and are subject to the PSA. If the token was issued through an ICO and has already been dealt with by Japanese or foreign exchanges, the tokens can be considered as virtual currency under the PSA, so long as the exchange market for such tokens exists. In June 2019, the Japan Virtual Currency Exchange Association (JVCEA) (a self-regulatory organisation created under the PSA) issued a range of guidance to clarify the requirements associated with cryptoassets. These requirements included: information about the token, including its purpose for the funds; separated management of funds, including both fiat and cryptoassets acquired by ICOs; and appropriate valuation of the token issued.

The other type of token that falls under securities legislation is subject to the FIEA revisions and the newly introduced concept of ERTRs. This concept explains the nature of tokens which are governed by the FIEA. The ERTRs are relevant to Article 2 (2) of the FIEA which represents proprietary value because it is transferable through an electronic data processing system, eliminating the rights that are mentioned in the relevant COO in regard to their negotiability. Although Article 2 (2) of the FIEA refers to manifold rights, the security token offerings (STO) amount to the Collective Investment Scheme Interests (CISI) under the FIEA. To establish a CISI the three following requirements should be fulfilled: if the investor has used fiat currencies or other assets to contribute to a business; the moneys or other assets are used to invest in the business; and investors are granted the right to returns of profits or assets deriving from the business investments. Moreover, if the tokens share similar characteristics to prepaid cards and can be used as consideration for goods or services, these can be considered "prepaid payment instruments" which are subject to the PSA.

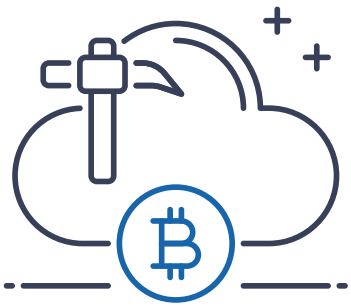
The FIEA revisions introduce regulations for cryptoasset derivative transactions in order to protect consumers and ensure secure and efficient dealings. In particular, derivative transactions including financial instruments or financial indicators have been subject to entry regulations in the FIEA. Cryptoassets are therefore incorporated under the definition of financial instruments in the FIEA. Additional factors such as prices and interest rates have been included in the definition of financial indicators. Since cryptoassets have been incorporated into the financial instruments definition, over-the-counter derivative transactions associated with cryptoassets or intermediary actions will establish a financial instruments business under the FIEA. Such transactions are formed by direct trading between two parties without an intermediary service. Furthermore, the FIEA revisions also introduce regulations that prohibit unfair acts in cryptoasset or cryptoasset derivative transactions. FIEA lists dissemination of rumours, fraudulent activities, intimidation, and market manipulation as examples of these acts. These unlawful acts are accompanied by penalties and legal action thereby tightening consumer protection and averting unjustifiable advantage.

The consumption tax of cryptoassets has been an important and prevailing issue in Japan. Initially, the sale of cryptoassets was subject to consumption tax if the office of the transferor was situated in Japan. However, after a series of revisions to Japan's tax laws (particularly in July 2017), consumption tax was no longer enforced on the sale of cryptoassets. This was subject to the cryptoasset in question and whether it satisfied the definition of cryptoassets under the PSA. The National Tax Agency (NTA) of Japan published the *'National Tax Agency Report 2019'* which specified that the NTA is organising campaigns to help those engaging in cryptoasset transactions to calculate their income and provide advice for filing returns. For large businesses, the NTA is emphasising the significance of business management in relation to tax affairs in order to increase the amount of filed tax returns.

The APTCP stipulates that exchange providers are required to execute various procedures to mitigate financial crime and fraudulent activities (AML/CFT). These procedures include enhanced customer due diligence, verifying identification of the customer and any persons managing the business on the behalf of the customer for transactions, archiving records for seven years, and reporting suspicious transactions. The PSA highlights various penalties which infringe the bill; such penalties include imprisonment, penal labour, and monetary charges. Japan is also a member of the Asia/Pacific Group on Money Laundering which is conducted by FATF. In *'The FATF Report to G20 Leaders' Summit'* (June 2019), Japan showed its continued support to the implementation of FATF recommendations and to strengthen AML/CFT initiatives internationally. Japan has been progressive by expanding the existing legislation to include cryptoassets (virtual currency) in order to comply with FATF standards. Furthermore, Japan may add policies based on its Regulatory Sandbox Scheme which was founded in June 2018, conducted by the COO. The regulatory sandbox intends to explore emerging technology – including blockchain – and investigate regulatory concepts to evolve the industry locally and internationally.

Singapore

Singapore's government has shown a keen interest in developing the blockchain sector; the country has seen substantial growth in the number of industries using this technology. Singapore is recognised as a world-leading fintech centre and has therefore taken a balanced approach to the regulation of cryptocurrencies in order to avoid kerbing innovation.



Cryptocurrency exchanges are regulated by the existing legal frameworks where they are applicable. At present, Singapore does not consider cryptocurrencies as legal tender. In spite of this, the Monetary Authority of Singapore (MAS) has launched *Project Ubin* and is actively developing a digital currency which will be issued by the central bank. Regulators' primary focus has been to maintain a stable financial ecosystem while exploring the use of tokens to produce inexpensive and effective financial transactions. The use of cryptocurrencies as a means of payment has been supported, so long as persons are prepared to accept them as payment. However, cryptocurrencies cannot equate to a store of value due to the fluctuation of prices and they are not recommended as an investment tool.

Notably, there are many types of cryptocurrencies which have different properties and consequently different tokens will prompt their own individual regulatory framework. The Payment Services Act 2019 (PSA) provides the regulatory requirements for cryptocurrency exchange services available in Singapore. The PSA clarifies that the following services constitute a payment service and are subject to licensing requirements: *(a) an account issuance service; (b) a domestic money transfer service; (c) a cross-border money transfer service; (d) a merchant acquisition service; (e) an e-money issuance service; (f) a digital payment token service; and (g) a money-changing service.* Before the inauguration of the PSA, cryptocurrency exchanges were largely unregulated unless they satisfied the definitions under the Securities and Futures Act 2001 (SFA). However, the PSA has brought cryptocurrency exchanges into the scope of the regulation if activities include payment services. The PSA requires payment institutions to comply with licensing obligations. For example, Digital Payment Token (DPT) Services are defined as:

(a) "any service of dealing in digital payment tokens;

(b) any service of facilitating the exchange of digital payment tokens." This suggests that those carrying out activities using DPT are permitted to sell, purchase, or exchange tokens for fiat currencies or other DPT provided that they have obtained a licence.

In 2017, the MAS declared that it would regulate the issue or offer of digital tokens that constitute securities under the SFA.[51] The SFA is the principal securities legislation in Singapore and it imposes requirements on digital tokens. The revised definition of securities provided by the MAS will include: *"equity instruments representing legal or beneficial ownership interests and debt instruments, such as shares, debentures (including bonds) and units in a business trust. ETFs will fall under the revised definition of "units in a collective investment scheme".*[52] If the digital token satisfies the definition of regulated products under the SFA, entities will be required to obtain a licence. Section 240 (1) SFA stipulated that entities will need to register a prospectus with MAS in accordance with the provisions set out in Section 243 SFA. The prospectus should be signed, lodged, and registered by the MAS. In Section 272B (1) SFA lists exemptions from the requirement. Furthermore, service providers who distribute advice on security tokens may be subject to the Financial Advisers Act 2001 (FAA) licensing requirements. The SFA and FAA both have powers to operate outside the given jurisdiction; for example, an activity operating both inside and outside of Singapore would be considered as an activity taking place in Singapore. Activities which take place outside of Singapore but which have a prominent effect on Singapore are considered as being inside the country. Likewise, the FAA suggests that those carrying out any action which encourages the public to use any financial advisory service in Singapore – irrespective of the intended effect aimed outside of Singapore – is acting as a financial adviser.

Singapore set out a strict anti-money laundering (AML) and countering the financing of terrorism (CFT) regime on financial institutions in "*MAS Notice PSN02: Prevention of Money Laundering and Countering the Financing of Terrorism*" published in 2019.

Utility tokens usually include Initial Coin Offerings (ICO) or Initial Token Offerings (ITO). This process includes persons trading digital payment tokens to the issuer in exchange for digital tokens at a fixed exchange rate. Digital tokens are typically devised in order to be used as a means of payment for goods or services by the issuer. The MAS produced *'A Guide to Digital Token Offerings'* in 2018 which demonstrates how ICOs/ITOs may be regulated by the MAS. For example, if the digital tokens are capital markets products under the SFA, the offer or issue of digital tokens must comply with securities laws. Capital market products defined by the SFA include: "*securities, units in a collective investment scheme, derivatives contracts, spot foreign exchange contracts for the purposes of leveraged foreign exchange trading, and such other products as the Authority may prescribe as capital markets products.*" The MAS will therefore assess the structure and rights attached to the digital token in order to determine whether it constitutes a capital markets product under the SFA. Nonetheless, this makes the offering of security tokens burdensome and expensive due to the requirements of obtaining a licence and registering a prospectus. These policies are in place to protect consumers by providing them with sufficient information to make an informed decision. The regulatory framework also ensures service providers work within the proposed measures in order to deliver a fair and transparent service.

A popular type of tokenised assets is precious metals, where the issuer of a token owns a precious metal and provides participants with a reasonable price for that precious metal. The tokenisation of assets may trigger stipulations under the Commodity Trading Act 1992 (CTA) as spot commodity trading. The CTA defined spot commodity trading as: "*the purchase or sale of a commodity at its current market or spot price, where it is intended that such transaction results in the physical delivery of the commodity.*" Therefore, a spot commodity broker is "*a person whether as principal or agent who carries on the business of soliciting or accepting orders, for the purchase or sale of any commodity by way of spot commodity trading, whether or not the business is part of, or is carried on in conjunction with, any other business*" and will be required to obtain a licence.

The Income Tax Act 1947 is applicable to businesses accepting payment in virtual currencies which are to be treated as revenue. Individuals or entities using virtual currency for investment reasons may incur a capital gain but will not be subject to capital gains tax as this is not applicable in Singapore. However, individuals or entities who trade using virtual currencies for commercial purposes, will be taxed on the profit gained. Such profits may come from the mining or trading of virtual currencies and in these situations taxation will be determined on a case by case basis. Taxation on the proceeds from an ICO will be dependent on whether the proceeds can be considered revenue. The Inland Revenue Authority (IRAS) of Singapore published *"IRAS e-Tax Guide: Income Tax Treatment of Digital Tokens"* in April 2020. The guide explains that proceeds from issuing payment tokens can be taxed based on their particularities and circumstances; whereas proceeds from issuing utility tokens will be regarded as deferred revenue, and that the proceeds from issuing security tokens are not taxable. Last, Goods and Services Tax Act 1993 (GSTA), is applicable to the sale of virtual currencies where IRAS has confirmed the sale of tokens as supply of services which is subject to tax rules under GSTA.[53]

Singapore set out a strict anti-money laundering (AML) and countering the financing of terrorism (CFT) regime on financial institutions in *"MAS Notice PS-N02: Prevention of Money Laundering and Countering the Financing of Terrorism"* published in 2019. The notice requires fintech firms to implement supervisory controls and 'know your customer' procedures in order to review profiles and report suspicious transactions. The paper provided a sample risk assessment, for the mitigation of such risks, which includes identification and verification processes as well as on-going monitoring responsibilities by financial institutions. MAS also published *"Guidelines to MAS Notice PS-N02 on Prevention of Money Laundering and Countering the Financing of Terrorism"* in 2020. The paper clarified definitions of key concepts and demonstrates examples of applying a risk-based approach to emerging technologies. The guidance further distinguished between simple and enhanced approaches to customer due diligence and provided examples in which each needs to be practiced. Furthermore,

the paper highlighted potential money laundering and terrorist financing risks arising from the use of virtual currencies. The MAS confirmed that Singapore recognises the range of risks involved for investors in relation to virtual assets. The MAS also highlighted the statutory provisions under the SFA which observe the AML/CFT guidelines. It is clear that the ambiguous nature of virtual currencies requires a stricter approach to the AML/CFT regime, particularly due to anonymous features of digital tokens. Authorities in Singapore have clarified the importance of adhering to AML/CFT guidelines and have suggested that the relevant provisions do not separate virtual currency and fiat currency transactions in this context. AML/CFT stipulations are therefore applicable to all dealings within the financial sector.

The MAS published the *"Consultation Paper on the Proposed Payment Services Notices on Prevention of Money Laundering and Countering the Financing of Terrorism"* in 2019. The paper explained that many money laundering and terrorist financing risks were associated with transactions using the digital payment token services, because of the inherent features of anonymity, and faster transactions across national borders. Therefore, the MAS suggested that AML/CFT provisions were to be imposed on licensees under the PSA which would include digital payment token services that trade in, or facilitate the exchange of, digital payment tokens (including the buying and selling of digital payment tokens like bitcoin), for fiat currency or another digital payment token. The paper suggested the implementation of the Financial Action Task Force standards and upcoming amendments to the PSA to deliver further AML/CFT regulations.

