Special report:
Cryptos on the rise

By Susannah Hammond and Todd Ehret

THOMSON REUTERS®

Contents

Introduction

Digital transformation and the deployment of crypto-assets have great potential to make payments and transfers more efficient. However, the speed and reach of transactions, together with the potential for anonymous activity and for transactions without financial intermediaries, also make crypto-assets vulnerable to misuse and raise the risk of money laundering.

Financial services firms, regulators and policymakers are all having to come to terms with the rise of a new class of product. This report examines some of these developments as well as the risks and benefits of this next iteration of digital transformation.

It also considers the problems arising from the lack of an internationally consistent definition of the term "crypto". It looks at the implications for financial services firms and their customers of the potential for central bank digital currencies and the possible emerging arms race as central banks examine the ramifications of, and seek to deploy, digital currencies.

The report acknowledges the emergence of bitcoin as a mainstream instrument and assesses how that has changed the risk profile with regards to potential money laundering and other misuse of cryptocurrencies for illicit or illegal activities. Cyber risk is a concern for all cryptos, and the report considers how firms, regulators and exchanges can enhance their cyber resilience.

The vast technological applications of blockchain and cryptography are spreading beyond cryptocurrencies into the art, entertainment and collectible worlds using representative non-fungible tokens. The regulatory prospects in those areas are even more fragmented and, for the most part, non-existent. As a result they have not been included in this report despite a likely need for regulation in the future.

A compendium included with this report provides an overview of the regulatory landscape for cryptocurrencies such as bitcoin. The compendium was first published on the Answers On blog[1] and provides valuable information about the legality, tax treatment, evolving regulatory framework or viewpoint on a country-by-country basis for approximately 60 jurisdictions.

1 Thomson Reuters Answers On | Legal Insights Europe

Defining crypto

"... there is no such thing as cryptocurrencies, they are all crypto-assets."

Christine Lagarde, president of the European Central Bank at Reuters Newsmaker with Christine Lagarde. April 2021

The successful use of crypto-assets presents many challenges. One problem is the lack of an internationally agreed definition of "crypto", or agreement on where cryptos sit with regards to regulatory jurisdiction.

In broad terms a crypto asset is a type of digital asset that depends primarily on cryptography and distributed ledger or similar technology. This definition, which is used by the Financial Stability Board, includes digital means of exchange and other digital tokens, such as security tokens, asset-linked tokens and utility tokens.

The Financial Action Task Force (FATF) uses a slightly different definition for the term "virtual assets", which is "a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes". That definition is not limited to digital assets that rely on cryptography and distributed ledger technology (DLT). Both definitions encompass, among others, bitcoin and so-called stablecoins.

The regulatory status of crypto-assets is dependent on whether the asset is deemed to be within the regulatory perimeter of a particular jurisdiction and an assessment of the risks associated with the crypto asset itself. Supervisory authorities consider several factors to understand the nature of, and risks posed, by crypto-assets. These include:

- Nature of the issuer (e.g., identifiable, non-identifiable; public, private; regulated, unregulated);
- Intended use of the crypto-asset (e.g., used as a means of raising funds, of investment, of payment, granting rights to services/products in a company's network or ecosystem);
- Holders' rights (e.g., claim to the delivery of an underlying asset, to a granted interest, to access or use a service in a network or platform);
- Claim redemption (e.g., contractual claim, fixed redemption claim, dependent on price development);
- Control over the ledger (e.g., open to the public, open to specific parties, closed to a limited number of authorized parties);
- Validation of the ledger (e.g., permissioned, permissionless); and
- Mechanism to transfer the crypto-asset's ownership (e.g., centralised, peer-to-peer, decentralized).

A further challenge is the varying classification and definition of a crypto asset service provider (CSP), the crux of the issue then being the application of rulebooks, specifically including anti-money laundering requirements, to the CSP. Several activities can be performed with crypto-assets. These include activities which by nature may be mapped to those performed in traditional financial markets such as providing money transfers, and others which are completely new to the financial system such as currency "mining". To encompass all services and actors involved, crypto asset-related activities may be mapped to the life cycle of the asset itself, resulting in three categories of classification:

- *Primary market activities* relate to the issuance and distribution of assets (e.g., issuer and investor onboarding, deal structuring, risk assessment, asset registration, distribution of the asset to market participants).
- *Secondary market activities* comprise trading (e.g., admission of the asset to trading, price discovery, order matching, asset transmission), clearing and settlement and servicing (e.g., asset management, custody).
- *Tangential activities* aim at supporting and ensuring that primary and secondary market activities are conducted in an efficient manner (e.g., infrastructure services, ancillary services).

One practical upshot is that CSPs may have to comply with different regulatory requirements within and across jurisdictions. These may include requirements related to authorisation, capital requirements, risk management, governance, security, operational resilience, reporting, market conduct and financial integrity. These requirements may vary depending on the nature of the service provided or the perceived risks posed by the features of the crypto asset for which the service is provided.

Another aspect of the definitions challenge is that of legal certainty. In May 2021, the UK Law Commission published a call for evidence[2] which seeks to pave the way to ensure the law recognizes and protects digital assets in a digitized world. The problem, as articulated by the Law Commission, is that market participants generally treat digital assets as property.

2 https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2021/04/Call-for-evidence.pdf

Property and property rights are vital to modern social, economic and legal systems. The law of England and Wales is flexible enough to accommodate digital assets, but certain aspects need reform to ensure consistent recognition and protection.

For example, the law recognizes a digital asset can be property and that a digital asset can be "owned". It does not, however, recognise the possibility that a digital asset can be "possessed" because the concept of "possession" is limited to physical things. This has consequences for how digital assets are transferred, secured and protected under the law.

The intention is that the call for evidence will be used to reform the law to provide legal certainty and to lay a strong foundation for the development and adoption of digital assets.

Definitions used in Consultation Paper 138 on proposals for the regulation of security tokens published in April 2021 by the Dubai Financial Services Authority

Crypto-asset or token — a digital representation of value, rights and obligations that are created, stored and transferred electronically, using distributed ledger technology or similar technology.

Distributed ledger technology (DLT) — a class of technologies that support the recording of encrypted data:

(i) held on a distributed ledger;

(ii) electronically accessible, from multiple locations, by a network of participants; and

(iii) that can be updated by those participants, based on agreed consensus, protocol or procedures (i.e., distributed consensus).

Security token — a token that confers rights and obligations that are:

(i) the same as those conferred by a share, debenture or futures contract (investments); or

(ii) substantially similar in nature, purpose or effect to those conferred by investments.

Safeguarding and administration (custody) of security tokens — holding or controlling security tokens on behalf of third parties by holding or having access to those assets through private keys.

Operating a facility that trades security tokens — operating or managing an infrastructure or facility where multiple third-party buying and selling interests for security tokens can interact in a manner that results in a contract for the sale or purchase of the security tokens.

Digital wallets — a software application or other tool which is used to control, safeguard or manage public and private cryptographic keys (or their equivalent) associated with security tokens.

Distributed consensus — the agreed consensus, protocol or procedures for verification, confirmation and updating data stored on a DLT application by its participants.

Source: Dubai Financial Services Authority Consultation Paper 138

3 https://dfsaen.thomsonreuters.com/sites/default/files/net_file_store/CP138_Regulation_of_Security_Tokens.pdf

Cryptocurrency regulation in the United States — an evolving and complex process

Despite the growing popularity of cryptocurrencies such as bitcoin in the United States, optimism about a crypto-friendly regulatory environment for digital assets may be premature.

Building a new regulatory framework will involve many stakeholders and extend beyond bitcoin and cryptocurrencies. Use of blockchain technology, electronic payments, stablecoins, central bank digital currencies and the digitalization of other assets through non-fungible tokens will all need to be addressed to varying degrees by regulators.

One of the biggest obstacles to speedy roll-out of new crypto regulations in the United States is likely to be friction and overlap between the regulators. The Securities and Exchange Commission (SEC) is widely seen as the largest, most powerful regulator, and Gary Gensler, its chair, is thought to be crypto-friendly.

The task of building a regulatory framework is unlikely to be left solely to the SEC, however. Other regulators, such as the Commodity Futures Trading Commission (CFTC), the Treasury Department's Financial Crimes Enforcement Network (FinCEN) and the Federal Reserve Board, will have roles to play in shaping future rules.

A related complication is that the complex and evolutionary nature of cryptos has led to differing interpretations from the various regulators. The SEC sees them as securities, the CFTC calls them commodities, while Treasury calls them currencies; even the Internal Revenue Service (IRS) treats them as property for tax purposes.

With such differing viewpoints, it may be up to Janet Yellen, Treasury secretary, and the Financial Stability Oversight Council to intervene. Yellen is seen as more of a crypto-skeptic, following concerns voiced during her confirmation hearings.

"We need to make sure that our methods for dealing with … terrorist financing change along with changing technology. Cryptocurrencies are of particular concern. I think many are used, at least in the transactions sense, mainly for illicit financing. We really need to examine ways in which we can curtail their use and make sure that [money laundering] doesn't occur through those channels," Yellen said.

The value of bitcoin and other cryptocurrencies, commonly volatile, plunged following her testimony, in a decline many participants attributed to the prospect of tighter regulation. After the hearing she provided additional comments which softened her tone, saying the United States needed to "look closely at how to encourage their use for legitimate activities".

"If confirmed, I intend to work closely with the Federal Reserve Board and the other federal banking and securities regulators on how to implement an effective regulatory framework for these and other fintech innovations," she said.

Yellen also cited the December 2020 proposed rule from FinCEN related to the treatment and regulation of crypto wallets. Yellen said she "intends to conduct a full and substantive review of the proposal, which will include an assessment of how to ensure proper input from stakeholders".

The SEC has taken an active stance on enforcement where fraudulent tokens or initial coin offerings (ICOs) violate existing regulations, typically under anti-fraud provisions or as unregistered securities offerings. The CFTC has adopted a similar approach.

The SEC's Examination Division published a risk alert in February 2021 which highlighted observations made during examinations of broker-dealers, investment advisers, exchanges and transfer agents. The alert noted that digital asset securities "present unique risks" and reminded firms to develop and expand their compliance programs to cover digital assets.

It is also unclear quite where bitcoin and cryptocurrencies will register on the list of priorities. Gensler may be crypto-friendly, but early signs suggest environmental, social and governance (ESG) and climate-related issues are seen as more important.

Many in the financial services, fintech, crypto and legal and compliance areas have called for cooperation and possibly a directive from either Congress or the executive branch regarding the development of a regulatory framework.

The challenge will be for regulators to work together to enforce existing regulations such as those relating to anti-money laundering (AML), anti-fraud, manipulation and customer protection, while avoiding the creation of unnecessarily prescriptive or heavy-handed new regulations which stifle innovation.

Congress gets involved

The House of Representatives passed the H.R. 1602, the Eliminate Barriers to Innovation Act[4], which seeks to clarify the regulatory roles of the SEC and CFTC in their efforts to regulate cryptocurrencies.

4 https://www.congress.gov/bill/117th-congress/house-bill/1602

Despite bipartisan sponsorship and support, and its relatively non-controversial and non-political ramifications, the fate of the bill in the Senate is uncertain. The bill is nonetheless an opening salvo in what looks set to be a lengthy process, and indicates a growing understanding on Capitol Hill while sending a signal to regulators of the importance of regulatory cooperation.

The bill calls for the creation of a working group to submit, within one year, a report on the current legal and regulatory framework. The working group should comprise representatives from the regulators as well as from financial technology companies, financial firms and small businesses.

The working group and report would also address a lack of clarity about cryptos and the United States' competitive standing relative to other countries. Other critical aspects will include legality, cyber security and business continuity.

Future best practices to reduce fraud, address manipulation, provide investor protection and comply with banking and AML laws and regulations should also be included in the report.

Whether the Eliminate Barriers to Innovation Act makes it through the Senate will in part be up to Charles Schumer, the Senate majority leader. Despite tweeting several years ago that "Bitcoin has significant potential," Schumer has called on companies to establish how to stop criminals from exploiting it.

Central bank digital currencies — an emerging arms race

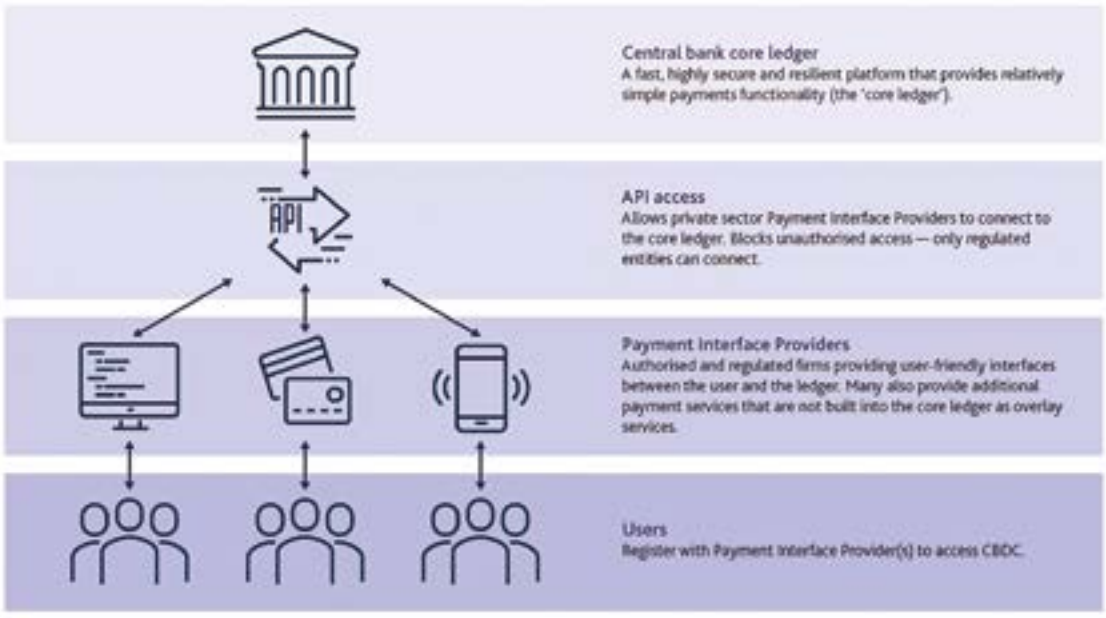
"The ability, ever more cheaply, smoothly and quickly, to pay, settle, record and analyse financial transactions through technology, whilst respecting privacy and security, will provide both opportunity and danger, in terms of global geopolitical positioning and systemic and market risk."

CityUnited recommendations to the UK Taskforce on Innovation, Growth and Regulatory Reform, April 2021

Source: CityUnited Project Recommendations to the Taskforce on Innovation, Growth and Regulatory Reform[5]

Central bank digital currencies (CBDC) are cryptographically secure digital currencies issued by central banks. They represent the next generation of payment technology and, due to their cryptographic and technological properties, they allow fractions of currency to be spent without the costly overheads. Even more importantly, every fraction of the digital currency can be forensically traced and tracked throughout its lifetime, giving the central bank full visibility and allowing it additional policy flexibility. CBDCs are expected to be faster and cheaper than existing payment systems.

Designing a CBDC – an illustrative model of CBDC designed to store value and enable payments by households and businesses.



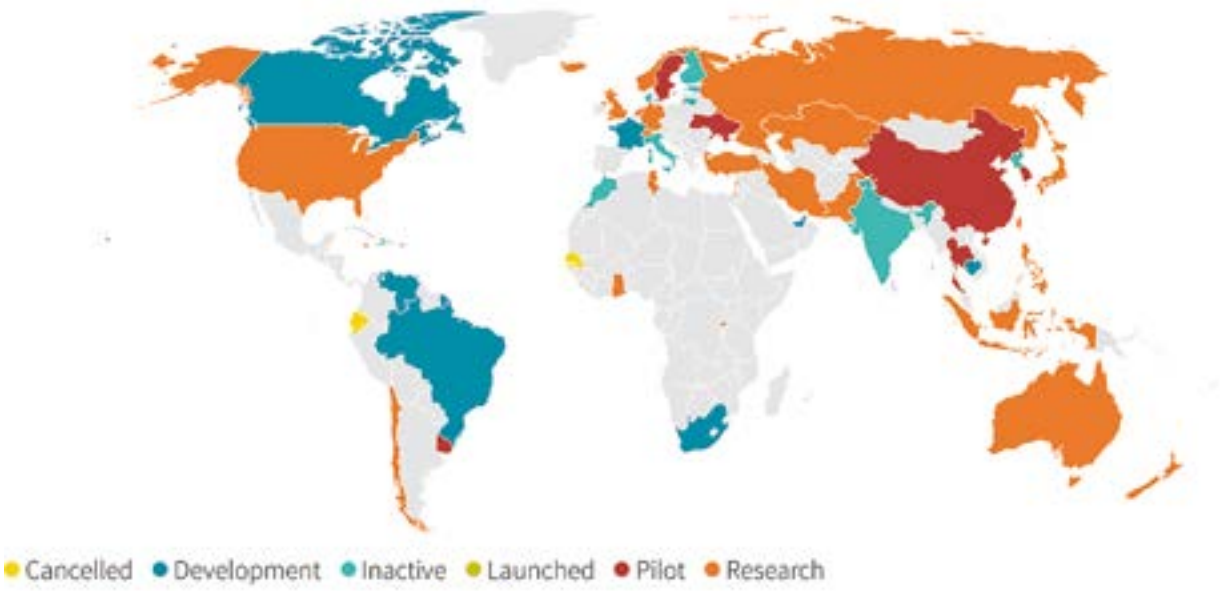
Source: Bank of England Discussion Paper on Central Bank Digital Currency – Opportunities, challenges and design. March 2020[6]

5 https://www.cityunitedproject.com/cup_submission_to_govt_TIGGR_taskforce_20210406.pdf

6 https://www.bankofengland.co.uk/-/media/boe/files/paper/2020/central-bank-digital-currency-opportunities-challenges-and-design.pdf?la=en&hash=DFAD18646A77C00772AF1C5B18E63E71F68E4593

Central Bank digital currences across the world

CBDC projects are moving ahead across the world – though few have gone past the drawing board



Note: European Central Bank is conducting research for euro zones.

Source: Harvard Kennedy School Belfer Center & Atlantic Council, Reuters research
Source: China proposes global rules for central bank digital currencies, Reuters Emerging Markets, March 2021[7]

There is a sense of inevitability about CBDCs, but the timescales, the parameters and the detailed design remain up for consideration.

Financial services firms need to remain engaged with the considerations both domestically and internationally. Central banks are policymakers; many are either direct or indirect regulators of financial services activities in their jurisdictions and as such will have an impact on how digital transformation is rolled out in practice. As central banks build their skills and develop their thinking, expectations for financial services firms will evolve, particularly with regards to cyber hygiene, operational resilience and governance in terms of the roll-out of new (digital) products.

Central banks may also engage with financial services firms directly as part of any testing of a possible CBDC and require potentially extensive additional data.

Analysis of recent activity in the United States, the UK and China gives a snapshot of how different jurisdictions are approaching CBDCs.

China

China has taken the decision to build and roll out a digital yuan[8]. It has progressed to testing stage, and China is expected to launch the digital yuan in time for the Beijing Winter Olympics in 2022. It is understood that, by design, the digital yuan will give the Chinese government additional economic tools as well as removing anonymity for the user.

The digital yuan is also expected to be rolled out for international use, which may give China a first-mover advantage. Numerous challenges remain, however, before the proof of concept becomes a reality for day-to-day domestic and international transactions. The challenges are being tackled through regional initiatives which seek to build cross-border payments systems which could be used for the digital yuan.

The People's Bank of China (PBoC) has launched domestic pilot projects testing the use of the digital yuan in retail transactions. The pilots involved distributing small amounts of digital currency to individual consumers to spend at participating retailers.

The PBoC retained the ability to invalidate the currency after a certain amount of time, seeking to ensure consumers spent the currency and so provided test data on the efficacy of the CBDC design. One part of the testing protocol was the retention of all transaction data which, it is expected, will be part of any wider roll-out of the digital yuan.

7 https://www.reuters.com/article/us-cenbanks-digital-china-rules-idUSKBN2BH1TA

8 https://www.reuters.com/article/us-china-currency-digital-explainer-idUSKBN27411T

UK

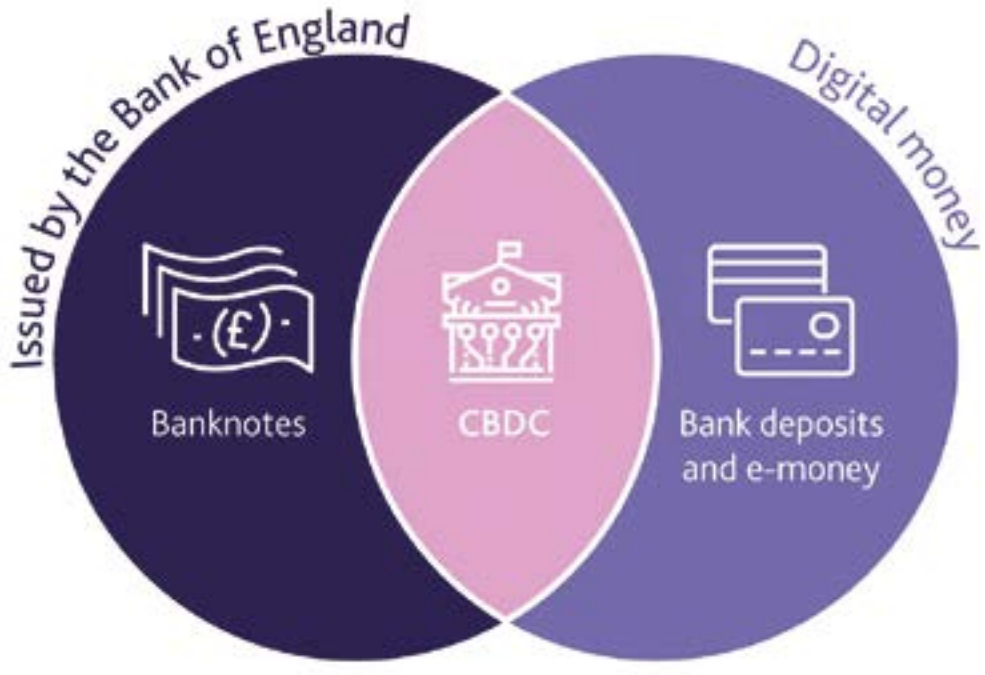
"In the platform model of CBDC [...] the Bank would build a fast, highly secure and resilient technology platform — the 'core ledger' — which would provide the minimum necessary functionality for CBDC payments. This would serve as the platform to which private sector firms, called payment interface providers, could connect in order to provide customer facing CBDC payment services."

Bank of England discussion paper – Central bank digital currency: Opportunities, challenges and design. March 2020

Source: Bank of England discussion paper: Central bank digital currency: Opportunities, challenges and design[9]

The Bank of England has yet to take a formal decision on CBDCs. A taskforce to explore the practicalities, challenges and benefits was announced in April 2021. From the perspective of the Bank of England, a CBDC would be an electronic form of central bank money that could be used by households and businesses to make payments. This would allow everyone to make electronic payments in central bank money.

If a UK CBDC were to be introduced, it would be denominated in pounds sterling, just like banknotes, so £10 of CBDC would always be worth the same as a £10 note. CBDC is sometimes thought of as equivalent to a digital banknote, although in some respects it may have as much in common with a bank deposit. Any CBDC would be introduced alongside, rather than replacing, cash and bank deposits.