In December 2019, MAS issued a consultation paper *'The Consultation on the Payment Services Act 2019: Scope of E-money and Digital Payment Tokens'* requesting feedback for the scope of e-money and digital payment tokens, while simultaneously focusing on regulatory aspects used by these payment methods. For example, further innovation has led to the formation of stablecoins which has challenged the concept of 'money' under the PSA. The consultation paper outlined the differences between e-money and digital payment tokens and sought a response from relevant industries. Stablecoins can potentially satisfy elements in each of these categories as well as constructing unique classifications. The consultation closed in January 2020 and MAS's decision is widely anticipated since it will not be revising the definitions of e-money or digital payment tokens. MAS established a Fintech Regulatory Sandbox to provide financial institutions and consumers with the opportunity to trial innovative financial services. MAS will establish applicable regulatory guidelines, contingent on the outcome of the trials. Currently, the sandbox stipulates legal and regulatory requirements to ensure a safe environment. The MAS has appointed penalties for any disruptions, to prevent harm to the nation's financial system. It is clear that Singapore has acknowledged the significance of a regulatory framework and is addressing any concerns raised. The fintech sector has had positive developments and authorities are prepared to bring digital tokens into the regulatory field.

South Korea

There is huge public interest in cryptocurrencies and distributed ledger technology (DLT) in South Korea. The South Korean government has focused on the development of blockchain technology. However, there are no clear legal frameworks regulating cryptocurrency space in this country.

In 2017, the Financial Supervisory Service (FSS) announced in a press release that cryptocurrencies are not associated with the financial regulatory landscape. The FSS provided a list of the following items which do not constititute cryptocurrencies: fiat currencies; prepaid electronic means or electronic currencies; or financial investment instruments. However, the FSS did not provide any indication of the legal status or classification of cryptocurrencies. Authorities have expressed their concern about consumer protection in relation to cryptocurrency and have also highlighted the correlation between cryptocurrencies and illicit activities such as money laundering and terrorist financing. In spite of the lack of regulations, the decision ruled by the Supreme Court of South Korea in 2018 suggested that cryptocurrencies could be confiscated as criminal proceeds, particularly because they represent economic value and can be categorised as property. The decision incorporated a narrow scope of interpretation which makes it unclear as to how the judgement will influence upcoming cryptocurrency regulations. South Korea has only just initiated its regulatory perspective on cryptocurrencies and is still due to provide clear guidelines relating to its legal status. Currently, cryptocurrencies are not considered legal tender in South Korea; however, the Bank of South Korea generated a task force to review the possibilities of backing its own cryptocurrency.

At present, regulators are uncertain in their approach towards virtual currencies. For example, the Financial Services Commission (FSC) issued a press release *'Special Measures to Eradicate Virtual Currency Speculation'* in September 2017 which banned people from facilitating trade with margin trading, loaning funds or cryptocurrencies from crypto exchanges. The FSC proclaimed these actions infringed the existing arrangements of lending, and credit laws, in South Korea. Therefore, the FSC deterred financial institutions from participating in transactions that contributed to these activities. In September 2017, the FSC published a warning against Initial Coin Offerings (ICOs) which hinder South Korea's securities law (Financial Investment Services and Capital Markets Act 2017, FSCMA). Nonetheless, authorities did not clarify how, and in which situations, these aspects could violate provisions in the FSCMA. If coins share similar properties with securities under the FSCMA, ICOs would have to abide by the restrictions on offerings outlined in the act. Whereas, coins, not constituting securities, could bring the legality of the ICO into question as there are no clear exclusions on offerings that do not hinder the existing legislation. Later, in September 2017, it was announced that any type of ICO is prohibited. Significantly, the FSC stated that it would introduce new policies regarding identification for accounts related to cryptocurrency exchanges. By January 2018, a *'Real Name Verification System'* was initiated which meant existing anonymous participants could only draw out remaining money and not make additional payments. Following this update, new participants will have to verify their identification before opening a cryptocurrency account. For the second time in 2017 the government banned financial companies from accommodating cryptocurrency exchanges of Bitcoin Futures. In January 2019, the FSS published a press release detailing the investigation it held on 22 different ICOs in 2018 which highlighted its condemnation of illegal activities associated with ICOs.

As there are no existing regulatory frameworks governing cryptocurrencies, authorities could apply existing South Korean legislation in order to regulate the space. The FSCMA defines securities as *"financial investment instruments issued by a citizen of Korea or a foreigner, for which investors do not owe any obligation to pay anything further on any ground, in addition to the money or similar that the investors paid at the time of acquiring such instruments."* The facts and circumstances of a token will be used to decide whether it can be categorised as a security. Furthermore, if an ICO has

similar characteristics to securities, as described in the FSCMA, it must represent the restrictions set out in the act. For example, making an offering of securities to fifty or more non-accredited investors would be treated as a public offering which would trigger offering restrictions. Even sales including fewer than fifty investors can constitute a public offer which would prompt issuers to provide a securities registration statement and an authorisation by the FSC. However, it is still uncertain whether cryptocurrencies constitute securities under the FSCMA. Cryptocurrencies, like bitcoin, have not been categorised as securities and are not subject to commodities laws in South Korea; therefore, no regulations exist for the sale of bitcoin or similar cryptocurrencies. Financial regulators have cautioned potential investors that institutions will not accept cryptocurrencies or cryptoassets as a financial investment product. Nevertheless, this statement was not made for the purpose of legal interpretation but as a warning to ensure consumer protection. The tax treatment of cryptocurrencies in South Korea is unclear. Cryptocurrencies are currently untaxed but the Ministry of Strategy and Finance has announced an upcoming review on taxation.

South Korea has introduced the *'Real Name Account System"* to remove anonymity and allow trading in cryptocurrencies. The FSC published *"Special Measure for the Elimination of Virtual Currency Speculation"* which explained the introduction of these special measures and stipulated that participants will be obliged to create a bank account to use virtual services. The dealer will have to verify the identity of the trader and register the trader's account with the bank. According to the Act on Reporting and Using Specified Financial Transaction Information (ARUSFT), financial institutions must monitor, file, and report suspicious transactions to South Korea's Financial Intelligence Unit. Transactions in cryptocurrency with a single user involving KRW 10 million (or more) in one day, or KRW 20 million (or more) over a seven day period, should be reported. Likewise, several transactions between a cryptocurrency exchange and a single user on five occasions or more in one day, or seven occasions or more within a seven day period, should also be reported. ARUSFT also provided strict customer due diligence requirements on financial institutions, including enhanced identity checks and record keeping and states: *"i) Where a customer opens an account or makes a single financial transaction of equal to or more than the amount prescribed by Presidential Decree: verification of matters prescribed by Presidential Decree, with regard to the personal information of the relevant party to a financial transaction; ii) Where it is apprehended that a customer will commit money laundering or financing of terrorism, such as cases where there is any suspicion as to whether he/she is the actual party to the financial transaction: verification as to whether the customer is the actual party to the financial transaction, and the purposes of the financial transaction."* The FSC published *"Amendments Proposed to the Enforcement Decree of the Act on Reporting and Use of Certain Financial Information"* in 2018 with the aim to enhance compliance of the international AML/CFT standards set forth by the Financial Action Task Force (FATF). After much consideration, South Korea has proposed a range of bills to regulate cryptocurrency in the National Assembly. The bills include licensing and supervisory requirements and anti-money laundering measures. However, these bills are pending and are yet to be enacted into Korean law. The bills would classify virtual currencies into digital assets and impose registration requirements with the FSC and Financial Intelligence Unit. Participants would also have to adhere to all AML/CFT regulations which will drive South Korea to meet the policies in the AML/CFT regime directed by FATF. In March 2020, the National Assembly of Korea passed the Amendment to the Act on Reporting and Use of Certain Financial Transactions Information (Amended AML Act). The amendment makes the existing AML requirements applicable to crypto asset service providers and will take effect in March 2021. Nevertheless, the authorities have declared that the regulation does not support cryptocurrency activities or offer any verification.

In summary, the government is prepared to invest in the development of blockchain technology and is reluctant to endorse cryptocurrencies. Authorities have clearly expressed the potential danger of engaging in cryptocurrencies, particularly ICOs; whereas blockchain technology fosters innovation which can enhance the economy without harming the integrity of the financial system. There has been no indication of upcoming legislation (apart from the Amended AML Act) but a concise regulatory framework is expected. South Korea has launched a financial regulatory sandbox *'Sandbox Korea'* which provides a chance for financial services and consumers to test innovative products in the market. The regulatory sandbox also provides an opportunity for regulators to explore the environment and develop regulations based on the outcomes of the trials.

India

The development and application of blockchain technology in India has increased significantly, particularly with the support of the Reserve Bank of India (RBI).

The development and application of blockchain technology in India has increased significantly, particularly with the support of the Reserve Bank of India (RBI). In March 2017, the Deputy Governor of the RBI delivered a speech entitled *'FinTech's and Virtual Currency'* which the RBI later published as *'Distributed Ledger Technology, Blockchain and Central Banks'* in February 2020. The article laid out the benefits of evolving blockchain technology. Indian residents have shown a key interest in using virtual currency and in spite of the government's motivation to promote financial technology (fintech), virtual currency is distinguished from legal tender. In December 2013 and February 2017, the RBI issued a press release cautioning members of the public against the use of virtual currency and stated that those engaging in such activities are doing so at their own risk. The RBI clarified that they have not issued licences nor authorised entities to operate such services. These press releases made the RBI's position clear and acknowledged the risks associated with virtual currency. Although the Indian government has not provided a definition for virtual currency, it continues to support prepaid instruments in exchange for products or services available on the platform.

The RBI published *'The Circular'* in April 2018, which declared a prohibition on all RBI regulated entities from dealing in cryptocurrencies. This was initiated due to the associated risks of virtual currency. Not only does the RBI consider virtual currency to lack intrinsic value but thinks that the anonymity given to the holder proactively aids money laundering and terrorist financing. Furthermore, proposals for Know-Your-Customer (KYC) and verification of user identity does not actively prevent fraudulent activities because the identification process is difficult to implement alongside the anonymous features. Another common issue amongst regulators is the lack of control exercised by a central authority over virtual currency transactions. Therefore, such entities were given a three month period to withdraw from all accounts engaging in cryptocurrency. Although the RBI did not directly ban the use of cryptocurrency, it actively obstructed any financial transactions between parties. The Securities Exchange Control of India (SEBI) has not declared its position on virtual currencies. In July 2019, the Inter-Ministerial Committee (IMC) issued a press release *'Report of the Committee on Virtual Currencies'* which proposed a regulatory approach for distributed ledger technology (DLT) and further development of virtual currency. The Committee suggested a blanket prohibition on the use of virtual currencies, together with the introduction of criminal prosecution and penalties for offenders. Last, the Committee recommended that the government remain neutral on a national digital currency until further studies had been carried out.

After the RBI issued the circular in April 2018, the case *'Internet and Mobile Association (IMA) v Reserve Bank of India (RBI)'* was brought to the Supreme Court of India (in March 2020). In this case, the circular was challenged on two grounds: that the RBI did not have the powers to authorise prohibitions on virtual currency dealings as it was not in their regulatory framework; that the circular unreasonably breached the petitioner's rights. The Supreme Court of India acknowledged that virtual currency belonged in its own category and differed from traditional currency. However, the court determined that although virtual currency is not treated as legal tender, it maintains similar functions to fiat currencies and consequently the RBI had the authority to action its regulatory power. Although, the court found that virtual currencies are manageable under the RBI, the court further inspected the test of proportionality on the circular. The doctrine of proportionality asserts that if reasonable restrictions were afforded, where business operations were not adversely affected, those restrictions should be adopted. In essence, the restrictions have to be proportionate to the concerns at hand. Therefore, the court maintained that

For the anti-money laundering and countering the financing of terrorism (AML/CFT) in India, procedures such as KYC and enhanced customer due diligence (CDD) have been embedded in various legislations under Indian law and RBI guidance.

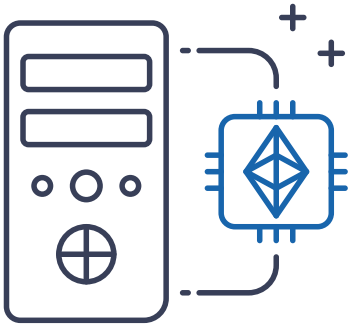
the circular was disproportionate because entities engaged in the virtual currencies had suffered a substantial loss. The court relied on various regulatory approaches from different jurisdictions and concluded that alternative measures were applicable in order to achieve its objective. The court determined that regulations would be a sustainable approach for mitigating the risks associated with virtual currency. Consequently, the court set the restriction aside which no longer constitutes valid law, while the RBI retracted the prohibition on financial institutions from dealing with virtual currency activities.