Source: Bank of England discussion paper on central bank digital currency. March 2020[10]

9 https://www.bankofengland.co.uk/paper/2020/central-bank-digital-currency-opportunities-challenges-and-design-discussion-paper

10 https://www.bankofengland.co.uk/paper/2020/central-bank-digital-currency-opportunities-challenges-and-design-discussion-paper

United States

The U.S. Federal Reserve has begun to consider the possibility of a digital currency and in February 2021 the central bank published[11] a report on preconditions designed to spark further inquiry.

> "Separately, a significant policy process would be required to consider the issuance of a CBDC, along with extensive deliberations and engagement with other parts of the federal government and a broad set of other stakeholders. There are also important legal considerations. It is important to understand how the existing provisions of the Federal Reserve Act with regard to currency issuance apply to a CBDC and whether a CBDC would have legal tender status, depending on the design. The Federal Reserve has not made a decision whether to undertake such a significant policy process, as we are taking the time and effort to understand the significant implications of digital currencies and CBDCs around the globe."
>
> **"An Update on Digital Currencies," remarks by Lael Brainard, member, board of governors of the Federal Reserve System, August 2020**

The suggested preconditions are seen to be necessary but not necessarily sufficient. There are five broad areas:

- Clear policy objectives.
- Broad stakeholder support.
- Strong legal framework.
- Robust technology.
- Market readiness.

Within each area, detailed elements are discussed. These areas and elements are far from exhaustive because many systems, tools, processes and structures will need to be in place for a CBDC. In addition, many of these elements are interconnected. For example, engaging with a broad array of stakeholders and monitoring market readiness could inform clear policy objectives and vice versa.

Assuming the other preconditions are met, much will depend on the technology which will, in turn, influence the design and functionality of a digital currency. In some cases, business and operational requirements for a particular CBDC design may require the development of new technology. A nationwide CBDC arrangement based on distributed ledger technology, for example, would require further advances, such as enhanced transaction throughput capabilities given the size of the U.S. economy. Access or integration points, such as digital wallets, may require additional development to meet operational standards. A CBDC that can operate offline, for example, may require use of other technology such as secure hardware. Significant technology development and assessment work will be needed in three core areas:

- System integrity.
- Operational robustness.
- Operational resilience.

11 https://www.federalreserve.gov/econres/notes/feds-notes/preconditions-for-a-general-purpose-central-bank-digital-currency-20210224.htm

The table below highlights main aspects of the technology capabilities needed to underpin a CBDC.

Technology capabilities	What aspects are important?
System integrity. A CBDC needs to perform as intended in an unimpaired manner and free from unauthorized manipulation.	• Ability provide a secure and efficient transfer of assets. • Accurate recordkeeping, effective anti-counterfeiting measures and robust fraud detection. • Ability for the arrangement to manage and protect against unauthorized access, use, disruption, modification, or destruction to provide system confidentiality, integrity and availability. • Careful implementation of strong information security controls to protect information assets.
Operational robustness. A CBDC must have the ability to operate correctly and reliably across a range of operational conditions.	• Provide instant settlement with continuous 24-hour/7-day availability. • Include flexible and adaptable technology so the arrangement can evolve as needed. • Due consideration to operational robustness of the ecosystem and not only that of the arrangement operator (for example, issuance and distribution of a CBDC to poorly designed or poorly operated digital wallets may pose risks to the entire arrangement).
Operational resilience. A CBDC also needs the ability to resist, absorb and recover from or adapt to adverse conditions.	• Give due consideration to the potential impact of connectivity outages if internet connection is required. • Address operational resilience from a people, information, systems, processes and facilities perspective. • Consider endpoint-to-endpoint resilience (that is, the "standard" for operational resilience should be at the end-user level and not solely with the settlement function of the arrangement).

Source: "Preconditions for a general-purpose central bank digital currency", by Jess Cheng, Angela N Lawson and Paul Wong of the Federal Reserve Board, FEDS Notes, February 2021[12]

The preconditions articulated, and the work it will take to achieve them, are interconnected, so efforts in one area may lead to developments in another. These developments could strengthen or weaken the forces for change toward a general-purpose CBDC issuance. Each of the preconditions on its own will take significant time to achieve and, as such, represent only a starting point.

One of the strongest proponents of a CBDC in the United States has been Christopher Giancarlo, former chair of the CFTC and co-founder of the the Digital Dollar Project, a non-profit firm. The Digital Dollar Project has announced that it will launch five pilot programs to test the potential uses of a central bank digital currency, the first effort of its kind in the United States.

The private-sector pilots initially will be financed by Accenture Plc and involve financial firms, retailers and non-governmental organizations, among others. The aim is to generate data that could help U.S. policymakers develop a digital dollar.

As noted above, CBDCs are the digital equivalent of banknotes and coins, giving holders a direct digital claim on the central bank and allowing them to make instant electronic payments.

Debit cards or payment apps are a form of digital cash, but those transactions are created by commercial banks based on money central banks credit to those banks' accounts. They are not fully government-backed, can take days to settle and often incur fees. Cryptocurrencies, meanwhile, are controlled by private actors.

12 https://www.federalreserve.gov/econres/notes/feds-notes/preconditions-for-a-general-purpose-central-bank-digital-currency-20210224.htm

"There are conferences and papers coming out every week around the world on CBDCs based on data from other countries," said Christopher Giancarlo, former chair of the CFTC and co-founder of the Digital Dollar Foundation.

"What there is not, is any real data and testing from the United States to inform that debate. We're seeking to generate that real-world data," Giancarlo said.

As guardian of the world's most widely used currency, the Federal Reserve is moving more cautiously. It is working with the Massachusetts Institute of Technology (MIT) to build a technology platform for a hypothetical digital dollar; however, Federal Reserve Chair Jerome Powell has said getting the digital dollar right was "far more important" than speed.

Giancarlo said Powell was correct to be cautious but that, as China pushes ahead, the United States must drive discussion on incorporating values such as privacy and freedom of commerce and speech into the development of CBDCs.

"It's vital that the United States asserts leadership as it has in previous technological innovations," Giancarlo said.

The pilot programs will complement the Fed's MIT project by generating data on the functional, sociological, business uses, benefits and other facets, of a digital dollar. The data is due to be released publicly.

Accenture has already worked on several CBDC projects in Canada, Singapore and France.

As with a comprehensive regulatory framework for cryptocurrencies, the creation of a CBDC in the United States will be a difficult task, although all signs suggest a serious effort is beginning to take shape.

Bitcoin has gone mainstream

Bitcoin is labelled as a cryptocurrency though for many retail customers it is treated as an investment as they seek to weather the volatility and benefit from the valuation gains which have characterized bitcoin in recent years.

However bitcoin is labelled it, along with other cryptocurrencies, bring unique challenges for financial services firms. What had been thought of as a curiosity has now gone mainstream, as highlighted by the 2021 listing of Coinbase (a CSP) in the United States which reported around 53 million users and a quarterly trading volume of $335billion.

The specific issues for financial services firms fall into four broad categories:

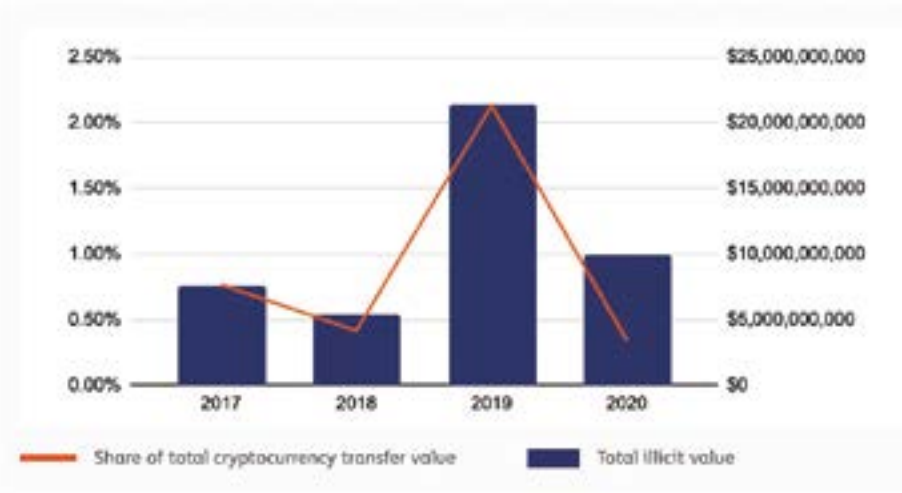
- How to keep customer cryptocurrencies secure — as an example, Coinbase keeps 98% of customer funds stored offline and distributes bitcoin geographically in safe deposit boxes and vaults around the world.
- How to comply with all relevant prevention of money laundering, sanctions and know-your-customer obligations and avoid the firm being used for financial crime.
- How to protect potentially vulnerable customers — the spectacular gains of bitcoin have attracted unsophisticated investors who may not understand what they have invested in and what the losses may be.
- How to manage the competitive threat from Big Techs which are increasingly seen to be entering the payments services marketplace leveraging their often-huge customer bases and technological expertise.

Another issue is the regulatory perception of cryptocurrencies. Policymakers and regulators are, to a certain extent, playing catch-up on the regulatory approach to the likes of bitcoin, with rhetoric not necessarily in line with reality.

> "Cryptocurrencies are 'a particular concern' when it comes to criminal activity and terrorist financing … I think many [cryptocurrencies] are used, at least in a transaction sense, mainly for illicit financing. And I think we really need to examine ways in which we can curtail their use, and make sure that anti-money laundering [sic] doesn't occur through those channels."
>
> **Janet Yellen, secretary of the U.S. Treasury, speaking at a Senate Finance Committee, January 2021**

The perspective that cryptocurrencies are "mainly for illicit financing" does not appear to be borne out by the data. The rapid growth in cryptocurrencies suggests that the majority of cryptocurrency is not used for criminal activity. According to an excerpt from Chainalysis' 2021 report, in 2019, criminal activity represented 2.1% of all cryptocurrency transaction volume (roughly $21.4 billion worth of transfers). In 2020, the criminal share of all cryptocurrency activity fell to just 0.34% ($10.0 billion in transaction volume).

Total cryptocurrency value sent and received by criminal entities vs. Criminal share of all cryptocurrency activity



Source: Chainalysis 2021 Crypto Crime Report, January 2021

The proportional decline point is further borne out by a 2011 United Nations Office on Drugs and Crime report[13] which estimated that between 2% and 5% of global GDP ($1.6 to $4 trillion) annually is connected with money laundering and illicit activity. The conclusion, therefore, is that criminal activity using cryptocurrency transactions is much smaller than that using fiat currency and its use would appear to be reducing year on year.

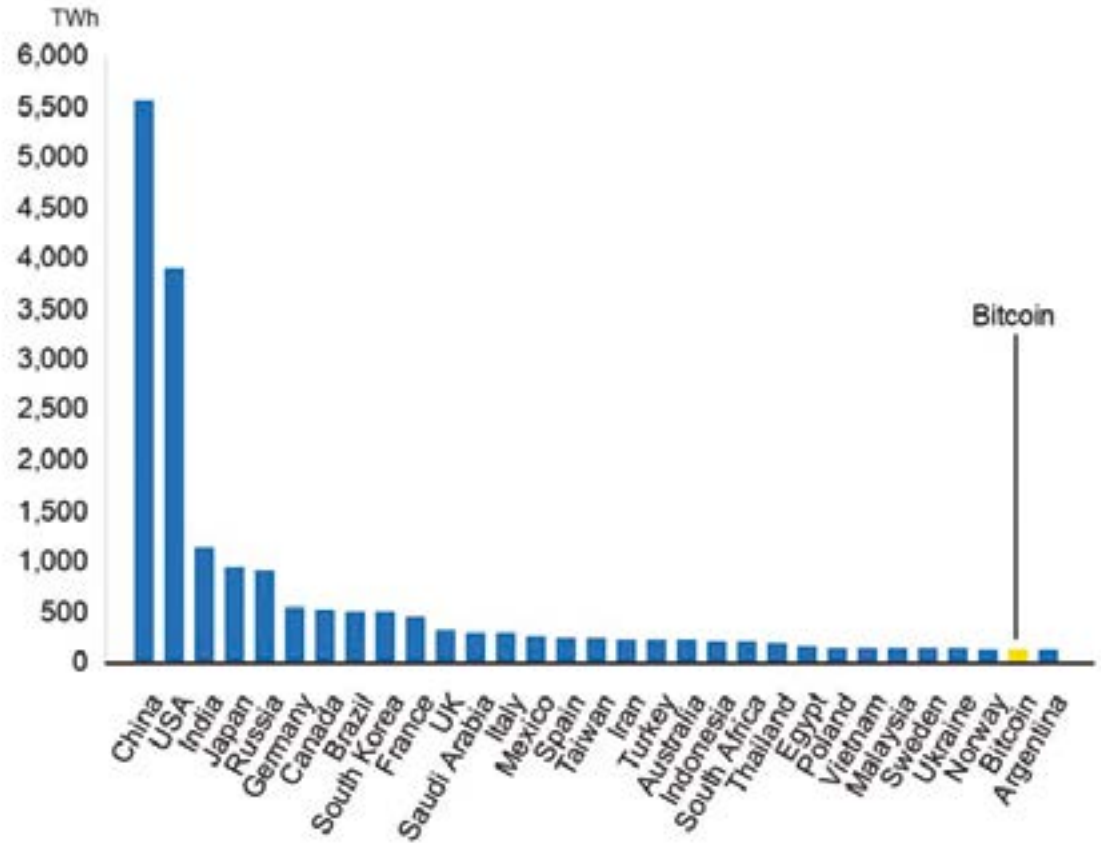
Firms would be well advised to engage with regulators on the risk realities of cryptocurrencies and, where feasible, seek to ensure the regulatory attention is on the broad issues rather than the often-myopic focus on the potential for illicit activity.

One such challenge is climate risk linked to the heavy demand for electricity used by computers to generate, or "mine" virtual currencies. According to the University of Cambridge Bitcoin Electricity Consumption Index, in February 2021, bitcoin mining was estimated to be one of the top 30 energy users in the world.

Proponents of cryptos have argued and will argue in the future that the broader benefits of cryptos must be considered. They argue that crypto miners are embracing the use of renewable energy such as hydroelectricity and are having a positive impact on the overall adoption and shift toward green energy. They also argue that energy consumption associated with bitcoin mining is difficult to compare to that of the global banking and payment systems within traditional financial services industries.

Bitcoin uses more energy than Argentina

If Bitcoin was a country, it would be in the top 30 energy users worldwide



National energy use in TW/h
Source: University of Cambridge Bitcoin Electricy Consumption Index BBC

Climate risk concerns and the electricity usage debate will continue in the future. A certainty though is that the ESG impact will be an important factor in future regulatory developments around the globe as policymakers craft new crypto regulations.

13 https://www.unodc.org/documents/data-and-analysis/Studies/Illicit_financial_flows_2011_web.pdf

The myriad risks of cyber-crime

"The speed of technological change and a growing reliance on third-party, technology-based services is increasingly introducing new risks and vulnerabilities to the sector. To begin to address this, the FSB is focused on achieving greater convergence in areas such as regulatory reporting of cyber incidents, and we will deliver those recommendations to the G20 in October."

Randal K, Quarles, Vice Chair for Supervision and Chair of the Financial Stability Board. March 2021

Crises frequently tend to be accompanied by a rise in those seeking to take advantage of the situation to perpetrate crime. In 2021, this will increasingly be associated with cyber risk, such as "ransomware" attacks demanding payment in cryptocurrencies. The benefits from digital transformation and the successful deployment of crypto-assets will be under threat if those using them have no confidence in the cyber resilience of the transaction or safekeeping.

Firms and CSPs need to be vigilant and ensure they have deployed the best possible defences against all forms of technologically enabled attack, as well as against those that seek to use cryptos to perpetrate crime.

In December 2020, the International Monetary Fund published a staff discussion note[14] entitled "Cyber Risk and Financial Stability: It's a Small World After All" focusing on the threat to financial stability from attackers that undermine, disrupt and disable information and communication technology systems.

The publication outlines the potential impact of cyber risk. It notes that attackers have broad access to technology, allowing them to operate across borders and to attack financial firms and central banks either for profit or simply to disrupt. An accompanying speech[15] entitled "Financial Inclusion and Cybersecurity in the Digital Age" given by Kristalina Georgieva , managing director of the IMF, stated two facts: on average, 106 people gain access to the internet in sub-Saharan Africa every second, while hackers attack[16] computers with internet access an average of once every 39 seconds.

The increase in the incidence of attacks, rising losses and the recognition of the potential for serious disruption to the functioning of the financial system has elevated cyber risk from a concern of IT departments to a central risk management issue for all financial institutions and a risk to system-wide stability.

In terms of definitions, "cyber" relates to the interconnected infrastructure of information and communications systems, data, processes, and persons and their interactions. "Cybersecurity" means the preservation of confidentiality, integrity, and availability of this infrastructure; "cyber risk" is the probability and impact of events that jeopardize cyber security or violate security or acceptable use policies, whether resulting from malicious activity or not. The IMF's report focuses on malicious activity.

Financial systems are at varying states of readiness to manage cyber-attacks, and the international response is fragmented. The IMF suggests there are six major gaps that, if addressed, could considerably reduce cyber risk and help safeguard financial stability. These build on the need to pay greater attention to prevention, mitigation, measurement and recovery. Addressing the gaps will require a collaborative effort by standard-setting bodies, national regulators and industry associations, as well as by international financial institutions and other capacity development providers.

The six major gaps identified, and hence areas for further work, are:

- Improving cyber risk analysis and integration into financial stability analysis.
- Driving greater consistency in regulatory frameworks, with financial supervisors. developing and promoting greater consistency in the design and implementation of national cyber-security regulatory frameworks.
- Enhancing operational resilience, response and recovery through development and testing of national and cross-border response protocols to significantly improve the ability of authorities to successfully respond to cyber incidents.
- Strengthening information-sharing by addressing obstacles to the exchange of cyber-security-related information.

14 https://www.imf.org/-/media/Files/Publications/SDN/2020/English/SDNEA2020007.ashx

15 https://www.imf.org/en/News/Articles/2020/12/10/sp121020-financial-inclusion-and-cybersecurity-in-the-digital-age?cid=em-COM-123-42402

16 https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds

- Intensifying the defence against cyber-attacks by building strong domestic capabilities and enhanced cross-border coordination of investigation and enforcement.
- Increasing capacity development by building skills, resources, and operational capacity in all countries.

The IMF is seeking to enhance the focus on cyber risk. In terms of the six areas for further work perhaps the most challenging is capacity development.

Cyber risk affects both advanced economies and low-income countries. The IMF warns countries that fall behind in their ability to resist and respond to attacks will suffer disproportionately as other countries build stronger defences. At the same time, attacks on countries strongly linked to the financial system could spill over to others and endanger financial stability.

The international community has various programs in place to assist low-income countries with the development of technical skills and resources, but additional attention to capacity and financial stability concerns would benefit the community as a whole. International financial institutions, including the IMF, have an important role to play in supporting capacity building and delivering technical assistance to financial supervisors and central banks in developing economies, to help them in their efforts to identify, measure, monitor, and address the risks to financial stability posed by cyber risks. This is imperative in an environment where the increasing digitalization of financial services delivery and the entry of many new providers may present new vulnerabilities.

Capacity development has challenges and starts from a low baseline. In September 2019, the IMF's Monetary and Capital Markets Department published a report[17] on cyber security risk supervision highlighting emerging practices that contribute to effective cyber security risk supervision. It emphasized how these practices can be adopted by regulatory and other bodies that are at an early stage of developing a supervisory approach to strengthen cyber resilience.

The cyber security risk supervision report highlighted the profound dearth of the specialist technical skills needed to combat cyber-attacks and build cyber resilience. An IMF survey of 40 developing jurisdictions revealed that 92.5% face skills shortages in cyber security regulation and supervision. The IMF said "anecdotal evidence points to a similar situation in advanced economies". Regulators will need to make considerable investments to fill such skills gaps, at a time when financial services firms are also seeking to recruit similar talent.

In the IMF's opinion, the critical lack of specialist skills should not prevent supervisors from beginning to build information-gathering and sharing systems or from improving basic security practices (cyber hygiene. Supervisors should also begin to deploy resources toward key assets and carry out basic cyber exercises, the IMF said.

Together, the IMF publications make many sensible recommendations for policymakers, financial services supervisors and, by association, the firms they regulate. The main theme is the need for more specialist skills. The IMF suggests firms can take a variety of approaches to capacity-building — for example, the acquisition of specialists, training generalist supervisors, leveraging internal resources — and says this should be expected to be a steady and continuous process. A good first step would be for firms and supervisors to undertake a skills audit to determine the exact level and nature of existing skills and then to allocate the appropriate level of resources to fill the most urgent gaps and start the required capacity building.

"The task of combating cyber-security risk can appear daunting, especially for supervisory authorities facing resource constraints, but some key actions must be taken by all," the IMF said.

Recent experience proves no corner of the financial system is immune to cyber-attacks, according to the IMF.

In an illustration of the impact of cyber-enabled crime, the estimated top-three successful crypto heists in the last decade netted around $1.3 billion:

- Coincheck crypto heist in January 2018, netted $534 million.
- Mt. Gox heist in November 2011, netted $450 million.
- KuCoin hack in September 2020, netted $280 million.

Of even more concern are the ramifications of cyber-attacks or hacking. At the end of 2020, the United States issued an emergency warning after discovering that "nation-state" hackers hijacked software used by almost all Fortune 500 companies and multiple federal agencies to gain entry to secure IT systems. The U.S. Department of Homeland Security's cybersecurity arm ordered all federal agencies to disconnect from SolarWinds' Orion platform, used by IT departments to monitor and manage their networks and systems. FireEye, a cyber-security company that said it had fallen victim to the hacking campaign, said it had already found "numerous" other victims including "government, consulting, technology, telecom and extractive entities in North America, Europe, Asia and the Middle East".

In May 2021, the Colonial Pipeline, a privately held company that transports 2.5 million barrels a day from Texas through the south-eastern United States supplying around 45% of the East Coast's supply of diesel, gasoline and jet fuel, was hit by a ransomware attack. The attack shut down the pipeline for nearly a week, causing refineries to curb operations and leading to major gas shortages, while airlines scrambled to divert jet fuel from other locations.

Colonial eventually paid a $4.4 million ransom to hackers in untraceable cryptocurrencies to regain control of their servers through a decryption tool to restore operations.

17 https://www.imf.org/~/media/Files/Publications/DP/2019/English/CRSEA.ashx

"Of the three areas I've covered, cyber presents arguably the most difficult prudential threat: unlike GCRA [governance, culture, remuneration and accountability] or climate risk, it's driven by malicious and adaptive adversaries who are intent on causing damage. Cyclones and bushfires can be devastating, but they're not doing it on purpose."

Wayne Byres, chair of the Australian Prudential Regulation Authority, in a speech to the Committee for the Economic Development of Australia, April 2021

The threat from financial crime also makes cyber resilience essential. A May 2020 paper[18] published by the FATF reported an increase in COVID-19-related crimes, including fraud, cyber crime and misdirection or exploitation of government funds or international financial assistance. The latter was seen as creating new sources of proceeds for illicit actors. The paper identified challenges, good practices and policy responses to new money laundering and terrorist financing threats and vulnerabilities arising from the COVID-19 crisis.