Because the use of virtual currencies facilitates a value exchange, Section 2 (1) Payment and Settlement Systems Act 2007 (PSSA) defines a payment system as *'a system that enables payment to be effected between a payer and a beneficiary'*. If the virtual currency system amounts to a payment system, Section 4 (1) PSSA requires that those engaging in such activities obtain authorisation from the RBI. The PSSA refers to payment systems rather than specific terms such as currency or legal tender. This means that virtual currency systems will need to be determined on a case by case basis with a view to whether the system facilitates payment between a purchaser and a beneficiary. However, many virtual currency based systems do not enable this action; for example, some people purchase virtual currency for investment purposes (and do not make payments) which can then be exchanged for fiat currencies. In this instance, the definition of a payment system is not satisfied and reflects the sale and purchase of an asset. Virtual currency holders are also not able to exchange them for value to the issuer unless through a sale in the ordinary market meaning that the value behind the virtual currency is not backed by the issuer, which suggests that a virtual currency is not likely to be treated a payment system. Furthermore, due to the anonymous nature of decentralised virtual currencies, regulators would not be able to direct issuers. In accordance with the decision in the *IAMAI* case, virtual currencies do not constitute a payment system under the PSSA.

According to Indian legislation and regulatory frameworks, virtual currencies are not currently treated as securities. Virtual currencies have not been incorporated in the definition of securities under the Securities Contracts (Regulation) Act 1956 (SCRA). The inference that can be drawn from this is that virtual currencies, such as bitcoin, do not provide an identifiable issuer in contrast with traditional securities. Tokens issued through Initial Coin Offerings (ICOs) can fall within the scope of the SCRA if they satisfy its requirements, alongside an identifiable issuer. In such instances, tokens may be subject to the Companies Act 2013 and the SCRA. Ultimately, the industry and its consumers are waiting for the government's response for regulation of virtual currency. Previously, the RBI had communicated its concerns in relation to the risks associated with the use of virtual currency. Money laundering and terrorist financing have been highlighted numerous times as a primary concern. As for the anti-money laundering and countering the financing of terrorism (AML/CFT) directives in India, procedures such as KYC and enhanced customer due diligence (CDD) have been embedded in various legislations under Indian law and RBI guidance. Although the procedures have not been made directly applicable to virtual currencies, regulatory frameworks (for example, Prevention of Money-Laundering Act 2002 and the RBI Master Direction – Know Your Customer Direction 2016) are applicable to businesses regulated by the RBI. The regulatory landscape of virtual currencies in India remains unclear. If regulators can implement a sustainable framework, swift progress can be made in fintech and innovation, both locally and internationally.

Russia

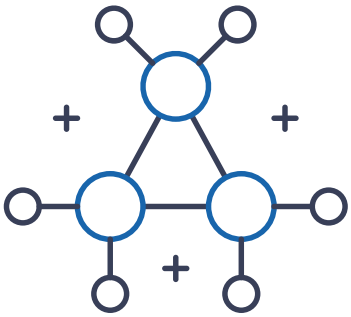
Russia intially welcomed the use of virtual currency and blockchain technology. However, given the risks associated with the characteristics of cryptocurrency, Russian authorities have subsequently taken a different perspective. The government has continued to support the innovation of blockchain but authorities have concentrated on relevant anti-money laundering measures.



The Central Bank of Russia (CBR) and the Ministry of Finance are the primary regulators for emerging financial technologies (fintech) in Russia. At present, there are no statutory frameworks governing the use of virtual currencies and no relevant definitions have been provided. Article 27 of the Federal Law "On the Central Bank of the Russian Federation" clearly expresses that the rouble is the only currency recognised as legal tender and the only means of payment in Russia. Furthermore, the Federal Law of the CBR Federation of 2002 specifies that the rouble is the only national currency and that any other currency – or currency substitute – is unknown in the jurisdiction. The suggestion that can be drawn from this is that virtual currency reflects a currency substitute, rendering it unknown. Furthermore, in January 2014, the CBR published a press release, *'On the use of "Virtual Currencies" in transactions, in particular, Bitcoin'*, which warned the public of the risks associated in trading with virtual currency and of increased possibilities of money laundering and terrorist financing. The Russian authorities do not maintain the same view for blockchain technology and intend to amend the Civil Code to implement smart contracts. However, the regulatory landscape for emerging technologies remains unclear as Russia has not explored the wider perimeters beyond their traditional systems, which may impede existing regimes. Furthermore, the Russian Supreme Court modified the 'Supreme Court Plenum Decree' in February 2019, which lays out crimes of money laundering. The amendment made clear that offenders gaining virtual assets from the result of a crime are subject to Article 174 and Article 174.1 of the Russian Civil Code on grounds of obtaining funds illegally. These changes were made in relation to Recommendation 15 provided by the Financial Action Task Force (FATF).

Moreover, the State Duma (the lower house of the Federal Assembly of Russia), has attempted to introduce regulations for virtual currency. The Draft Law on Digital Financial Assets is applicable to any legal entity, regardless of residency and availability to the wider public. The CBR announced that the draft law had been approved in its second reading in July 2020. In August 2019, the CBR made an announcement (*'Russia introduces first law regulating digital rights'*) which included amendments to the Russian Civil Code to provide legal instruments for investors and regulated agreements actioned through information technology systems in order to finance investments. Regulators are considering the framework for this category of rights and also the regulation of virtual currencies. The Russian Civil Code was amended by law in "On Introduction of Changes to Parts One, Two and Four of the Civil Code of the Russian Federation" (Digital Rights Law). The Digital Rights Law was enforced in October 2019 and did not explicitly refer to virtual currency; however, it was the first attempt at adopting regulations which involve virtual currencies. Through the Digital Rights Law, Article 141.1 was introduced in the Civil Code, which provides a definition for digital rights as well as the conditions and policies for exercising such rights. The Digital Rights Law amends Article 128 of the Civil Code on the objects of civil rights which is applicable to civil law entitlements and transactions. The objects include money, securities, and property rights, and now digital rights have also been included. This suggests that the Civil Code acknowledges that digital rights are assets. Although cryptocurrency has not been mentioned, the definition can include virtual currency. Last, the Digital Rights Law amends Articles 160 and 309 of the Civil Code which regulates fulfilment of obligations and agreements. The amendment of these articles will enable parties to make transactions using electronic or digital means which includes smart contracts.

Nevertheless, additional initiatives have been proposed to regulate virtual currency matters; for example, a draft law "On Digital Financial Assets". This law contributes to key aspects regarding issuance, exchanges, and



transactions through Initial Coin Offerings (ICOs), and is often referred to Digital Financial Assets Law. Another draft law "On Attracting Investments with the Use of Investment Platforms" lays out regulations for ICOs or Initial Token Offerings (ITO). However, these draft laws are awaiting approval and are in the process of re-organisation for compliance with the Digital Rights Law. The draft law for the Digital Financial Assets Law is a staple piece of regulation for the governance of virtual currencies. Since 2019, the State Duma proposed to adopt the legislation; however, the second reading has not yet been approved. Notably, there are mixed opinions within Russian authorities whether to either ban or regulate virtual currencies. The outcome of the draft laws may reflect strict regulations against virtual currency and could stifle innovation. For example, the draft law proposes authorised categories can only operate trade with digital assets, which includes traditional financial institutions. Such operators will need to register with the CBR and must be Russian legal entities. Entities issuing digital financial assets must provide information on the issuer, beneficial owners, the scope of rights, and whether smart contracts have been utilised to sell or purchase digital financial assets. Moreover, there is no explicit legislation addressing the tax treatment of virtual currencies; however, the Tax Code of the Russian Federation is applicable. In November 2018, the Ministry of Finance clarified that all profits gained from cryptocurrency related activities are subject to personal income tax. The PWC Report provided a summary of the initiatives delivered by the Ministry of Finance. The report explicitly noted, *inter alia*, that any economic benefit gained from transactions using cryptocurrency is taxable for all tax payers and must be paid through income tax. The taxpayer is obliged to calculate the taxable amount and file the tax declaration themselves.

The primary legislation providing anti-money laundering and countering the financing of terrorism (AML/CFT) policies in Russia is Federal Law No. 115-FZ "On Counteracting Legalisation (Laundering) of Illegal Income and Terrorism Financing" (August 2001). Secondary regulations have been provided by the Federal Financial Monitoring Service, the CBR, and the Federal Tax Service. Although there are no explicit legislations that address virtual currencies, the draft laws intend to amend the AML/CFT laws to incorporate digital financial assets. For example, the draft legislation proposes that trade operators and informational system operators will be accountable under the AML/CFT regulations. The draft law proposes a number of procedures including enhanced identification processes, record keeping, internal control and compliance program, and suspicious transaction reporting to relevant authorities. In September 2017, the CRB issued an *'Information Letter'* warning consumers about possible illegalities surrounding transactions using virtual currency. The CRB warned consumers about engaging in transactions with anonymous users, to prevent money laundering and terrorist financing activities. Furthermore, the CRB stressed that using virtual currencies is still a young concept in Russia. Subsequently, in April 2018, the CRB initiated trials of a regulatory sandbox in order to explore various fintech innovations without infringing on Russia's existing legislations. The regulatory sandbox was developed to investigate the regulatory landscape, and the Russian Ministry of Economic Development created a draft law "On Experimental Legal Regimes in the Sphere of Digital Innovations in the Russian Federation". The intention of this draft law was to introduce relaxed AML/CFT policies to manage digital technologies and make progress in innovation. Ultimately, Russian regulators and authorities are working towards constructing a stable framework for virtual currencies.

Australia

Australia has taken a constructive approach towards the regulatory framework of cryptocurrency and innovation. Its aim is to develop regulatory mechanisms to manage the growth of innovative technology. The Australian government is determined to progress cryptocurrency and distributed ledger technology (DLT).

For example, the launch of the Digital Transformation Agency 2018-25 pilots blockchain systems, together with government services, in an attempt to build trust with residents and reduce costs. During Australia's Payment Summit 2017 the Governor of the Reserve Bank of Australia (RBA) clarified that the RBA is not issuing an Australian digital dollar but exploring the possible impact of an electronic currency issued by the central bank. Financial regulators think that cryptocurrencies are volatile and unstable, and aid illegal transactions. The Australian approach to emerging technologies represents a speculative interest until appropriate measures are developed to eliminate difficulties using cryptocurrencies. Australia does not consider cryptocurrencies as legal tender but has nonetheless shown great enthusiasm towards DLT and is actively developing strategies and regulatory frameworks for this space.

Australia has not produced independent legislation to regulate cryptocurrencies but legislation has been incorporated into existing financial laws. The legislation itself has not been adjusted to accommodate cryptocurrencies but instead Australia's Securities and Investments Commission (ASIC) has actioned a series of reports and guidance on how cryptocurrencies may sit within the existing legislature. In particular, authorities have given specific attention to methods of trading and exchange services, while also examining the nature of cryptocurrencies. As there are no remote statutory arrangements for the proprietorship of cryptocurrencies or cryptoassets, depending on their characteristics and structure, they may constitute *'a financial product'*, bringing them under the scope of the Corporations Act 2001 (CA 2001). The act administers regulations of securities in Australia and defines a *'financial product'* as: "*(a) makes a financial investment, (b) manages financial risk and (c) makes non-cash payments*". The following chapters of the CA 2001 provide a potential regulatory framework for virtual currencies. Chapter 6D CA 2001 regulates the fundraising of financial products and stipulates disclosure requirements and procedures of offering securities. Chapter 7 CA 2001 provides regulatory requirements for financial services and markets, disclosures relating to sales, and purchases of financial products. Importantly, regulations of virtual currencies are dependent on whether they meet the definition of a financial product provided by the CA 2001. Bitcoin is not considered a financial product but should be treated as property under Australian law. Other cryptocurrencies which share similar properties to bitcoin will be evaluated by their structures to determine their resemblance to a financial product. This may prove difficult as the nature of cryptocurrencies does not easily equate with the conventional financial classifications. However, recent guidance provided by the ASIC offers advice on how virtual currencies may be classified as financial products.

The act provides a broad criteria for the definition of financial products. The ASIC has provided clarification through an information sheet "*INFO 225 Initial Coin Offerings and Cryptoassets*" (INFO 225). INFO 225 claimed that cryptocurrencies whose properties can be compared with those of financial products are subject to the obligations under the CA 2001 and the Australian Securities and Investments Commission Act 2001 (ASIC Act). These regulations apply to members considering to raise funds through an ICO or maintaining a business that involves cryptoassets and cryptocurrency tokens. The guidance offers a range of papers that demonstrate how statutory obligations will apply to issuers, cryptoasset intermediaries, transaction processes, trading platforms, and consumers. For example, *"Regulatory Guide 1: AFS Licensing Kit"* (RG 1) explained that issuers of cryptoassets and tokens qualifying as financial products will be obligated to hold an Australian Financial Services License (AFSL). This includes wallet and custody service providers who will also be required

"*INFO 225 Initial Coin Offerings and Cryptoassets*" (INFO 225) states that cryptocurrencies whose properties can be compared with those of financial products are subject to the obligations under the CA 2001 and the Australian Securities and Investments Commission Act 2001 (ASIC Act). These regulations apply to members considering to raise funds through an ICO or maintaining a business that involves cryptoassets and cryptocurrency tokens.

to hold necessary depositary authorisations. Likewise, *"Regulatory Guide 36: Licencing Financial Product Advice and Dealing"* (RG 26) confirms that cryptoasset intermediaries are also captured by the AFSL requirement. This includes those issuing advice on trading or offering a type of intermediary service for cryptoassets. The guide highlights that those offering a cryptocurrency related service must satisfy the definition of a financial product provided by the CA 2001. Furthermore, the guide provided a comprehensive summary on aspects that constitute a financial product service which includes *'providing financial product advice'*, *'dealing in a financial product'*, *'arranging'*, and elements that satisfy the business test. The business test determines whether a person provides a financial service using *'system, repetition and continuity'*, consequently initiating licensing requirements.