Emerging risks and vulnerabilities could result in criminals finding ways to:

- Bypass customer due diligence measures.
- Increase misuse of online financial services and virtual assets to move and conceal illicit funds.
- Exploit economic stimulus measures and insolvency schemes as a means for natural and legal persons to conceal and launder illicit proceeds.
- Increase use of the unregulated financial sector, creating additional opportunities for criminals to launder illicit funds.
- Misuse and misappropriate domestic and international financial aid and emergency funding.
- Exploit COVID-19 and the associated economic downturn to move into new cash-intensive and high-liquidity lines of business in developing countries.

FATF has cited virtual assets among its concerns. It has also highlighted the more widespread use of the unregulated financial sector which could also entail cryptos given the inconsistent regulatory definitions in place. Firms need to undertake a gap analysis to ensure their own practices are in line with the good or better practices referenced by FATF.

Cyber is one area where the basics done consistently well will go a long way toward providing firms and their customers with a reasonable degree of resilience.

18 https://www.fatf-gafi.org/media/fatf/documents/COVID-19-AML-CFT.pdf

Closing thoughts

Policymakers, regulators and firms all need to play their part in ensuring that cryptos are as "safe" as possible not only in terms of investment risk but with regards to regulatory certainty and cyber resilience.

> "And if things develop as some might believe, tomorrow's financial system will not be made up of banks, central banks and national currencies but of electronic signals that transfer cryptocurrencies from one digital wallet to another."
>
> **Ida Wolden Bache, deputy governor of Norges Bank (Central Bank of Norway), speech entitled "FinTech, BigTech and cryptos — will new technology render banks obsolete?", May 2021**

Supranational policymakers must continue to work toward consistent definitions of what is, and what is not, inside the regulatory perimeter. Cryptos may be treated as a currency, an investment or a security under current regulatory regimes, or they may not be covered at all. Cryptos, bitcoin in particular, may have gone mainstream but if they are to deliver their potential there is a need for clarity about how they are supervised.

A good first step would be alignment on definitions. Even if jurisdictions end up banning some or all cryptos (particularly for retail customers), it would be on the basis that international financial services had a common understanding of what was legal, and where.

In particular, there needs to be a line of sight to the risks attached to crypto products. A coherent suite of definitions will be needed, and regulators then need to agree on the risks inherent in cryptos, specifically on the risks, including:

- Financial stability;
- Vulnerable customers and those excluded from the digital world;
- The potential for money laundering and other illicit activities to take advantage of the lack of transparency and potential for anonymity;
- Competitive disruption as Big Techs develop their crypto offerings;
- The need for better cyber hygiene and operational resilience.

The developing understanding of crypto risks and their root causes will also need much better data to be shared by firms, CSPs and others. Regulators need to upgrade both technology and skill sets. Technological skill sets are already at a premium and regulators should consider investing in the skills which will be required to supervise cryptos. Firms should do the same.

The regulatory overlay for crypto-assets is rapidly evolving as several countries are at the forefront of adoption and are establishing themselves as crypto-friendly. Singapore, Bermuda, the EU, and the UK are establishing themselves as allies to varying degrees. Parts of Africa and India have meanwhile taken steps to restrict or prohibit citizens from owning or using cryptos.

Top officials in India have called cryptocurrencies a "Ponzi scheme" but have said there will be "a very calibrated position taken." The senior official told Reuters, however, that the plan is to ban private crypto-assets while promoting blockchain. The Reserve Bank of India has also voiced concern, citing what it said were risks to financial stability from cryptocurrencies while working on launching its own digital currency.

In September last year, the EU introduced a proposal to regulate crypto-assets. The Markets in Crypto-assets Regulation[19] (MICA), if adopted, will regulate all issuers and service providers dealing with crypto-assets. This could be the first comprehensive rulemaking of its kind, although it is unclear whether the regulations will provide the certainty sought by many participants or be overly burdensome, which could deter future innovation.

With crypto-asset rulemaking in Europe off to a head start, it remains to be seen if the United States will race to catch up, or given the need to accommodate multiple stakeholders, take a more wait-and-see approach. Harmonization or coordination of rules will be essential, but may not happen for some years.

In the interim, the regulatory landscape for digital assets will evolve, probably more slowly than some desire and likely at a much slower than the forms of technology themselves.

It is in everyone's interest that cryptos are subject to a regulatory regime with a clear perimeter, coherent definitions and an agreed, well-informed stance on risk and risk management.

19 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593

Compendium – Cryptocurrency regulations by country

Cryptocurrency regulations by country

June 1, 2021

By Todd Ehret and Susannah Hammond, Regulatory Intelligence

The public appetite and enthusiasm for cryptocurrencies such as bitcoin have exploded in recent years. First introduced in 2008 as an alternative and disruptive technology to traditional banking and payments, bitcoin and other digital currencies or digital assets were met with skepticism and caution as they were not understood. Their anonymity also made cryptocurrencies susceptible to misuse in illicit activities.

Much has changed in recent years, as the number of users has exploded, and some established financial services firms have also begun to test the crypto waters. Prices have rocketed despite incredible volatility, and financial regulators and regulations have struggled to keep pace.

The regulatory regime surrounding cryptocurrencies is fragmented and stretches to the extremes of outright bans in some jurisdictions, to some countries that are advocates.

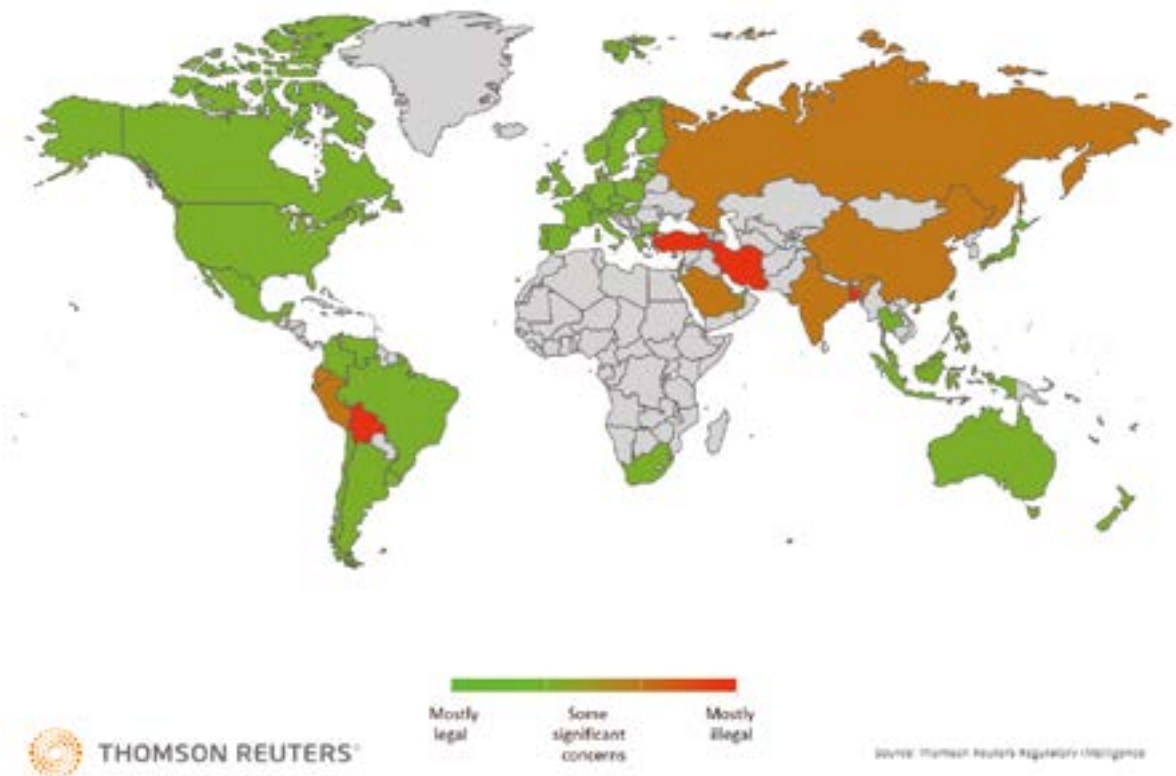
Complete restrictions are somewhat rare and difficult to enforce, with crypto markets regularly shrugging off news of restrictions in some jurisdictions, but regulators are scrambling to clarify rules and keep pace with crypto's exploding popularity.

The regulatory overlay related to digital assets such as bitcoin and other cryptocurrencies in its infancy, and the challenge of building a regulatory framework often is complex and uncertain.

Many market participants insist on a more established regulatory regime and certainty, which likely means new rules, regulations, or at a minimum official guidance. The race to create such a regulatory regime is now underway.

Crypto-assets, cryptocurrencies, central bank digital currencies and non-fungible tokens make up the new "crypto" universe, and each provides unique benefits, challenges, and complexities. This annex provides a country-by-country summary of the cryptocurrency regulatory picture. The list below focuses on cryptocurrencies such as bitcoin. It provides an overview for each country, the regulatory state of play and links to the primary financial regulatory authorities or relevant documents. Much of the regulatory framework is still developing, and regulations and restrictions also vary greatly depending on uses such as payments, investments, derivatives, and tax status. Most countries have generally found ways to tax gains or income derived from cryptocurrencies, and some have more specific obligations than others. Few pure "tax havens" remain.

Regulatory Intelligence may delve deeper into other aspects of cryptos such as non-fungible tokens and digital central bank currencies in future articles or special reports.



North America

Canada – Canada has been an early adopter and is seen as quite "crypto-friendly" with several approvals of bitcoin exchange-traded funds (ETFs). Canadian Securities Administrators (CSA) and the Investment Industry Regulatory Organization of Canada (IIROC) have issued guidance requiring crypto trading platforms and dealers in Canada to register with the local provincial regulators. Firms dealing with cryptos are considered money service businesses (MSBs) and must also register with the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC). The requirements also apply to foreign-based firms if they have Canadian customers.

The Canada Revenue Authority (CRA) generally treats cryptocurrency like a commodity for purposes of the Income Tax Act.

Mexico – Mexico has embraced cryptocurrencies and is seen as a very crypto-friendly jurisdiction. The Mexican government and the financial authority, CNBV enacted a new set of fintech laws in March 2018. Its largest crypto exchange, Bitsos, has more than 1 million users on its platform.

Mexico's Federal AML Law was amended in March 2018 to include transactions with "virtual assets".

Mexico's tax framework for cryptocurrencies is expected to change as there is no official position. Most see cryptos as intangible assets where gains would be taxed at 30% for corporations and anywhere from 2% to 35% for individuals.

United States – The regulatory framework for cryptocurrencies is evolving despite overlap and differences in viewpoints between agencies. Although the Securities and Exchange Commission is widely seen as the most powerful regulator, Treasury's FinCEN, the Federal Reserve Board, and the CFTC have issued their own differing interpretations and guidance. The SEC often views cryptos as securities, the CFTC calls bitcoin a commodity, and Treasury calls it a currency. The Internal Revenue Service (IRS) defines cryptocurrencies as "a digital representation of value that functions as a medium of exchange, a unit of account, and/or a store of value" and has issued tax guidance accordingly.

Despite the muddied regulatory framework, the United States is seen as home to the largest number of crypto investors, exchanges, trading platforms, crypto mining firms and investment funds.

Central and South America

Argentina – In Argentina, investing in cryptocurrencies is legal but they are not considered legal currency or tender as they are not issued by the government. Although there are no regulations, profits are taxable. Legislation has been proposed to create a national legal and regulatory framework for crypto-assets as a means of payments, investments, and transactions.

The Argentina Securities and Exchange Commission (CNV) will be the regulatory body with oversight responsibilities and plans to maintain a national registry of operations with transactions reported to the Financial Information Unit (FIU) for compliance with anti-money laundering requirements.

Argentina's Federal Administration of Public Income (AFIP) and central bank have requested more information from domestic crypto exchanges and banks. Gains from cryptos are generally taxable at a 4% to 6.5% rate on gross income for each digital currency transaction.

Bolivia – The Bolivian government banned the use of cryptocurrencies such as bitcoin in 2014, in the belief that it would facilitate tax evasion and monetary instability. "It is illegal to use any kind of currency that is not issued and controlled by a government or an authorized entity," Bolivia's central bank (BCB) said.

Brazil – Cryptocurrencies in Brazil are largely unregulated. Legislators have, however, begun to propose a series of regulations that might fill the void if enacted. The Brazilian Securities and Exchange Commission, or CVM has approved two crypto ETFs. The Brazilian government has declared that bitcoin is an asset and therefore is subject to capital gains taxes. Brazil has said that existing AML laws extend to virtual currencies in a few contexts.

The Special Department of Federal Revenue of Brazil has published a document on cryptocurrency taxes in the country.

Chile – The Chilean government has committed to develop a regulatory and oversight framework for cryptocurrencies and the growing number of cryptocurrency exchanges in the country. In the absence of a legal framework, the Central Bank and the Financial Market Commission has said that existing regulations are applicable to cryptocurrencies.

The Chilean Internal Revenue Service (SII) is the only institution so far to have issued legislation on cryptocurrencies in Notice no 963, issued on May 14, 2018. The SII released a determination on the taxation of income obtained from buying and selling cryptocurrencies. It said that Tax Form 22 would require the declaration "from the sale of foreign currencies of legal course or assets digital/ virtual, such as cryptocurrencies (for example, bitcoins)".

Colombia – In Colombia there is no specific legislation regulating the use of cryptocurrencies. The Banco de la República, the country's monetary, exchange and credit authority, and the Superintendencia Financiera de Colombia (SFC), the government agency responsible for overseeing financial regulation and market systems, released statements on cryptos warning they are not legal tender or valid investments for supervised entities, and firms are not authorized to advise or manage them.

The Superintendency of Corporations in Colombia has stated that companies can legally purchase cryptos such as bitcoin, however such "intangible assets" are unregulated. The country's tax authority, Directorate of National Taxes and Customs (DIAN) said "virtual currencies are not money for legal purposes. However, in the context of mining activity, insofar as they are received in exchange for services and/or commissions, they correspond to income and, in any case, to goods that can be valued and generate income for those who obtain them as from be part of your patrimony and take effect in tax matters."

The SFC has authorized the creation of a sandbox test environment for supervised firms and crypto-asset exchange platforms to test the handling of transactions.

Ecuador – In January 2018 the Central Bank of Ecuador informed citizens that bitcoin "is not a means of payment authorized for use in the country". Financial transactions are not controlled, supervised, or regulated by any entity in the country, and this presents a financial risk to those who use it.

Despite this warning, the Central Bank has said that " the purchase and sale of cryptocurrencies - such as bitcoin - through the internet is not prohibited".

Peru – There has been no specific legislation in Peru related to cryptocurrencies and no supervision is provided by the Securities Market Agency (SMV), the Banking, Insurance and Pension Fund Manager Agency (SBS), or the Peruvian Central Reserve Bank (BCRP). The BCRP has said that these financial assets are not legal tender, nor are they supported by central banks, so they fail fully to meet the functions of money as a medium of exchange, unit of account and store of value.

The regulators in Peru have issued several public warnings about the potential risks of loss in virtual currencies as they are not supervised by the SBS, and that the assets could be used in unlawful activities. The SBS has said it will assess the option of regulating the cryptocurrency sector to prevent asset laundering activities.

Uruguay – There is no specific legislation on cryptocurrencies in Uruguay. The Uruguayan Chamber of FinTech has, however, announced the formation of a cryptocurrency committee to analyze what future regulations might look like. The country is widely viewed as bitcoin and blockchain-friendly with no regulations specifically banning or permitting the use of cryptocurrencies.

Venezuela – Prior to 2018, law enforcement arrested and seized assets of bitcoin miners but has now declared cryptocurrencies such as bitcoin legal. The Superintendency of Crypto-assets and Related Activities of Venezuela (SUPCACVEN) is the governmental agency in charge of regulations, control, and protection of crypto-assets. The government of Venezuela has also created its own cryptocurrency called the Petro, which is backed by the value of Venezuelan oil.

Europe

Austria – The Financial Market Authority (FMA) has warned investors that cryptocurrencies are risky and that the FMA does not supervise or regulate virtual currencies, including bitcoin, or cryptocurrency trading platforms. "Bitcoins are a virtual currency and are not subject to supervision by the Financial Market Authority. For some bitcoin-based business models, it may, however, be necessary to hold a license issued by the Financial Market Authority."

Cryptocurrencies are legal and are not considered a form of currency or a financial instrument. The Austrian Ministry of Finance classes cryptocurrencies as "other (intangible) commodities".

As a member of the EU, regulations and guidance issued by the European Supervisory Authorities (the European Banking Authority (EBA), the European Insurance and Occupational Pensions Authority (EIOPA) and the European Securities and Markets Authority (ESMA)) apply . Virtual currencies are defined by the European Central Bank (ECB) as "a digital representation of value, not issued by a central bank, credit institution or e-money institution, which, in some circumstances, can be used as an alternative to money".

Belgium – The Belgian Financial Services and Markets Authority and the National Bank of Belgium have published guidance and warnings to the public regarding scams and concerning investor protection. Belgium has, however, fostered a strong fintech community involved in digital assets and blockchain.

Gains on cryptocurrencies are taxable by the Special Tax Inspectorate (STI) as "miscellaneous income".

As a member of the EU, regulations issued by the European Supervisory Authorities (EBA, EIOPA and ESMA) apply. Virtual currencies are defined by the European Central Bank (ECB) as "a digital representation of value, not issued by a central bank, credit institution or e-money institution, which, in some circumstances, can be used as an alternative to money".

Bulgaria – The Bulgarian National Bank and the Bulgarian Commission for Financial Supervision have not defined cryptocurrencies as financial instruments or electronic money. Firms providing services for cryptocurrencies such as exchanges and digital wallets are required to register with the National Revenue Agency and declare activities, as gains on transactions are taxable and treated as income.

Bulgarian regulators have issued various standard warnings to the public and potential investors about risks associated with digital assets and ICOs. As a member of the EU, European Supervisory Authorities (EBA, EIOPA and ESMA) regulations and guidance apply.

Czech Republic – In the Czech Republic, cryptocurrency is largely unregulated and is regarded as a commodity rather

than a currency and are not an official means of payment. The Czech National Bank (CNB) permits Czech banks to offer crypto-related services as long as they comply with AML regulations.

The Czech Republic has implemented a stricter legal model than AMLD5 requiring that every cryptocurrency-related firm be regulated by the Czech government. AML regulations apply to anyone that provides cryptocurrency services, including "those who buy, sell, store, manage, or mediate the purchase or sale of cryptocurrencies or provide other services related to such currencies as a business."

Cryptocurrencies for individuals are taxed at a rate of 15%, while businesses are taxed at a rate of 19%.

Denmark – The Danish Financial Supervisory Authority (FSA) is the main supervisory authority in Denmark. Cryptocurrency regulation is, however, influenced by EU law. An amendment in January 2020 to the Danish Act on Measures to Prevent Money Laundering and Financing of Terrorism defines a virtual currency as "a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically".

Denmark has also implemented the Fifth European Directive on Anti-Money Laundering (AMLD5)

The Danish central bank, the Nationalbanken, is working on developing a digital currency, the "e-krone."

Estonia – Estonia has been an early crypto frontrunner with more than 1300 crypto exchanges. In January 2021 the Ministry of Finance in Estonia proposed to regulations for virtual currency service providers. The new regulations require "virtual currency service" firms to have their registered office, management, and place of business located in Estonia. Such firms include wallets and trading platforms,

Although virtual currencies are not subject to securities regulation in the EU, the new rules attempt to address some of the regulatory issues. Firms will be subject to the supervision of the Financial Supervision Authority which will require minimum capital standards, IT standards, audits, and reporting. All current license holders are required to re-apply for a new license.

Income derived from cryptocurrencies in Estonia are taxable by the county's Tax and Custom Board.

Finland – In May 2019, Finland's Financial Supervisory Authority (FSA) began regulating virtual currency exchange providers, wallets, and issuers of virtual currencies. Registration is required to ensure compliance with statutory requirements surrounding reliability of the provider, protection of client money, segregation of assets, marketing, and compliance with AML/CFT regulations.

The FSA has warned consumers of the risky, volatile and speculative nature of the investments. Finland has joined the European Blockchain Partnership and agreed to the Fifth European Directive on Anti-Money Laundering (AMLD5).

France – In April 2019, the French National Assembly adopted the Plan d'Action pour la Croissance et la Transformation de Enterprises (PACTE – Action Plan for Business Growth and Transformation) that will establish a framework for digital asset services providers. France's Financial Market Authority (AMF) has adopted new rules and regulations for cryptocurrency service providers and ICOs, related to the (PACTE).

The French Ministry of Finance plans to propose new AML/CFT rules related to digital assets. The new rules would impose new requirements on crypto exchanges and would prohibit anonymous accounts. The new regulations would better harmonize the French AML framework with Financial Action Task Force (FATF) principles and respond to new risks associated with digital assets.

Germany – The German government was one of the first countries to provide legal certainty to financial institutions allowing them to hold crypto-assets. Regulations stipulate that citizens and legal entities can buy or trade crypto-assets as long as it is done through licensed exchanges and custodians. Firms must be licensed with the German Federal Financial Supervisory Authority (BaFin).

Germany has signed up to requirements under the EU Fifth Anti-Money Laundering Directive (AMLD5). Germany has established licensing requirements for custody services and has defined crypto-assets as a digital representation of value, not issued or guaranteed by a central bank or public authority, with no legal status of currency or money. Crypto-assets are, however, based on agreement and accepted a means of exchange or payment, an investment, and can be transferred, stored, and traded electronically.

Greece – The Hellenic Capital Market Commission views cryptocurrencies as portfolio assets and not currency. It requires providers of digital wallets, custody services, and exchange services between cryptos and fiat currencies to be registered.

Greece has joined the European Blockchain Partnership and agreed to the Fifth European Directive on Anti-Money Laundering (AMLD5).

Taxation for mining is considered income from commercial enterprises and the profits that will arise after deducting the operating expenses are taxed according to the general provisions and the applicable tax rates. Holders of cryptocurrencies are taxed at a rate of 15% as income from capital gains.

Bailiwick of Guernsey – The territory of Guernsey within the British Isles is known as a Crown Dependency but is not part of the United Kingdom, rather a self-governing possession of the British Crown. The Guernsey Financial Services Commission (GFSC) is the body responsible for the regulation of the finance sector.

Although the GFSC has warned of the risks associated with cryptos, it has taken a light regulatory approach. According to the GFSC website, "Virtual or crypto currencies could interact with our regulatory laws in a number of ways and therefore any application would need to be assessed on its individual merits. We will assess any application by the same criteria we use for other asset types or structures, which means we would look to ensure that key controls are appropriate - for example around custody, liquidity, valuation of assets and investor information."

The GFSC has stated that it will assess applications on individual merits against the criteria used for asset types or structures, as cryptocurrencies "could interact with regulatory laws in a number of ways." Applicants must demonstrate how they will comply with AML/CTF laws and rules. The GFSC has also said it would be cautious to approve applications for ICOs and applications for any kinds of digital currency exchanges.

There are no specific laws in Guernsey regulating the taxation of virtual currencies. However, Guernsey is party to an intergovernmental agreement with the United States regarding the Foreign Account Tax Compliance Act of 2009 (FATCA).

Hungary – The National Bank of Hungary, the Magyar Nemzeti Bank (MNB) has issued a public statement warning citizens who use or invest in cryptocurrencies such as bitcoin, citing their unregulated nature and risks with cryptocurrencies. The MNB published a report on FinTech and digitalization in April 2020 that included an analysis of the FinTech sector, profitability, and services across the FinTech market.