The following guide, *"Regulatory Guide 211: Clearing and Settlement Facilities: Australian and Overseas Operators"* (RG 211), is for miners and transactions processors involved in the clearing and settlement (CS) process for cryptoassets. The guidance explains the application and exemption processes, including the subsequent steps after the licence has been administered. Service providers managing a CS facility in Australia or overseas are therefore required to obtain a CS facility licence, unless they have been exempted by the minister.[54] The requirements imposed by the licence are noted in the CA 2001, and include observance of the RBA's economic values while reducing systemic risks. The licensees must also supply a fair and effective service when managing conflicts of interest and ensure efficient supervisory measures.[55] The obligations on licensees continue after they have been granted a licence; this involves compiling an annual report containing a self-assessment of the provisions implemented. These obligations have been imposed to maintain a stable financial system, while highlighting the importance of protecting investors involved in financial products and CS facilities.

Furthermore, *"Regulatory Guide 172: Financial Markets: Domestic and Overseas Operators"* (RG 172) contains information on licensing obligations applicable to cryptoasset exchanges and trading platforms. For example, the guide laid out whether cryptoasset transactions when cleared or settled will activate a CS facility, thereby requiring a CS facility licence. Section 791A CA 2001 communicates that those operating a financial market in Australia must obtain an Australian market licence or an exemption. Section 767A CA 2001 defined a financial market broadly to include a variety of market places and constituted a facility which:

(a) *"offers to acquire or dispose of financial products are regularly made or accepted; or*

(b) *offers or invitations are regularly made to acquire or dispose of financial products that are intended to result or may reasonably be expected to result, directly or indirectly, in:*

(i) *the making of offers to acquire or dispose of financial products; or*

(ii) *the acceptance of such offers."* RG 172 also stated that the definition applies to all forms of technology or physical structures that would allow persons to trade through the use of the facility. The guidance also highlighted specific conduct that does not constitute a financial market which is exempt from holding a licence. Section 767A(2)(a) CA 2001 stated that

(a) *"a person making or accepting offers or invitations to acquire or dispose of financial products on the person's own behalf, or on behalf of one party to the transaction only, unless the regulations specify circumstances in which such conduct does constitute operating a financial market and the person's conduct occurs in circumstances so specified;*

(b) *conducting treasury operations between related bodies corporate;*

(c) *a person, being the holder of a licence under an Australian law relating to the licensing of auctioneers, conducting an auction of forfeited shares;*

(d) *any other conduct of a kind prescribed by regulations made for the purposes of this paragraph."* Section 792A CA 2001 outlined licence obligations in relation to facilitating a financial market. The stipulations require service providers to ensure that the market is fair and transparent (in spite of conflicts between

The Australian Taxation Office (ATO) has confirmed that cryptocurrencies are subject to Capital Gains Tax (CGT) and Income Tax.

commercial interests) and that the market is operated in an orderly fashion. Additional licensing obligations include monitoring and implementing procedures to comply with market operations.

Payment services that include 'non-cash payment' – including cryptoasset payment and merchant service providers – will need to acquire an AFSL. *"Regulatory Guide 185: Non-cash Payment Facilities"* provides substantial guidance on the regulatory approach for non-cash payment (NCP) facilities under the CA 2001. The guidance describes the NCP facility as an emerging sector and therefore caters to a variety of facilities. The paper delivers the ASIC's general regulations on licensing and related disclosures. Relief from provisions of the CA 2001 may be available, although requests will be determined on a case by case basis on the grounds of general exemptions from the CA 2001. The general policy on relief, *"Regulatory Guide 167 Licensing: Discretionary Powers"* (RG 167) and product disclosure requirements from *"Regulatory Guide 169 Disclosure: Discretionary Powers"* (RG 169) will also be considered. The ASIC noted that certain products do not need a licence to operate, such as loyalty schemes, low value facilities and non-reloadable products that are only marketed as gift facilities. The relief for low value NCP facilities will have to satisfy the given test:

(a) *"the total amount available for the making of non-cash payments under all facilities of the same class held by any one client does not exceed $1000 at any one time;*

(b) *the total amount available for making non-cash payments under all facilities of the same class does not exceed $10 million at any time; and*

(c) *the facility is not part of another financial product."*

INFO 225 also included *"Information and Warnings about ICOs"* on ASIC's detailed 'Money Smart' webpage for consumers. The page has information on the types of cryptocurrencies and how ICOs operate. The underlying risks of fraud and fluctuation rates using ICOs and cryptocurrencies have also been emphasised. INFO 225 also explains that misleading or deceptive conduct associated with ICOs and cryptoassets are prohibited under Australian law. The ASIC has been delegated powers from the Australian Competition and Consumer Commission to take action against deceptive conduct. This applies to trade, commerce, or any relations to financial services or products. Schedule 2 of the Competition and Consumer Act 2010 is applicable to ICOs in relation to offering services or products to consumers. The provisions state that investors should not be misled by false information and should be supplied with accurate details and representation. Other consumer protections can be found in the ASIC Act which provides the ASIC with the powers to administer this law. Protection to investors is provided by maintaining the integrity of the financial system and the interests of the entities involved. ASIC has specified some examples of misleading or deceptive conduct associated with ICOs: one of these could be using websites or applications to imply greater levels of public interest in commercial activity for an ICO; withholding essential information about the ICO; or falsely implying the ICO is a regulated product. The ASIC will use its powers to investigate ICO service providers and eliminate any illicit activities. Failure to comply with the legislation will lead to compensation, sanctions and penalties.

On the subject of taxation, the Australian Taxation Office (ATO) has confirmed that cryptocurrencies are subject to Capital Gains Tax (CGT) and Income Tax. *"Tax Treatment of Crypto-currencies in Australia - Specifically Bitcoin"* clarified that CGT applies when disposing cryptocurrencies. A disposal can transpire when an individual: *"sells or gifts cryptocurrency, trade or exchange cryptocurrency (including the disposal of one cryptocurrency for another cryptocurrency), convert cryptocurrency to fiat currency, or use cryptocurrency to obtain goods or services."* Income Tax regulations are stipulated in the Income Tax Assessment Act 1936 and the Income Tax Assessment Act 1997. Those using virtual currencies for commercial purposes will be considered as trading stock, therefore proceeds from the sale of virtual currencies will be considered as income and subject to income tax. Furthermore, an expert task force was administered by the ATO to challenge

cryptocurrency related tax evasions. The ATO also works alongside virtual currency service providers, accumulating records to conduct investigations, and ensure users are adhering to tax rules.

Australian regulators enforced the Anti-Money Laundering and Counter-Terrorism Financing Amendment Act 2017 (AML/CFT Act) to bring cryptocurrencies under the legislative framework. The AML/CFT Act only applies to digital currency exchange services (DCE) and imposes a series of obligations on DCE service providers. The act defined digital currencies 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

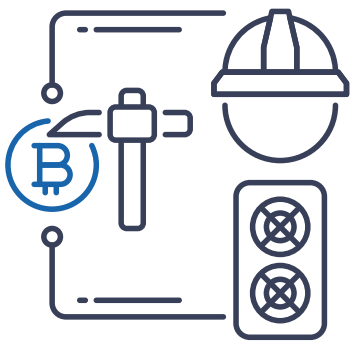
(ii) is not issued by or under the authority of a government body; and

(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/CTF Rules." DCE services are obligated to register with Australian Transaction Reports and Analysis Centre (AUSTRAC); consequences for inadequate registration could result in up to two years imprisonment and/or penalties of up to $105,000. Furthermore, registered entities are required to engage in Know-your-customer (KYC) procedures to collate sufficient records in order to adequately identify consumers. Service providers are also obliged to implement supervisory arrangements in order to monitor and report suspicious transactions to AUSTRAC. The AML/CFT Act recognises the rapid growth of innovative technology and intends to support the fintech sector by enforcing consistent regulatory checks and compliance. Nevertheless, the ASIC approach to ICO enforcement will continue to focus on fraud and consumer protection. It is likely that AUSTRAC will carefully assess the sector's compliance with AML/CFT policies to ensure a clear framework for crypto businesses while the ATO strengthens its approach to compliance enforcement to protect the financial industry and avert further losses from the Australian tax base. Entities offering financial services or products in the financial market are also obliged to acquire Australia's Financial Service (AFS) licence. The ASIC clarifies that applications are assessed on their eligibility to provide financial services and are not assessed on their reliability or quality. After obtaining the AFS licence, firms can carry out the following services: provide financial advice; deal in financial products; operate a registered scheme; offer a custodial or depository service; and provide traditional trustee company services.[56]

Australia has been responsive towards innovation in the fintech sector and has engaged in several developments, including regulatory variations. For example, ASIC and AUSTRAC have introduced the Innovation Hub to support financial firms navigate changes in Australian law. The Innovation Hub does not provide legal or financial services, but provides access to informal assistance on policy perspectives. However, the Australian government launched an enhanced regulatory sandbox (ERS) on 1 September 2020, which replaced the previous regulatory sandbox administered by the ASIC. The ERS allows consumers and businesses to test fintech services without obtaining the AFS licence. In accordance with the Corporations (FinTech Sandbox Australian Financial Services Licence Exemption) Regulations 2020 users can test a broader range of financial services for a longer duration of up to 24 months. Participation in the ERS requires persons to complete a prearranged form with the ASIC, and satisfy the minimum requirements and ongoing conditions with Australia's Financial Conduct Authority (AFCA). Although there are no existing programs to facilitate technological innovations, the regulatory sandbox demonstrates Australia's primary interest in developing regulation for its fintech sector. Moreover, the ASIC has engaged with regulators from the UK and has signed an Enhanced Cooperation Agreement for information sharing, cooperation, and joint policy efforts. The ASIC has also made agreements with Hong Kong, Singapore, Canada, Kenya and Indonesia. These arrangements expedite global fintech market trends and encourage competition. In essence, Australia is expected to offer further regulations once innovation has developed and ERS outcomes have been concluded.



United Arab Emirates (and Abu Dhabi)

The United Arab Emirates (UAE) government is determined to make advances in the blockchain industry and is striving to increase productivity to support government transactions and improve payment procedures. The government has also implemented ambitious targets associated with budgeting and conserving energy.

This is a direct result from Sheikh Hamdan Bin Mohammad Bin Rashid Al Maktoum's launch of Dubai's Blockchain Strategy (DBS) in October 2016. This initiative was created to prepare the UAE to be completely driven by blockchain technology by the end of 2020. DBS has three leading pillars: government efficiency; industry creation; and international leadership. The initiative is supported by the Smart Dubai Office (SDO) and the Dubai Future Foundation (DFF). It is clear that the UAE government is a prominent figure in the development of blockchain technology and has also established the Global Blockchain Council (GBC). The GBC explores potential applications and implications of innovation within the business and financial areas. The GBC is responsible for enabling transactions using the blockchain platform within a range of commercial and non-commercial sectors, in order to increase proficiency and consistency. The use of virtual currencies is not prohibited in the UAE and in spite of the interest in the development of blockchain technology, virtual currencies are not considered legal tender.

The UAE Central Bank and the SCA have classified ICOs as securities and will collaborate with the Abu Dhabi Securities Exchange (ADSE) and Dubai Financial Market (DFM) to create trading platforms for ICOs. In September 2018, the UAE's Securities and Commodities Authority (SCA) proposed the implementation of regulations for Initial Coin Offerings (ICO) towards the end of 2019 to provide institutions with an opportunity to initiate crowdfunding schemes and strengthen the government's regulatory position on virtual currencies. Nevertheless, there have been no new regulations or amendments to the existing securities legislation to govern ICOs and virtual currencies. The SCA will aid the Abu Dhabi and Dubai stock markets using the latest blockchain technology for cryptocurrency sales and ICOs. Although virtual currencies are generally recognised in the UAE, regulators have issued warnings, especially for money laundering and terrorist financing (ML/TF) purposes. In October 2017, the governor of UAE Central Bank announced that digital currencies are not operated through authorised bodies and individuals could be exposed to ML/TF activities.[57] The announcement also clarified that those involved in such circumstances will not be protected or indemnified.[58] In spite of the absence of new regulations, the UAE securities and financial laws may be applicable, depending on the coin/token in question. Furthermore, the SCA published *'The Circular'* in February 2018, which warned those dealing with virtual currencies to consider carefully the risks involved. The SCA explained that it does not regulate ICOs and that investors engaging in such activities are doing so at their own risk. The SCA illustrated some of the risks involved with ICOs. For example, certain ICOs are not regulated which can facilitate fraudulent activities; other ICOs are associated with foreign exchanges and are regulated by foreign laws, meaning that investigations for fund recovery may become complex. Trading in virtual currencies is also considered volatile and prices tend to move aggressively within the cryptocurrency market which can prove unsatisfactory for liquidity. Ultimately, it may be challenging for retail investors to calculate the accurate prospects from an ICO, given that the information in the White Paper can be misleading or inadequate.