Lawmakers have considered reducing taxes on cryptocurrency trading to 15% of income, down from the current rate of 30.5% to try to stimulate the economy after being hard hit by the COVID pandemic.

Cryptocurrency regulations are underdeveloped in Hungary. However, Hungary has joined the European Blockchain Partnership and agreed to the Fifth European Directive on Anti-Money Laundering (AMLD5).

Ireland – The Central Bank of Ireland has issued warnings on the risks associated with cryptocurrencies such as bitcoin and Ether as they are unregulated. Although they can be used as a means of payment, they do not have legal tender status, and are not guaranteed or regulated by the Central Bank of Ireland, or any other central bank in the EU. Ireland's Department of Finance has proposed the creation of a new blockchain working group to help create a coordinated approach to rules around cryptos. The group published a report titled, "Virtual Currencies And Blockchain Technology."

Ireland's Office of Revenue Commissioners released a manual on the tax treatment of various transactions under cryptocurrencies. It clarified that ordinary tax rules apply, and that cryptocurrency mining would generally not be subject to VAT.

Ireland has joined the European Blockchain Partnership and agreed to the Fifth European Directive on Anti-Money Laundering (AMLD5).

Isle of Man – The territory of Guernsey within the British Isles is known as a Crown Dependency but is not part of the United Kingdom, rather a self-governing possession of the British Crown. The Isle of Man is considered one of the most attractive locations for crypto companies because of secure data centers, low cost of electricity, friendly regulatory and tax environment.

The Isle of Man Financial Services Authority (FSA) and the Digital Isle of Man, an executive agency within the government's enterprise department published guidance aimed at giving companies greater clarity when setting up blockchain-related business in the jurisdiction.

Cryptocurrencies such as bitcoin are considered securities and fall outside regulatory oversight. However, companies involved with the assets must register with the FSA and comply with AML/CTF requirements. Tokens or cryptocurrencies that offer a store of value or access to services and are not a form of e-money would be unregulated.

Italy – Italy joined the European Blockchain Partnership (EBP) along with 22 other countries in April 2018. The EBP was established to enable member states to work together with the European Commission on blockchain technology.

Cryptocurrencies and blockchain are regulated at the legislative level in Italy under Legislative Act no. 90. The decree in 2017 grouped cryptocurrency exchanges with foreign currency exchanges. Although the decree states that cryptocurrencies are not issued by the central bank and are not correlated with other currencies, it is a virtual currency used as a medium of exchange for goods and services. Italian AML regulations are based on EU and FATF recommendations.

Bailiwick of Jersey – The territory of Guernsey within the British Isles is known as a Crown Dependency but is not part of the United Kingdom, rather a self-governing possession of the British Crown. In 2016 amendments to the Proceeds in Crime Law categorize virtual currency as a form of currency. Financial services business such as exchanges are subject to Jersey's AML requirements and must comply with the island's laws, regulations, policies and procedures related to AML/CTF.

Virtual currency exchanges are a supervised business and are required to register with, and fall under the supervision of, the Jersey Financial Services Commission (JFSC).

Mining of cryptos on a small scale in Jersey is not taxable. However, exchanging cryptocurrencies to and from conventional currencies and other cryptocurrencies will be liable to income tax, if they are considered to be "trading."

Latvia – Latvia's Financial and Capital Market Commission has warned investors that cryptocurrencies "operated in

an infrastructure that is currently characterized by lower regulation than in the financial and capital markets."

In the past several years Latvia has launched an effort to improve its AML regulations. In 2019 it expanded the role of the Financial and Capital Market Commission to cover AML/CTF and impose beneficial ownership requirements on local limited companies, foundations, unions, and other enterprises.

The Latvian Finance Ministry imposes a 20% tax on capital gains from cryptocurrencies

Latvia signed a declaration creating the European Blockchain Partnership.

Lithuania – The Bank of Lithuania (LB) defined cryptocurrencies in 2017. Also known as virtual currencies, cryptocurrencies such as bitcoin is non-regulated digital money that can be used as means of payment, and this money is issued and guaranteed by a non-central bank.

Lithuania requires crypto firms to register with the country's Center of Registers. Registrants must adopt comprehensive KYC and AML procedures and are expected to inform the Financial Crime Investigation Service (FCIS) about large transfers.

In a June 2020 report from the EU, Lithuania has made progress towards eliminating gaps in its regulation and supervision of cryptocurrency and claims to have gone beyond requirements in the fifth EU Anti-Money Laundering Directive (AMLD 5).

Lithuania State Tax Inspectorate considers cryptos as "property" and asses a 15% rate on the gains.

The Netherlands – The Dutch Central National Bank De Nederlandsche Bank N.V., (DNB) requires crypto firms to register. In May 2020 the Dutch Implementation Act amended Dutch AML rules and implemented the Fifth European Directive on Anti-Money Laundering (AMLD5).

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

Norway – The Financial Supervisory Authority of Norway "Finanstilsynet" and the country's Ministry of Finance has established money laundering regulations which apply to "Norwegian providers of virtual currency exchange and storage services."

Although the laws require firms such as storage services and exchanges that convert cryptos to fiat currency to comply with AML rules, it does not impose other regulatory obligations on other crypto services.

"Finanstilsynet will ensure that virtual currency exchange and storage providers comply with the money laundering rules. However, FSA does not have any tasks monitoring other areas of these providers, such as investor protection," the regulator said.

Poland – The National Bank of Poland and the Polish Financial Supervision Authority (KNF) have warned of the risks associated with cryptocurrencies. The KNF has said that the cryptocurrency market is not a regulated or supervised market. "The KNF does not authorize, supervise or exercise any other supervisory powers in relation to the trade in cryptocurrencies. Some entities operating in the cryptocurrency market are authorized to provide payment services, in particular to settle payments made with legal tender (fiat money) in exchange for the cryptocurrencies being bought or sold."

Cryptocurrencies are not considered legal tender. Gains on digital assets are, however, subject to capital gains taxes and VAT. Poland signed a declaration creating the European Blockchain Partnership (EBP).

Portugal – Despite issuing warnings about the risks related to cryptos, Portugal is widely seen as the most crypto-friendly country in Europe. The legal status of cryptocurrency in Portugal was officially clarified in a statement by the Portuguese tax authorities and was subsequently reaffirmed by the *Journal de Negocios*. Portugal does, however, follow EU regulation as has agreed to the Fifth European Directive on Anti-Money Laundering (AMLD5).

The country's non-habitual tax regime (NHR) has attracted many crypto traders as it allows for exemptions and reductions in tax for a 10-year period for individuals of high cultural or economic worth.

"An exchange of cryptocurrency for 'real' currency constitutes an on-demand, VAT-free exercise of services," the Portuguese tax authorities have said.

Spain – Spain was a notable early hot spot for cryptocurrencies among EU members, with merchants accepting payments and bitcoin kiosks in the streets. Despite no formal legal status, virtual currencies in Spain are taxable as income and under VAT.

In 2021 the Spanish Securities and Exchange Commission, the Comision Nacional del Mercado de Valores (CNMV) and the Bank of Spain issued a joint statement warning of the risks and volatility. The joint statement also highlighted that, from a legal standpoint, cryptocurrencies are not a means of payment and are not backed by a central bank or other customer protection mechanisms or authority.

The Royal Decree Law 5/2021 included a provision giving the CNMV power to regulate advertising related to cryptocurrencies.

Sweden – The Swedish Financial Supervisory Authority (FSA) and the central bank have publicly declared bitcoin as a legal. From a tax perspective they are viewed as an asset, not a currency or cash.

The FSA has warned of the risks associated with cryptos and investment products with cryptos as underlying assets such as exchange traded products (ETPs). Sweden has imposed regulatory registration requirements that subjects custodians, wallet providers, and exchanges to comply with the Swedish Anti-Money Laundering Act.

Sweden's Central Bank, the Riksbanken, has been a leader in developing a digital central bank currency, the e-krona.

Switzerland – Switzerland is known as one of the most cryptocurrency-friendly nations in the world. Switzerland's financial markets regulator, the Swiss Financial Market Supervisory Authority (FINMA) has defined licensing requirements for cryptocurrency businesses of all types including bitcoin kiosk operations, and has created requirements for blockchain companies.

Cryptocurrency businesses are subject to AML regulations and licensing requirements under FINMA. FINMA's regulatory environment complies with the FATF's digital asset regulation issued in June 2019.

Turkey – Although not "illegal" in Turkey, authorities have demanded user information from crypto trading platforms. Turkey's Central Bank has banned the use of cryptocurrencies, and other such digital assets based on distributed ledger technology cannot be used, directly or indirectly, to pay for goods and services. The central bank has said crypto-assets are "neither subject to any regulation and supervision mechanisms nor a central regulatory authority".

United Kingdom – The UK Financial Conduct Authority (FCA), HM Treasury, and the Bank of England make up the country's Crypto-assets Taskforce.

The FCA has created regulations to cover know your customer (KYC), AML and CFT tailored for crypto-assets. It has also created regulations to cover virtual asset service providers (VASPs) but has been careful to not stifle innovation. Crypto exchanges must register with the FCA unless they have applied for an e-money license. Cryptocurrencies are not considered legal tender and taxes are levied based on activities. The FCA has banned the trading of cryptocurrency derivatives.

The UK published a call for evidence on digital assets in April 2021. The request seeks input from stakeholders ahead of publication of a consultation paper on digital assets which will make proposals for new laws.

Asia, Australia and rest of world

Australia – In 2018 new laws for digital currency exchange providers operating in Australia were implemented by the Australian Transaction Reports and Analysis Centre (AUSTRAC), Australia's financial intelligence agency and anti-money laundering and counter-terrorism financing (AML/CTF) regulator.

Firms are required to register and implement KYC policies, report suspicious transactions, and comply with AML legislation.

Bangladesh – The Bangladesh Central Bank issued warnings in 2014 and 2017 related to transactions in cryptocurrencies and warned violations could be punishable by up to 12 years in jail under existing money laundering and terrorist financing regulations. Despite prohibitions on the use of cryptocurrencies, Bangladesh has proposed a national "blockchain strategy" perhaps signaling a change in the future. However, concerns over a foreign flight of local capital is a major concern hindering cryptos.

Bermuda – The offshore finance and insurance center Bermuda, has adopted a business-friendly approach to the oversight of cryptos and related businesses. The Digital Asset Business Act and the Companies and Limited Liability Company Initial Coin Offering Amendment Act, passed in 2018, defines digital assets and provide standards governing ICOs and digital asset businesses.

ICOs are classified as a restricted business activity that requires approval from the Bermuda Monetary Authority. Digital asset businesses are required to register and comply with AML/CTF regulations, specifically, the Proceeds of Crime Acts.

There are no specific taxes on income, capital gains, or other taxes on digital assets in Bermuda.

Cayman Islands – In May 2020, Cayman Islands lawmakers enacted several new legislative acts regulating the cryptocurrency industry. The centerpiece, the Virtual Asset Service Provider (VASP) Law, makes it mandatory for digital asset businesses to be registered with the Cayman Islands Monetary Authority (CIMA).

The Cayman's new crypto regulations provide regulatory certainty for VASPs and align with international anti-money laundering (AML) and counter-terrorism funding (CFT) regulations to protect consumers and to meet the requirements of the FATF Recommendations.

China – The People's Bank of China banned financial institutions form dealing in cryptocurrencies in 2013 and later expanded the bans to crypto exchanges, and ICOs. China has been the epicenter for mining because of low electricity costs. Although a ban on crypto mining was considered, in 2019 the government reconfirmed that it would remain legal. In May 2021, China's Financial Stability and Development Committee, the financial regulatory agency under Vice-Premier Liu He, said the Chinese government would "crack down on bitcoin mining and trading behaviour, and resolutely prevent the transfer of individual risks to the society."