Securities and similar instruments are regulated by the Federal Law No. 4 of 2000, Concerning the Emirates Securities and Commodities Authority and Market in the UAE. The SCA has been granted authority by the legislation to act as the second Federal regulator and any securities engaged in exchanges commercially must be licensed by the SCA. The statutory framework defines securities as *"Shares, bonds and notes issued by joint stock companies, bonds and notes issued by the Federal Government or Local Governments, public authorities and public institutions in the State, and any other domestic or non- domestic financial instruments accepted by the Authority."* The powers granted to the SCA allows them to

determine whether virtual currencies fall within the scope of the definition provided. Furthermore, both the Dubai Financial Services Authority (DFSA) and the Dubai International Financial Centre (DIFC) have declared that they do not regulate digital assets or virtual currencies/tokens. They also share a similar opinion of the UAE Central Bank and have made an announcement about the risks associated with its activities. Both regulatory bodies have not issued any licences to institutions that intend to participate in activities related to virtual currencies. The DIFC prevents persons from executing financial services on investments relating to securities and derivatives without authorisation. 'Financial activity' has been outlined in Regulatory Law 2004 as the following: *"accepting deposits; providing credit; providing money services; dealing in investments as principal; dealing in investment as an agent; arranging deals in investments; managing assets; advising on financial products; managing a collective investment fund; providing custody; arranging custody; effecting contracts of insurance; carrying out contracts of insurance; operating an exchange; operating a clearing house; insurance intermediation; insurance management; managing a profit-sharing investment account; operating an alternative trading system; providing trust services; providing fund administration; acting as the trustee of a fund; operating a representative office; operating a credit rating agency; arranging credit and advising on credit; and operating a crowdfunding platform."* The DIFC have also restricted financial advertising that encourages investors to enter an agreement regarding a financial service. In September 2017, the DFSA published *'DFSA Issues General Investor Statement on Cryptocurrencies'* and warned potential investors about the risks associated with ICOs. The DFSA clarified that it does not regulate such products or provide licences to practise in such dealings. In the statement the DFSA advised prospective investors to exercise reasonable care and consider the prevalent risks when entering an investment.

In October 2019, the SCA published draft regulations regarding cryptoassets: The Regulation for Issuing and Offering Cryptoassets. The regulation details various aspects of the cryptoasset industry within UAE, including trading, issuing, and offering coins/tokens. It provides policies for investor protection and demonstrates compliance with the AML/CFT provisions. The draft regulatory framework will help implement measures to control market intermediaries. It also delivers procedures and requirements for various market participants, such as custodians, traders, broker dealers, and promoters. The introduction of this regulation shows the increasing authority of the SCA and recognition of digital assets and virtual currencies as securities. It also implies better control and management of the cryptocurrency market by the UAE government. However, the draft regulation still needs to be approved and implemented and it is therefore unclear whether the regulation will be effective.

In January 2017 the UAE Central Bank issued the Regulatory Framework for Stored Values and Electronic Payment Systems (Stored Value Regulations). This regulation specifies that the Central Bank does not regulate virtual currency and defines it as: *"any type of digital unit used as a medium of exchange, a unit of account, or a form of stored value. Virtual Currency (s) is not recognised by this regulation. Exceptions are made to a digital unit that: a) can be redeemed for goods, services, and discounts as part of a user loyalty or rewards program with the Issuer and; b) cannot be converted into a fiat /virtual currency."* Bitcoin and similar platforms are not subject to the Stored Value Regulations. In June 2019, Emirates National Bank of Dubai published the article, *'Don't fight the Fed'*, which shared the same position as the UAE Central Bank. The bank does not prohibit transactions in virtual currencies or digital assets but refuses to process suspicious transactions.

After the UAE's successful implementation of the DBS, the Dubai Land Department (DLD) is producing its own blockchain system to record retail estate contracts. This is to connect the DLD with local utility companies (for example, Dubai Electricity and Water Authority).. The initiative will encourage residents to make electronic payments which will result in cost effective and environmentally sound outcomes. Furthermore, financial institutions and other corporate organisations are exploring blockchain technology to improve systems, in particular, Know-Your-Customer (KYC) procedures to aid the anti-money laundering and countering the financing of terrorism directives (AML/CFT). The launch of the e-KYC utility project by the Abu Dhabi Global Markets (ADGM) also fits into this goal by creating requirements for the regulatory framework of the e-KYC while using distributed ledger technology (DLT). Furthermore, the Financial Services Regulatory Authority (FSRA) in the ADGM contributes to the classification and management of virtual currency. The ADGM also issued *'The Guidance – Regulation of Digital Securities Activities in ADGM'* in October 2017. The guidance provides investors with the relevant legal information and the treatment of ICOs in the ADGM. It has also been advised that the guidance is read alongside the Financial Services and Markets Regulation 2015 (FSMR). If the tokens in an ICO share similar properties to a security, such tokens will be categorised as security tokens and fall under the ADGM's regulatory authority. The guidance also stipulates that some ICOs will not constitute an offer of securities under the FSMR, particularly when the tokens in question do not reflect the characteristics of a security. In these examples, the tokens that fall outside the remit of securities are likely to be unregulated.

The FSRA published a consultation paper, *'ADGM Regulatory Framework for Spot Cryptoasset Markets'*, in April 2018. This paper suggested a framework to administer cryptocurrency activities in the ADGM.

The FSRA published a consultation paper, *'ADGM Regulatory Framework for Spot Cryptoasset Markets'*, in April 2018. This paper suggested a framework to administer cryptocurrency activities in the ADGM.

Clearly, the FSRA is keen to devise a stable regulatory framework to ensure control and transparency over cryptoasset undertakings. The proposed framework follows the FSRA's previous guidance on ICOs: *'Guidance – Regulation of Crypto Asset Activities in ADGM'* published in June 2018. However, the proposed regulatory framework has not been enacted and until this point in time coins/tokens that reflect securities will be considered in line with the existing regulatory framework.

The UAE focused on delivering a stable AML/CFT framework in 2019. However, financial regulators and the SCA have still issued several warnings about the risks involved when dealing with virtual currency. The UAE government is also committed to producing its own cryptocurrency, such as EMCASH in 2017. This was the UAE's first attempt of its own cryptocurrency and was implemented into a payment system for school fees and government services. It was launched in collaboration with Emcredit Limited and The Object Technology Group Limited, a business based in the United Kingdom. Another cryptocurrency was later developed for payments in cross-border transactions with Saudi Arabia. It is clear that the UAE government is taking a leading role within the virtual currency industry and will eventually develop a strong regulatory regime.

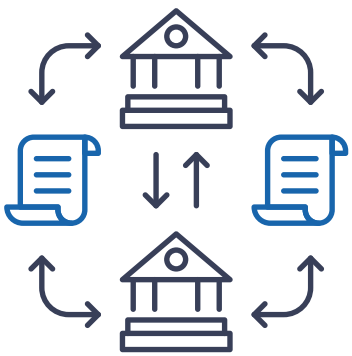
After the Middle East and North Africa Financial Action Task Force (MENAFATF) reviewed the UAE's AML/CFT regime in 2019, the UAE strengthened the regulations significantly. The changes include the implementation of a risk-based approach, which is in line with international standards and suggested by FATF's recommendations. The primary AML/CFT legislation is the Federal Law No. 20 of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism And Financing of Illegal Organisations (AML/CFT law). Alongside the Cabinet Resolution No. (10) of 2019 Concerning the Executive Regulation of Federal Law No. 20 of 2018 (AML/CFT Executive Regulation). The AML/CFT Law and the AML Executive Regulation are applicable throughout the UAE. The new AML Law defines ML and TF and details the outcomes for such activities. Moreover, Law No. 7 of 2014 on Combating Terrorism Offences (the CTO Law) addresses the prevention of such crimes. The predominant ML offence is defined in Article 2 of the AML/CFT Law: *"the offence renders a person a perpetrator of money laundering who;*

(a) conducts any transaction aiming to conceal the funds' illegal source;

(b) conceals the true nature, origin, location, way of disposition or ownership of rights with respect to the proceeds of a transaction;

(c) acquires, possesses or uses the proceeds upon receipt; or

(d) assists the perpetrator of the office to escape punishment. Importantly, it is only considered money laundering if the person is fully aware that such funds are derived from misconduct." Virtual currency falls within the scope of the UAE's AML/CFT legislation since 'funds' signify assets in digital or electronic form. The UAE Central Bank also manages the Financial Intelligence Unit (FIU) which collects reports of suspicious transactions from obliged entities such as the DFSA and the FSRA. In June 2019, the UAE government announced that regulated bodies, including financial firms, will be required to use 'goAML', a UN-developed software to report any suspicious activity associated with ML/TF to the FIU. The UAE is committed to meet international standards of the AML/CTF regime.



Caribbean Region

Cayman Islands

The Cayman Islands are well known for their virtual currency industry, particularly due to their favourable approach towards cryptocurrency, increasing investments, and supporting a growing number of new opportunities. They are largely celebrated for their neutral tax treatment and non-existent cryptocurrency regulations.

Regulators have not generated new legislation or extended existing financial regulations to specifically cater for virtual currencies. As a result, the Cayman Islands have gained mass popularity for inducting Initial Coin Offerings (ICO) Furthermore, the Cayman Islands Monetary Authority (CIMA) is the leading body supervising entities engaging in virtual currency transactions. Although the CIMA is working towards the creation of a regulatory framework for digital assets, it is expected that the Cayman Islands will uphold their large-scale productivity in this area. Cryptocurrencies are not considered legal tender in the Cayman Islands.

Due to the lack of clear regulations for virtual currencies, existing legislation may be applied to digital assets. Considerations for such regulations include the type of activity involved and whether the digital asset can relate to the instrument of the existing legislation. For example, the Mutual Funds Law (MFL) regulates various types of funds functioning in, and from within, the Cayman Islands. When entities issue equity interests with the aim of spreading investment and allowing investors to retain profits from the acquisition, preserving, dealing or disposal of investment, this may trigger obligations from statutory regulations and enable licensing or registration requirements from the CIMA. The type of digital asset is not of huge significance, as long as the digital asset contributes to an investment. The MFL gives powers to the CIMA to regulate particular aspects of the funds category. For example, according to the MFL a fund will issue equity and not contractual interests, which eliminates coin/token issuers. The fund must also be a collective investment tool, issue equity interests that are exchangeable by the investors. The fund must be established within the Cayman Islands or constitute a foreign fund that is available to the public of the Cayman Islands. The type of funds listed above must hold a licence and be registered with the CIMA.

Furthermore, entities engaging or dealing with virtual currencies can fall under the scope of the Securities Investment Business Law (SIBL). If the digital assets reflect the characteristics of a security, entities will be obliged to register and obtain a licence from the CIMA. Dealing in securities is provided by Schedule 2 of the SIBL as:

(a) "buying, selling, subscribing for or underwriting securities as an agent; or

(b) buying, selling, subscribing for or underwriting securities as principal where the person entering into that transaction

(i) holds themselves out as willing, as principal, to buy, sell or subscribe for securities of the kind to which the transaction relates at prices determined by that persons generally and continuously rather than in respect of each particular transaction;

(ii) holds themselves out as engaging in the business of underwriting securities of the kind to which the transaction relates; or

(iii) regularly solicits members of the public with the purpose of inducing them, as principals or agents, to buy, sell, subscribe for or underwrite securities and such transaction is entered into as a result of such person having solicited members of the public in that manner." Although the legislation does not explicitly refer to virtual currencies or digital assets, some instruments may reflect the properties and definition of securities. Therefore, a case by case method will be used to determine the scope of the digital asset alongside the existing classifications. Nevertheless, the offering or sale of virtual currencies within the Cayman Islands may activate existing regulatory provisions. Particularly, the Companies Law rejects any company from offering its securities to the public which has been established in the Cayman Islands and is not listed on the Cayman Islands Stock Exchange. Furthermore, the Limited Liability Companies Law

imposes registration requirements for companies working outside of the Cayman Islands; this type of company will have a separate legal identity to circumvent liability. Moreover, individuals dealing with virtual currencies within the Cayman Islands (those who are selling or issuing digital assets), may fall under the scope of the SIBL, irrespective of where the dealings take place. There are no principal income, capital gains, or corporate tax laws imposed in the Cayman Islands for exchanges, issuing, or holding digital assets. For stamp duty it is possible to apply on original documents produced in the Cayman Islands. Registered entities in the Cayman Islands may apply for a tax exemption certificate, certifying that no impending laws enforced after the date of exemption can be applied to their operations. This exemption can be purchased for a fee of 1,830 USD and remains valid for between 20 and 50 years.

According to the Money Services Law (MSL) 'money services business' is defined as *"the business of providing, in or from within the Islands, any of the following services – (a) money transmission; (b) cheque cashing; (c) currency exchange; (d) the issuance, sale or redemption of money orders or traveller's cheques; and (e) such other services as the Cabinet may specify by notice published in the Gazette"*. Section 5(1) MSL explains that persons administering a 'money service business' in or from within the Cayman Islands must obtain a licence from the CIMA; failure to do so will incur penalties. Although there are no direct references to digital assets within the legislation, a critical interpretation of the law may mean that some current legislation can be applied.

For anti-money laundering and countering the financing of terrorism (AML/CFT), the applicable legislation would be the Proceeds of Crime Law (PCL), which is – for the most part – relevant to all entities executed in the Cayman Islands. Under the PCL, money laundering, together with ancillary activities, is considered a criminal offence. Schedule 6 of the PCL stipulates that certain entities conducting relevant financial business (RFB) must adhere to the Anti-Money Laundering Regulations. For the purposes of virtual currency, a list of businesses contained in the definition of the RFB within the PCL include:

(a) 'banking or trust business carried on by a person who is for the time being a licensee under the Banks and Trust Companies Law;

(b) acceptance by a building society of deposits made by any person (including the raising of money from members of the society by the issue of shares);

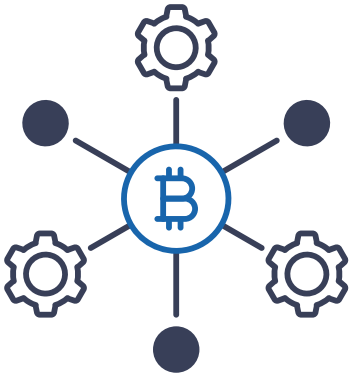
(c) business carried on by a co-operative society within the meaning of the Co-operative Societies Law;

(d) insurance business and the business of an insurance manager, an insurance agent and an insurance broker, who is licenced pursuant to the Insurance Law, that is connected with insurance business;

(e) mutual fund administration or the business of a regulated mutual fund within the meaning of the Mutual Funds Law;

(f) the business of company management as defined by the Companies Management Law."

According to the Anti-Money Laundering Regulations any entity engaged in an RFB is required to comply with Know-Your-Customer (KYC) and due diligence procedures. The AML Regulations require entities to initiate record keeping, carry out identification procedures. Entities conducting an RFB must also allocate an AML compliance officer in order to ensure compliance of policies and to communicate regularly with the CIMA. A reporting officer must also be appointed to observe suspicious activity and report such activity to the Financial Reporting Authority. The AML program must conduct a risk based approach to prevent illicit financial activities and monitor financial transactions. Entities are also obliged to observe the list of countries that do not comply with the recommendations of the Financial Action Task Force; this includes checks against all applicable sanction lists. Ultimately, entities are required to adopt and implement appropriate systems of control in order to mitigate risks. Consequently, authorities in the Cayman Islands have been enthusiastic about maintaining a balance between pro-innovation and a commitment to the prevention of AML/CFT. It is likely that authorities in the Cayman Islands will develop upcoming legislation to provide consistent regulations for digital assets.



Jamaica

Jamaica has not outlined any statutory frameworks regulating cryptocurrency transactions and do not consider virtual currency as legal tender. The Bank of Jamaica (BOJ) is committed to expanding innovation within the financial services sector. However, authorities are prioritising the stability of the existing financial regime and have not produced any policies to govern virtual currencies.

The BOJ has stated that authorisation is required by the bank itself for persons to carry out virtual currency related operations. The BOJ is also committed to demonstrating risks associated with virtual currencies and is advising the public about these risks. Nevertheless, Jamaica is adopting new agendas for digital asset trading and is exploring regulatory frameworks.

The Securities Act 1993 (SA) does not make explicit reference to virtual currencies; however, investment contracts may fall within the ambit of the definition provided by this act. For example, Section 2 of the SA defines securities as: "*(c) documents or writings commonly known as securities; (d) rights in, or options in respect of, a derivative; …(f) collateral trust certificates, pre-organization certificates, or subscriptions, transferable shares, investment contracts, voting trust certificates or certificates of deposit for securities; …(h) any right, interest or instrument designated by the Commission by order made with the approval of the Minister and published in the Gazette*". This suggests that the definition of securities is extensive and may incorporate the characteristics of investment contracts and other similar instruments related to digital assets.

Section 22(a) of the Banking Services Act 2014 (BSA) requires electronic money service providers to obtain a licence. The BSA defines electronic money as: "*monetary value represented by a claim on the issuer thereof, which value is*

(a) stored or recorded by electronic means;

(b) provided by the issuer in exchange for the present or future receipt of moneys or other valuable consideration from the person entitled to make the claim;

(c) transferable and accepted as a means of payment by persons other than the issuer, whether via point of sale or similar technology or otherwise;

(d) redeemable or repayable, whether in full or in part, on demand for cash, by deposit into a bank account or through the use of any automated banking or automated teller machine or any similar device; or

(e) not referable to credit facilities, whether secured or unsecured, extended by the issuer." Similarly, properties of virtual currency transactions can be incorporated into the scope of this definition and may be subject to the stipulated provisions. Furthermore, the *'Guidelines for Electronic Retail Payment Services (ERPS) 2019'* which was delivered through the Payment, Clearing and Settlement Act 2010 (PCSA) defines electronic money as "*E-money means electronically, including magnetically, stored monetary value on any device or instrument or server as represented by a claim on the Payment Service Providers (PSP), which is issued on receipt of funds for the purpose of making payments and which is accepted as a means of payment by persons other than the PSP. This includes e-money stored on a*

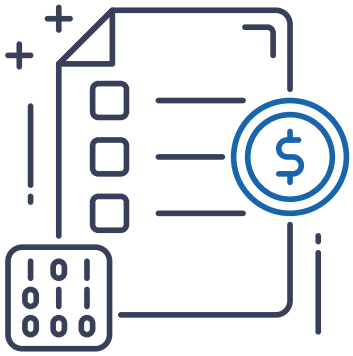
Guidelines for Electronic Retail Payment Services (ERPS) 2019' defines electronic money as *"E-money means electronically, including magnetically, stored monetary value on any device or instrument or server as represented by a claim on the Payment Service Providers (PSP), which is issued on receipt of funds for the purpose of making payments and which is accepted as a means of payment by persons other than the PSP."*

Jamaica participates in the Caribbean Financial Action Task Force (CFATF) and must comply with its 40 recommendations. While Jamaica has agreed to implement anti-money laundering and countering the financing of terrorism (AML/CFT) measures, it is obliged to adopt procedures to mitigate such activities.

device such as a SIM card or a server and accessible via telephone, internet or other access devices, cards, and other similar instruments but excludes any electronic means to permit transfers to/and from a deposit or current account held by a DTI". The definition provided could include digital assets; depending on whether virtual currency is treated as electronic money, the PSCA and its guidelines would apply. There are no tax obligations on virtual currency transactions in Jamaica.

Jamaica participates in the Caribbean Financial Action Task Force (CFATF) and must comply with its 40 recommendations. While Jamaica has agreed to implement anti-money laundering and countering the financing of terrorism (AML/CFT) measures, it is obliged to adopt procedures to mitigate such activities. For example, customer due diligence checks and know-your-customer (KYC) procedures must be conducted in order to comply with the recommendations. As part of this approach, the CFATF has developed particular guidance on access to the regulated financial system. CFATF continues to observe developments and prevent risks by developing the most appropriate practices to address money laundering and terrorist financing issues.

Jamaica is making advances in financial technology (fintech) innovations. The Jamaica Stock Exchange (JSE) has actively worked towards supporting new trading systems and joined the Canadian fintech organisation 'Blockstation' in April 2019. Jamaica is the first stock exchange globally to enter an agreement for the live trading of digital assets and security token offerings in a controlled environment. The enterprise emerged due to growth in the virtual currency market and the continuing popularity of Bitcoin. Although regulators have not developed clear guidelines for the use of virtual currency, the JSE and the Bank of Jamaica (BOJ) will produce regulations to expedite the new digital trading scheme. Jamaica is manifestly exploring different possibilities for fintech innovation.

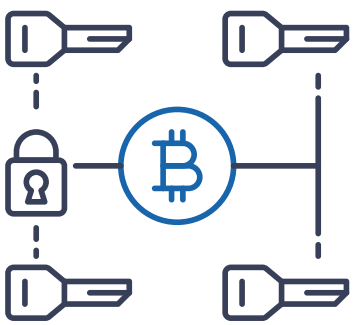


St. Lucia

St. Lucia has not established a regulatory framework for virtual currencies. Virtual currencies are not treated as legal tender, or backed by the Central Bank.

However, authorities have agreed to enter the Eastern Caribbean Central Bank (ECCB) pilot program. The ECCB pilot will explore the outcomes of the newly created digital version of the Eastern Caribbean dollar (DXCD) in conjunction with the official national currency. This pilot scheme is fundamental to understanding the accessibility of the digital dollar and questions whether it can create a secure digital financial system using blockchain technology. The absence of a regulatory framework for virtual currencies in St. Lucia poses significant risks for investors and the wider economy.

The absence of a regulatory framework for virtual currencies in St. Lucia poses significant risks for investors and the wider economy.



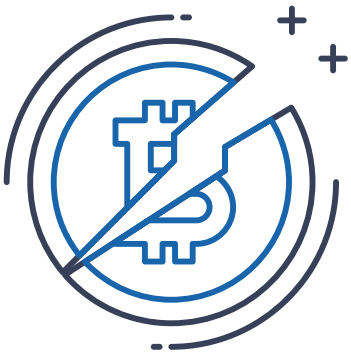
Trinidad & Tobago

Virtual currencies in Trinidad are unregulated; however, virtual currency exchanges are legal provided they do not generate illicit activities. Virtual currencies are not considered legal tender.

In 2018, the Ministry of Finance of Trinidad issued a media release: *'Digital Currency – BarterCoin Exchange and Initial Coin Offering In Trinidad and Tobago.'* The institution remains neutral on the proposed launch of BarterCoin and has not endorsed or connected with the Initial Coin Offering (ICO). Financial regulators and Trinidad's Securities and Exchange Commission (TSEC) have confirmed *"The Commission, has not as of this date approved any Initial Coin Offering. The ongoing offerings are unregulated and speculative investments, with considerable risk to the investor."* The document reports a number of potential risks concerning fraud, information asymmetry and liquidity which are related to virtual currency operations. In sum, the Ministry of Finance advises the wider public to exercise caution when entering into any form of investment associated with virtual currency.

The Chief Executive Officer of TSEC gave a presentation at the Telecommunications Authority of Trinidad and Tobago's 28th ICT Open Forum in March 2018. The presentation included definitions, characteristics, and key functions of virtual currencies. It also highlighted a summary of international and regional policy developments, applications for the securities industry, and the benefits and risks involved. The international regulatory overview of virtual currencies made it clear from the presentation notes that a balance is needed to cover both innovation and an appropriate regulatory framework. Three categories for the regulation of virtual currency were identified: tax considerations; financial surveillance; and securities regulation. In particular, there were proposals for potential applications for the securities industry: for example, ICOs, investment trusts, venture capital funds, and development of new securities. One may infer from this that regulators in Trinidad may consider expanding existing securities legislation to incorporate virtual currencies. The benefits which were mentioned in the presentation included the development of the securities industry, economic growth, and financial innovation. The risks associated with virtual currencies are related to dangers of anonymity, money laundering and financing of terrorism, and high volatility. The priority of the authorities is to protect investors and uphold the integrity of the financial system.

The Anti-terrorism Act 2005 and the *Proceeds of Crime (Large Transactions) Order 2019* are the primary legislations mitigating ML/TF. Although the statutory framework does not explicitly mention virtual currencies, the provisions are applicable to such operations. Trinidad and Tobago have made significant progress within their anti-money laundering and countering the financing of terrorism (AML/CFT) regime. The jurisdiction is no longer subject to strict monitoring by the Financial Action Task Force (FATF). The country has strengthened their AML/CFT system and reformed the insufficiencies which were identified by FATF in November 2017. TSEC published *'Anti-Money Laundering and Counter Financing of Terrorism (AML-CFT) Guidelines for the Securities Sector'* in November 2018. Trinidad and Tobago are participants in the Caribbean Financial Action Task Force and are working to advance the AML/CFT regime.

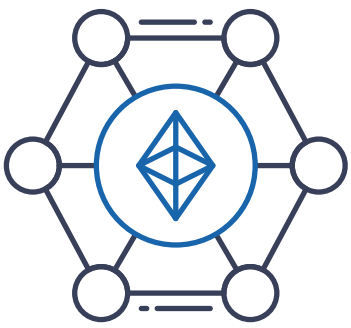


TSEC published *'Anti-Money Laundering and Counter Financing of Terrorism (AML-CFT) Guidelines for the Securities Sector'* in November 2018. Trinidad and Tobago are participants in the Caribbean Financial Action Task Force and are working to advance the AML/CFT regime.

Africa

South Africa

There are no specific statutory instruments or regulations governing the use of virtual currencies in South Africa. Virtual currencies are not prohibited. In December 2014, the South African Reserve Bank (SARB) published *'Position Paper on Virtual Currencies'*.