Despite the prohibitions on some crypto activities, and warnings it is not illegal for Chinese to hold or trade bitcoin or other cryptocurrencies, however, many are considering

relocating, or opting for work arounds such as foreign-based exchanges and websites.

The PBOC has embraced blockchain technology and has been on the forefront of developing the central bank's digital currency, the digital yuan.

Hong Kong – Hong Kong has long been vying to be a FinTech hub. However, the Hong Kong Securities and Futures Commission (SFC) has enacted a strict regulatory framework and licensing requirements for virtual asset service platforms (VASPs). It has also proposed a ban of crypto trading for retail investors. Only professional investors who have over HK$8 million in assets would be allowed to trade.

Bitcoin is defined as a virtual commodity and not legal tender. There are no capital gains taxes and AML/CFT laws apply to every individual or business in Hong Kong, irrespective of activity and are in accordance with FATF requirements.

India – In 2018 the Reserve Bank of India (RBI) banned cryptocurrency trading and prohibited Indian banks from dealing with cryptocurrency exchanges over consumer protection, AML, and market integrity concerns. However, in 2020 the Indian Supreme Court struck down the ban clarifying that no prohibition exists.

Despite widespread concerns, skepticism, and the prior bans on cryptocurrencies, India has encouraged innovation and the use of blockchain. It has also begun work on a state-backed digital central bank currency, the digital Rupee.

Indonesia – In Indonesia virtual currencies are not considered legal tender. In 2019 the Indonesian Commodity Futures Trading Regulatory Agency (Bappebti) approved regulation no. 5/2019 which legally recognizes and regulates bitcoin and other cryptocurrencies as commodities. Derivative transactions, and cryptocurrency exchanges are also subject to regulatory requirements of Bappebti.

The regulation defines a "Crypto Asset" as "an intangible commodity in the form of a digital asset that uses cryptography, a peer-to-peer network and distributed-ledger technology to regulate the creation of new units, verify transactions and ensure transaction security without the involvement of a third party intermediary."

Bank Indonesia, the country's central bank has banned the use of cryptocurrencies as a payment tool.

Iran – The Iranian Central Bank has authorized banks and currency exchanges to use cryptocurrencies mined by licensed crypto miners in the county. Although mining is legal, the country takes a heavy-handed approach requiring firms to sell cryptos to the central bank to fund imports.

The country has issued over a thousand licenses to crypto miners and shut down unlicensed firms. Trading outside the country has been banned, to stop capital flight. The use of cryptos for payments has also been banned.

Israel – The Israeli Securities Authority has ruled that cryptocurrency is a security (link in Hebrew) subject to Israel's Securities Laws.

The regulator has warned the public of the risks associated with cryptocurrencies. The Israel Money Laundering and Terror Financing Prohibition Authority has taken a similar approach to AML/CTF requirements as FATF. The Israel Tax Authority defines cryptocurrency as an asset and demands 25% on capital gains.

Japan – Japan has one of the most progressive and developed regulatory regimes for cryptocurrencies. Cryptocurrency exchanges must be registered and comply with traditional AML/CFT and other regulations. They are regulated under the Payment Services Act (PSA) which defines "cryptocurrency" as a property value and not a legal tender.

In December 2017, Japan's National Tax Agency ruled that gains on cryptocurrencies should be categorized as "miscellaneous income" and taxed accordingly. There have been several new regulations and amendments to the PSA and to the Financial Instruments and Exchange Act (FIEA), introducing the term "crypto-asset," and regulating crypto derivatives trading. Cryptocurrency custody service providers (that do not sell or purchase crypto-assets) fall under the scope of the PSA, while cryptocurrency derivatives businesses fall under the scope of the FIEA.

In April 2020, Japan was the first country to create self-regulatory bodies, the Japanese Virtual Currency Exchange Association (JVCEA) and the Japan STO Association. The JVCEA and the STO Association promote regulatory compliance and play a significant role in establishing best practices and ensure compliance with regulations.

Malaysia – The Securities Commission Malaysia (SC) issued guidelines on the regulation of various digital currency platforms operating in the country. The Capital Markets and Services (Prescription of Securities) (Digital Currency and Digital Token) Order 2019 ruled that digital tokens are "securities" for purposes of securities laws.

Digital currency is defined as "a digital representation of value recorded on a distributed digital ledger that functions as a medium of exchange and is interchangeable with any money including through the crediting and debiting of an account." All exchange offerings and digital asset custodians are required to register and "assess and conduct the necessary due diligence on the issuer, review the issuer's proposal and the disclosures in the whitepaper, and assess the issuer's ability to comply with the requirements of the Guidelines and the SC's Guidelines on Prevention of Money Laundering and Terrorism Financing."

New Zealand – The Financial Markets Authority of New Zealand has determined that certain activities considered "financial services" include exchanges, wallets, deposits, broking and ICOs involving crypto-assets that are classed as "financial products" under the FMC Act of 2013, additional

obligations will apply. The Inland Revenue Department (IRD) of New Zealand considers cryptocurrencies as "property" with gains and losses taxable.

Philippines – The Philippine Central Bank, the Bangko Sentral ng Pilipinas (BSP) requires virtual asset service providers (VASPs) to register. The BSP has developed an AML framework in line with FATF guidelines.

The BSP licensing requirements include exchanges of virtual assets and fiat currency. All transactions are treated as cross-border wire transfers and crypto service providers are expected to comply with relevant BSP rules. Additionally, BSP licensed firms must comply with rules for money service businesses such as liquidity risk management, IT risk management, and consumer protection.

The National Internal Revenue Code (NIRC) of the Philippines states that any income of an individual or corporation, in whatever form, obtained in the Philippines is taxable.

Russia – In 2020, Russian President Vladimir Putin signed into a law that regulates digital financial asset transactions. Under the law which took effect on January 1, 2021, digital currencies are recognized as a payment means and investment. However, the digital currency cannot be used to pay for any goods and services.

Previously digital currencies were banned. Russian banks and exchanges can become exchange operators of digital financial assets if they register with the Bank of Russia.

The Central Bank of Russia has also unveiled plans to develop a digital central bank currency, the Digital Ruble.

Saudi Arabia – The Saudi Arabian Monetary Authority (SAMA) and Minster of Finance have warned "against dealing or investing in virtual currencies including cryptocurrencies as they are not recognized by legal entities in the kingdom. They are outside the scope of the regulatory framework and are not traded by financial institutions locally. Such crypto currencies have been associated with fraudulent activities and attract suspicion of use in illegal and illegitimate financial activities in addition to their high-investment risks related to frequent price fluctuations."

While SAMA has warned the public of risks of cryptocurrencies, and that they are not legal tender, bitcoin is accepted by small businesses and merchants.

SAMA has begun using blockchain technology in its activities in the banking sector and to keep pace with market trends. SAMA has also created a regulatory sandbox for collaboration on new digital banking services and blockchain education programs.

Singapore – Cryptocurrencies are regulated by the Monetary Authority of Singapore (MAS). The Payment Services Act of 2019 regulates traditional and cryptocurrency payments and exchanges. The Securities and Futures Act is also applicable for public offerings and issues of digital tokens.

A May 2020 Guide to Digital Token Offerings published by the MAS, details the regulations surrounding digital tokens and their applicability to securities, collective investments, derivative contracts and the determination if a token is a type of "capital market product." The AML/CFT provisions under the PSA address the risk of financial crimes and promotes best practices, including KYC, to help crypto businesses comply with the new regulatory framework.

The Inland Revenue Authority has said, "Businesses that choose to accept digital tokens such as bitcoins for their remuneration or revenue are subject to normal income tax rules. They will be taxed on the income derived from or received in Singapore. Tax deductions will be allowed, where permissible, under our tax laws."

South Africa – The South African Reserve Bank, the Financial Sector Conduct Authority, and the National Treasury, and an Intergovernmental FinTech Working Group have published plans to develop a registration regulatory framework. The plans would codify FATF AML recommendations.

Virtual currency is not considered legal tender in South Africa.

The South African Revenue Service (SARS) considers cryptocurrencies such as bitcoin to be intangible assets rather than currency or property. They are taxed as long-term or short-term income ranging from 18% to 40% allowing for deduction of costs.

South Korea – Regulators in South Korea have taken a cautious approach to cryptocurrency exchanges and companies. Companies are subject to equivalent AML and tax obligations as other financial institutions.

In the wake of several large crypto-exchange hacks, South Korea passed the "Act on Reporting and Using Specified Financial Transaction Information," also known as the Financial Transaction Reports Act (FTRA), which requires virtual asset service providers (VASPs) to register and comply with AML regulations.

South Korea has sought to ensure market integrity compliance with the FATF.

Taiwan –Taiwan's Central Bank and Financial Supervisory Commission (FSC) have warned that cryptocurrencies are not currencies, but rather commodities and have no legal protection. The FSC has been empowered under the country's Money Laundering Control Act and Terrorism Financing Prevention Act to require users on trading platforms to register their "real names." The FSC implemented new money laundering regulations for the nation's cryptocurrency exchanges, requiring them to report transactions valued at more than NT$500,000 (US$17,770),

The FSC has required platform operators operating STO business to obtain a securities dealer's license and comply with the securities business prevention system Money Laundering and Anti-Terrorism (AML/CFT) regulations. Banks must report suspicious anonymous transactions. However, there are presently no regulations on crypto mining.

Thailand – The Securities and Exchange Commission (SEC) of Thailand regulates cryptocurrencies under an Emergency Decree on Digital Asset Businesses B.E. 2561 issued in 2018. Under the decree, digital asset businesses are required to apply for a license, monitor for unfair trading practices, and are considered "financial institutions" for AML purposes among others.

Gains on taxed as income and subject to a top tax bracket of 35%.

United Arab Emirates – The UAE has been forward-looking in crypto and blockchain. The Dubai Financial Services Authority (DFSA) included a crypto regulatory framework in its 2021 business plan for firms operating in the Dubai International Financial Center.

The UAE Securities and Commodities Authority issued its regulation in 2020, which seeks to provide clarity as to how crypto and other digital assets may be used as a stored value when purchasing various goods and services.

The Financial Services Regulatory Authority (FSRA) of Abu Dhabi Global Market (ADGM) has enhanced its "Guidance for the Regulation of Crypto Asset Activities"

The UAE and Saudi Arabia are reportedly working on research for a CBDC dubbed "Project Aber."

About the authors

SUSANNAH HAMMOND

Susannah Hammond is senior regulatory intelligence expert for Thomson Reuters with more than 25 years of wide-ranging compliance, regulatory and risk experience in international and UK financial services. She is co-author of "Conduct and Accountability in Financial Services: A Practical Guide" published by Bloomsbury Professional.

uk.linkedin.com/in/susannahhammond @SannaHamm

TODD EHRET

Todd Ehret is a Senior Regulatory Intelligence Expert for Thomson Reuters Regulatory Intelligence. He has more nearly 25 years' experience in the financial industry where he held key positions in trading, operations, accounting, audit, and compliance for broker-dealers, asset managers, private equity, and hedge funds. Before joining Thomson Reuters he served as a Chief Compliance Officer and Chief Operating Officer at a Registered Investment Adviser/Hedge Fund for nearly a decade.

us.linkedin.com/in/todd-ehret-91827264

Visit https://legal.thomsonreuters.com/en/products/regulatory-intelligence
Compliance Clarified – A Podcast by Thomson Reuters Regulatory Intelligence

Our intelligence working for you

About Thomson Reuters Regulatory Intelligence
Thomson Reuters Regulatory Intelligence is a market leading solution that empowers you to make well-informed decisions to confidently manage regulatory risk, while providing the tools to make proactive decisions and action change within your organization. It has been developed with a full understanding of your compliance needs – locally and globally, today and in the future.

Learn more: **legal.tr.com/regulatory-intelligence**

THOMSON REUTERS®