The Central Bank demonstrated that they are entirely responsible for issuing South African rand banknotes and coins, which at present constitute the only legal tender in the country. The bank highlighted that decentralised virtual currencies which are convertible (such as bitcoin), do not comprise legal tender. Beneficiaries are not obliged to accept virtual currencies as a means of payment. Furthermore, the paper discussed numerous risks related to the inherent features of virtual currency and warns investors about price volatility, fraud, money laundering, and terrorist financing (ML/TF) schemes. The paper also illustrated that such risks are likely to cause consumer risk due to the lack of regulation managing the space. SARB explained that participants who have been affected by such losses are not offered legal protection and those who engage in virtual currencies do so at their own risk. Although SARB has warned consumers about the individual risks, SARB also mentioned that virtual currency – at the given time – was not considered an abundant threat to the system at large. SARB also emphasised that it is likely to change its position in relation to policy developments.

South Africa has shown a growing interest in developing innovation, particularly in the fintech sector. The Intergovernmental Fintech Working Group (IFWG) was established in 2016 to create a forum for regulators to explore the progression of crypto-related activities and uncover possible implications to the economy. The group also considered prospective regulations and policies which could enable growth and development in the fintech sector. The various policy makers and regulators who embraced the IFWG – for example, the National Treasury, the South African Reserve Bank (SARB), the Financial Sector Conduct Authority (FCSA), the South African Revenue Service (SARS) and the Financial Intelligence Unit (FIU) – are all significant bodies within the finance sector in South Africa. In 2018, the Crypto Asset Regulatory Working Group (CARWG) was jointly created under the auspices of the IFWG and SARS guidance. The CARWG agenda was to assess the disposition of crypto assets and consider regulatory measures for upcoming legislation. The group was also tasked to ascertain the various effects and implications of cryptoassets in relation to public policy. The demand for regulation of cryptoassets gradually increased due to the rapid growth of virtual currencies and their potential risks to the financial system.

South Africa developed a practical method to respond to the growing use of cryptoassets in the country. Policy makers and regulators identified the risks involved in the following areas: trading; buying or selling virtual currencies; payments; Initial Coin Offerings (ICOs); crypto derivatives; and market provisioning. The CARWG recognised that these areas are subject to change within the developing market and will need to be monitored regularly. South Africa is open to advice from neighbouring countries and international bodies for the purpose of developing their regulatory framework. In January 2019, the IFWG and the CARWG issued a joint consultation paper: *'Consultation Paper on Policy Proposals for Crypto Assets'*. The purpose of the paper was to lay out relevant information on cryptoassets. The paper reviewed a range of crypto related activities and identified specific areas for further development including the following:

(i) 'Purchase and sale of cryptoassets;

(ii) Payments using cryptoassets;

(iii) Capital raising through ICO; (iv) Crypto derivatives and funds; and

(v) Market provisioning."

Crypto-related operations are direct results of decentralised technology such as blockchain and distributed ledger technology (DLT). South African regulators do not hold virtual currencies in the same regard as fiat currencies; however, they accept that some cryptoassets may satisfy the functions of

fiat currency, securities, and other financial instruments. The definition of cryptoassets has accordingly been carefully moulded to reflect the classification and regulatory treatment of such assets. The proposed definition states that: *"Crypto assets are digital representations or tokens that are accessed, verified transacted, and traded electronically by a community of users. Crypto assets are issued electronically by decentralised entities and have no legal tender status, and consequently are not considered as electronic money either. It therefore does not have statutory compensation arrangements. Crypto assets have the ability to be used for payments (exchanged of such value) and for investment purposes by crypto assets users. Crypto assets have the ability to function as a medium of exchange, and/or unit of account and/or store of value within a community of crypto asset users.* Due to the sudden popularity of virtual currencies and cryptoassets, regulators in South Africa found that revising existing legislation to accommodate virtual currencies was the most efficient way forward. CARWG suggested that authorities should not put off regulatory responsibility as virtual currencies had become an imminent issue. This explains its reluctance to creating a new regulatory framework exclusively for cryptoassets and virtual currencies. South Africa is keen to initiate engagement with fintech agencies in order to develop policies and innovation. At present, there are no specific regulations governing virtual currencies. However, financial products as stipulated under the Financial Sector Regulation Act 9 of 2017 may be applicable to some cryptoassets or virtual currencies. For example, the relevant financial sector laws include: Banks Act 94 of 1990; Financial Advisory and Intermediary Services Act 27 of 2002; Companies Act 71 of 2008; Financial Markets Act 19 of 2012; Collective investment Schemes Control Act 45 of 2002. Financial legislation applies explicitly to financial products in which cryptoassets are a new category. It is clear that virtual currencies will be beyond the scope of the majority of financial laws.

The Draft Taxation Laws Amendment Bill was published in July 2020 and proposed various amendments to the Income Tax Act 58 of 1962 and the Value Added Tax Act 89 of 1991. These amendments were suggested in order to eliminate the uncertainty surrounding tax treatment of virtual currencies in South Africa. For example, Section 2 of the VAT Act will introduce a broader scope of 'financial services', issuance or transfer, and ownership or acquisition of cryptoassets. Consequently, cryptoassets will be exempt from VAT under Section 12 of the VAT Act, subject to approval. Cryptoassets will be incorporated into the description of 'financial instrument', indicated by the amendments to income tax. Amendments to Section 20A of the Income Tax Act cover the acquisiton or disposal of cryptoassets, meaning that investors will not be able to balance the losses sustained from dealing in cryptoassets from any other trade. Such losses are therefore limited to the income earned from cryptoasset trade. The purpose of the bill was to classify the nature of cryptoassets and clarify their tax treatments. At present, the bill is pending for approval and until it is implemented into the tax regime, the status of cryptoassets will remain unclear.

The Financial Intelligence Centre Act 28 of 2001 (FICA) is South Africa's primary legislation for governing anti-money laundering and countering the financing of terrorism (AML/CFT). The statutory framework holds 'accountable institutions' responsible for preserving business ethics, strategy, and organisational integrity to ensure better economic performance in South Africa. For example, such institutions are obliged to implement customer due diligence checks, exercise reporting, and keep up to date records. Schedule 1 of the FICA supplies a list of 'accountable institutions' and makes reference to banks and money transfer services. Reporting obligations to the FIU is not just applicable to accountable institutions but includes those who are engaged in virtual currency dealings. Furthermore, virtual currency service providers must register as accountable institutions under the FICA and will be subject to AML/CFT provisions. Section 29 of FICA explicitly mentions that any person who has an association to a business and has knowledge of, or suspects that: *"a) The business has received or is about to receive the proceeds of unlawful activities or property connected to an offence relating to financing of terrorism; b) A transaction or series of transactions to which the business is a partly, facilitated or is likely to facilitate the transfer of the proceeds of unlawful activity or property relating to TF activities; has no apparent business or lawful business; may be relevant to the investigation of tax evasion or related generally to the financing of terrorism; or c) The business has been used, or is about to be used for money laundering purposes, or the financing of terrorism,"* must report to the FIU within a given period. Such reporting requirements are applicable to all entities involved in a business engaging with cryptoassets. South Africa is a member of the Financial Action Task Force (FATF) and the Eastern and Southern Africa AML Group (ESAAMLG). FATF has approved South Africa's implementation of AML/CFT directives and has noted improvement and progress in developing a consistent system for combating illicit activities since its last mutual evaluation report in 2003.[59]

Nevertheless, South Africa is exploring a range of avenues to develop innovation, particularly IFWG's and CARWG's initiatives to define a regulatory approach. As a result, policy makers will be able to create a sustainable regulatory framework that is proportionate to the risks and benefits of the fintech sector. It is clear that South Africa is likely to produce legislation in order to be in a position to promote processes and opportunities for innovation that are socially and economically desirable, and in line with public interest.

Nigeria

Cryptocurrencies are not considered legal tender in Nigeria and are not subject to a specific regulatory framework. Cryptocurrency has had an impact on Nigeria's financial system and authorities have therefore developed solid ideas on its use and functions.

In January 2017, the Central Bank of Nigeria (CBN) issued the *'Circular'* warning financial institutions about transacting in virtual currencies as they do not constitute legal tender and are subject to price volatility. The statement also cautioned those engaging in virtual currencies and clarified that those taking part do so at their own risk. The CBN also mentioned the high risks surrounding money laundering and terrorist financing (ML/TF) activities. The *Circular* clearly expressed CBN's position on virtual currency and indicated their prospective approach to regulations. Notwithstanding early warnings, a Bitcoin Ponzi scheme caused financial loss to two million people in Nigeria in 2017. Consequently, the Nigerian Deposit Insurance Corporation (NDIC) issued further warnings and emphasised that entities involved in such operations will not receive consumer protections or insurance when trading in virtual currencies. The NDIC also clarified that – at present – Nigeria's monetary system only contains its national currency and is facilitated by the CBN. In late 2017, the Deputy Director of CBN mentioned that the Central Bank does not regulate or manage bitcoin, nor do they own it. Nevertheless, financial authorities are co-ordinating guidelines on the use of virtual currency in order to implement appropriate measures. In January 2018, the Governor of CBN illustrated that it does not support cryptocurrencies and the residents of Nigeria should anticipate firm instructions on virtual currency. Nigeria's government and financial authorities such as the CBN and the Securities and Exchange Commission (SEC) have shared regular updates on the nature of virtual currency and its market. These warnings intend to isolate virtual currencies from fiat currencies and the wider monetary system. Authorities have emphasised that the majority of companies which facilitate virtual currency operations are unregulated and investors are not offered consumer protections. Although the exchange of virtual currencies is not prohibited, the CBN has initiated a reviewing process that will (in due course) inaugurate a blockchain and virtual currency regulatory framework. Nigeria is yet to produce legislation to govern virtual currencies and cryptoassets.

Despite the lack of regulations governing virtual currency in Nigeria, the SEC has provided general guidance on the cryptoasset market. Since cryptoassets differ from the traditional financial system, exercising the same regulatory framework may be insufficient. It is necessary for regulators and the SEC to confirm a regulatory approach. Importantly, authorities would classify the nature of cryptoassets and virtual currencies in order to determine its regulatory scope. Likewise, the capital market shares similar services of the cryptoasset market: for example, asset management, collective investment schemes, advisory and legal services. However, the crypto market is constructed on blockchain technology and is considered susceptible to fraud and other illicit activities. A licensing system can therefore minimise the level of risk. Following the publication of the *Circular*, AML/CFT directives were launched to introduce stronger identification and verification procedures. An enhanced level of monitoring and supervision for suspicious transactions was also implemented with accompanying reports to the Nigerian Financial Intelligence Unit (FIU). Furthermore, entities operating in virtual currencies must adhere to the Central Bank of Nigeria Anti-money Laundering and Combating the Financing of Terrorism in Banks and other Financial Institutions in Nigeria Regulations 2013. The AML/CFT legislation provides guidelines for financial institutions to implement effective measures and ensure compliance. In February 2018, the CBN issued a press release entitled *'Virtual Currencies not Legal Tender in Nigeria'*. The CBN once again emphasised that virtual currencies do not constitute legal tender in Nigeria and warned investors about the risk of losing funds through their investments. In July 2019, the NDIC issued a press release *'NDIC Urges Caution on Adoption of Cryptocurrencies'*, warning the general public about using virtual currencies as their principal means of financial dealings, given that the area is

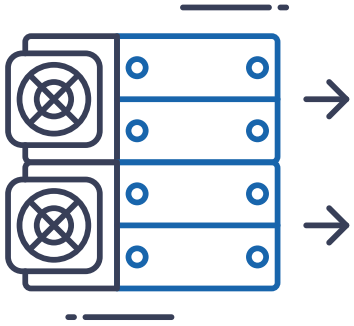
The Nigerian Cybercrime (Prohibition, Prevention) Act 2015 stipulates that all financial institutions and fintech companies must implement Know-Your-Customer (KYC) procedures alongside enhanced identity and verification checks. This is applicable to all electronic transactions and data collected must be secured for a duration of two years.

unregulated and consumer protections are unavailable. Fraud seems to be especially prevalent, perhaps because traditional banks do not support such organisations.

The Nigerian Cybercrime (Prohibition, Prevention) Act 2015 stipulates that all financial institutions and fintech companies must implement Know-Your-Customer (KYC) procedures alongside enhanced identity and verification checks. This is applicable to all electronic transactions and data collected must be secured for a duration of two years. Furthermore, the Central Bank of Nigeria Consumer Protection Framework dictates that all financial institutions under the supervision of the CBN must retain private consumer data and implement safeguarding measures to avert data disclosure. . Nigeria is also a member of the Intergovernmental Action Group against Money Laundering in West Africa (GIABA), implemented by the Financial Action Task Force. In 2013, they published a report to help build the regulators' and authorities' awareness in Nigeria about the different levels of terrorist financing within the country.

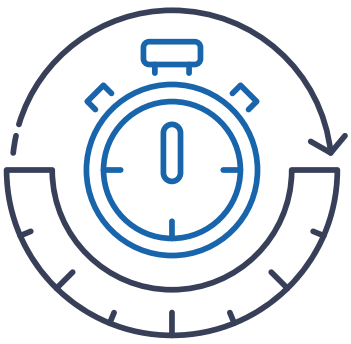
In 2018, the Nigerian House of Representatives called on the CBN and the NDIC to establish a regulatory framework for blockchain technology in Nigeria. This was due to the rapid growth in the development of virtual currencies and the public's acceptance of them making it necessary for the authorities to expand regulations to differentiate between standard and virtual currencies. The Nigerian Senate also launched an investigation committee in 2018 ('*Committee on Banking and other Financial Institutions*'), to examine the feasibility of bitcoin. Although the committee insisted that the NDIC, CBN and SEC share the risks of trading with bitcoin, they also wanted advice on how to manage its employment. In April 2019, the Fintech Roadmap for the Nigerian Capital Market issued a report on *'The Future of Fintech in Nigeria'* which urged the SEC to determine a classification for virtual currencies as either securities or commodities, but excluding currency. The report also requested that the SEC provide recommendations and proposals for the risks deriving from blockchain technology. The report highlighted that the SEC will oversee and conduct regulations for virtual financial asset exchanges.

In sum, the government has been the driver for introducing AML/CFT directives and a regulatory system. Authorities in Nigeria are also hoping to explore technological and economic advancement by using virtual currencies. However, as explained above, the characteristics of such technology increases the risks of fraudulent and unlawful activities which requires policymakers in Nigeria to accommodate the new technology with appropriate laws. Collaboration with financial institutions and regulators to implement customer due diligence requirements and ensure compliance is also necessary. In spite of the early misuse of virtual currencies in Nigeria, authorities are keen to develop new structures to govern virtual currencies with a full understanding of the technology and its impact as opposed to issuing pre-emptive legislation.



Kenya

Virtual currencies are unregulated in Kenya and are not considered legal tender. However, residents are lawfully permitted to engage with virtual currencies at their own risk. Despite the absence of a regulatory framework, Kenya is becoming a leading figure in Africa for its adoption of cryptocurrencies.



Various currencies are in the process of development and the government and policymakers are prioritising the roll out of a regulatory framework in order to protect investors and boost the overall economy. Kenya's National Land Commission has endorsed the use of blockchain technology to create transparency in land ownership in order to reduce fraudulent activities and the confusion around the sale of land.[60] The report *'Emerging Digital Technologies for Kenya: Exploration and Explanation'* issued by the Ministry of Information, Communication and Technology (MICT) in July 2019, lays out strategic recommendations for the expansion of technologies and the regulatory landscape for emerging developments, including blockchain. The report delivers a potential assessment and implementation proposal to the Kenyan government for the prevention of criminal activities and corruption. By contrast, the Central Bank of Kenya (CBK) issued a public notice *'Caution to the Public on Virtual Currencies such as Bitcoin'* in December 2015. The notice emphasised that virtual currencies do not constitute legal tender and consumers will not be protected in the event of liquidation or fraudulent undertakings. The notice further highlighted various risks associated with the use and exchanges of virtual currencies. For example, it was noted that its anonymous nature makes transactions largely untraceable and subject to exploitation. Consumers are susceptible to money laundering and high volatility in virtual currencies, meaning that entities will not be entitled to compensation or be able to retrieve any losses incurred. The notice discouraged entities from making transactions in bitcoin and/or similar currencies. Nonetheless, the Capital Markets Authority (CMA) is the designated regulatory body for the activities of market intermediaries. It is responsible for supervising, licensing, and monitoring actions that directly affect the economy and has an overview of long term productive investments. The CMA is in the process of establishing the criteria for a digital asset framework with a view to expanding the scope of virtual currency.

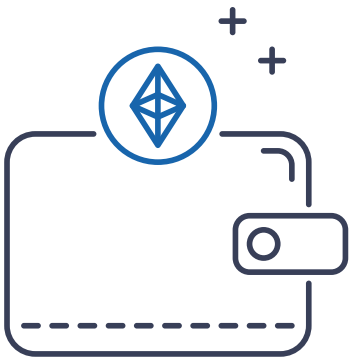
The National Information, Communications and Technology (ICT) Policy provided by the MICT in November 2019 promotes the progressive implementation of transparency and security in a safe environment. The intention of the framework is to protect investors, attract foreign investment, and enforce taxation to support infrastructure. The policy outlines a range of supporting mechanisms which can raise capital and help realise the potential of the digital economy such as identity management, distributed ledger technology (DLT), cryptography, and the expansion of existing legislations which may be applicable to the digital space. The policy seeks to establish Kenya as the fintech centre for the region while simultaneously facilitating various business opportunities. The policy expands on Kenya's Vision 2030 Long-term Development Blueprint which aims to revolutionise Kenya into a middle-income economy, a globally competitive nation, and successfully facilitate sustainable development. Furthermore, the Distributed Ledgers Technology and Artificial Intelligence Taskforce has conducted a study on *'Emerging Digital Technologies for Kenya: Exploration and Explanation'*. The report proposes a series of recommendations to optimise the use of blockchain technology in order to combat corruption. For example, the Taskforce encouraged the Kenyan government to create a digital asset framework, particularly to minimise national debts and securely facilitate initial coin offerings (ICO) to raise funds in support of local investors. It also recommended that a National Payment Gateway should be created using a public-private partnership method, which may enable financial inclusion and construct a system where interactions between all modes of payment would be possible. Furthermore, blockchain technology has distinctive properties that can generate faster and inexpensive processes. The Kenyan government should therefore use blockchain to identify fraudulent activities and create a digital identification service for residents in order to store official documents securely and alleviate corruption. The introduction

of a regulatory framework can provide the appropriate tools for service providers and financial institutions to mitigate and report illicit activities. Blockchain technology also has the capacity to enhance governmental operations and public services which could reinforce trust between authorities and the public sector. The Taskforce suggested that the Kenyan government facilitate such improvements by providing a single-source for all governmental documents and services and thereby improving cyber security.

Kenya's Cabinet Secretary for National Treasury and Planning has issued a draft Value Added Tax (VAT) (Digital Marketplace Supply) Regulations 2020 (VAT Regulations), which is awaiting approval from the government. The regulations offer guidance on the taxation of a digital marketplace and clarify that VAT is charged on taxable services delivered in Kenya through a digital marketplace through business to consumer (B2C) transactions. Those who are subject to the regulations are listed under Section 8 (2) of the Value Added Tax Act No. 35 of 2013 (VAT Act). The VAT Regulations propose that electronic services under Section 8 (3) of the VAT Act constitute taxable supplies. Section 8 (3) states that 'electronic services' refers to: *"any of the following services, when provided or delivered on or through a telecommunications network; (a) websites, web-hosting, or remote maintenance of programs and equipment; (b) software and the updating of software; (c) images, text, and information; (d) access to databases; (e) self-education packages; (f) music, films, and games, including games of chance; or (g) political, cultural, artistic, sporting, scientific and other broadcasts and events including broadcast television."* Furthermore, the VAT regulations impose a simplified VAT registration framework which clarifies that non-resident persons making B2C supplies of taxable services to persons in Kenya are required to register for VAT and pay at the standard rate of 14%. Individuals will be required to register within a 30 day period after the enactment of the Regulations. In circumstances in which those are unable to register, a tax representative can account for the VAT on their behalf. The VAT registration is available online where individuals will receive a personal identification number to proceed with the VAT procedures. It is also possible to apply for deregistration to the Commissioner if a change in circumstance occurs.[61]

Kenya's primary legislation on anti-money laundering and countering the financing of terrorism (AML/CFT) directives is found in the Proceeds of Crime and Anti-Money Laundering (Amendment) Regulations Act 2017 (AML Act) and The Prevention of Terrorism Act 2012 (Terrorism Act). Kenya is also a member of the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) provided by the Financial Action Task Force (FATF). FATF approved the improvements of Kenya's AML/CFT regime in its '*Improving Global AML/CFT Compliance: On-going Process*' report dated to June 2014. Kenya has still not established a legal or regulatory framework to combat AML/CFT in the use of virtual currencies according to the risks which have been identified by FATF. The legislation and AML/CFT initiatives do not incorporate the risks involved when transacting in virtual currencies and therefore consumers are more susceptible to exploitation. For example, in the case of *Lipisha Consortium Ltd and Bitpesa Ltd v Safaricom Petition 512 [2015] eKLR*, the High Court of Kenya ruled that bitcoin represented monetary value and that it was appropriate for Safaricom to suspend the services of Lipisha and Bitpesa Ltd after dealing in Bitcoin without permission from the Central Bank of Kenya.

Regulatory plans for virtual currencies are still on the drawing board in Kenya. In June 2017, the CMA issued the *'Stakeholders' Consultative Paper on Policy Framework for Implementation of a Regulatory Sandbox to Support Fintech Innovation in the Capital Markets in Kenya'*. The regulatory sandbox was created for financial institutions and relevant firms to test emerging fintech innovations in a regulated environment for a set time period. In January 2019, the CMA published a press release *'CMA Warns Against Kenicoin Initial Coin Offering and Trading'* which requested consumers to recognise the risks associated with virtual currencies before participating in ICOs. The CMA also highlighted that such activities are unregulated and must be approved by relevant authorities. In March 2019, the Capital Markets Authority Board issued the *'Regulatory Sandbox Policy Guidance Note (PGN)'* in which a regulatory framework is provided for institutions to explore the potential of fintech innovations for the benefit of larger financial markets in Kenya. Kenya is working towards developing fintech innovation at the same time as a stable regulatory framework which can be clearly and easily applied to emerging technologies. Authorities in Kenya are considering a regulatory approach that incorporates interactions with the financial sector.



Endnotes

1. https://complyadvantage.com/knowledgebase/crypto-regulations/cryptocurrency-regulations-eu-european-union/
2. https://www.fca.org.uk/markets/mifid-ii
3. GLI
4. https://www.pwc.com/mt/en/publications/financial-crime-news/PMLFTR.html
5. https://www.lawfirmpoland.com/5th-aml-directive-in-poland/
6. Pg. 6 of the ICO Guidelines
7. https://cointelegraph.com/news/the-bank-of-lithuania-released-a-cryptocurrency-but-its-for-collector
8. Although the term 'securities dealer' was replaced by 'securities firm' in the Financial Institutions Act (FinIA) in January 2020, the requirements remain the same.
9. D&B pdf
10. https://uk.practicallaw.thomsonreuters.com/7-382 3275?transitionType=Default&contextData=(sc.Default)&firstPage=true
11. https://gowlingwlg.com/en/insights-resources/guides/2019/doing-business-in-canada-securities-law/#pt1
12. https://ca.practicallaw.thomsonreuters.com/7-570-0154?transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1
13. https://www.canlii.org/en/ca/scc/doc/1977/1977canlii37/1977canlii37.html
14. https://ca.practicallaw.thomsonreuters.com/7-570-0154?transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1
15. https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf Pg. 10
16. https://crcoinico.com/
17. https://2009-2017.state.gov/documents/organization/239329.pdf
18. http://www.cvm.gov.br/subportal_ingles/menu/investors/legal-structure.html#:~:text=Legal%20and%20Regulatory%20Structure%20of%20the%20Brazilian%20Securities%20Markets,-The%20Securities%20and&text=The%20main%20Laws%20that%20guide,)%2C%20the%20%22Corporation%20Law%22
19. https://news.bitcoin.com/venezuela-passes-law-legalizing-crypto-mining-forces-miners-to-join-national-mining-pool/
20. https://globaltaxnews.ey.com/news/2019-6628-argentine-tax-reform-bill-sent-to-congress
21. Law reviews
22. https://home.kpmg/xx/en/home/insights/2014/04/argentina-thinking-beyond-borders.html (+ GLI)
23. PwC document
24. Law Reviews
25. PwC doc
26. https://www.mas.gov.sg/news/media-releases/2017/mas-clarifies-regulatory-position-on-the-offer-of-digital-tokens-in-singapore
27. https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulations-Guidance-and-Licensing/Securities-Futures-and-Fund-Management/Regulations-Guidance-and-Licensing/FAQs/FAQs-on-Product-Definitions.pdf
28. https://www.iras.gov.sg/IRASHome/GST/GST-registered-businesses/Learning-the-basics/Goods-and-Services-Tax--GST---What-It-Is-and-How-It-Works/#:~:text=Learning%20the%20basics%20%3E-,Goods%20and%20Services%20Tax%20(GST)%3A%20What%20It%20Is%20and,goods%20and%20services%20in%20Singapore.&text=Goods%20that%20are%20exported%20and%20international%20services%20are%20zero%2Drated.
29. https://download.asic.gov.au/media/1241348/rg211-published-18-december-2012.pdf pg. 11
30. https://download.asic.gov.au/media/1241348/rg211-published-18-december-2012.pdf Pg. 47
31. https://asic.gov.au/for-finance-professionals/afs-licensees/do-you-need-an-afs-licence/what-is-an-afs-licence/
32. https://gulfnews.com/how-to/your-money/uae-central-bank-warns-against-using-digital-currency-1.2111379
33. https://www.centralbank.ae/sites/default/files/2019-12/Cryptocurrency%20Statement%20English.pdf
34. https://www.fatf-gafi.org/countries/s-t/southafrica/documents/mutualevaluationofsouthafrica.html
35. Blockchain and Cryptocurrency in Africa (Baker McKenzie Report) Pg. 5
36. https://www.ey.com/en_gl/tax-alerts/kenya-introduces-vat-regulations-on-supply-of-digital-services