Special Report

Cryptos on the rise 2022

A complex regulatory future emerges

THOMSON REUTERS®

Contents

Introduction

Crypto-assets and the vast universe of associated products and services have grown rapidly in recent years and are becoming increasingly interlinked with the regulated financial system. Policymakers appear to be struggling to keep track of risks posed by a sector where most activities are unregulated, or at best lightly regulated.

Financial stability risks could soon become systemic in some countries, according to the International Monetary Fund (IMF).

> ***"Crypto-assets are potentially changing the international monetary and financial system in profound ways."***
>
> ***– IMF blog, December 2021.***

There is also concern that uncoordinated regulatory actions may facilitate potentially destabilizing capital flows. The IMF estimates cryptos' market capitalization at $2.5 trillion. This may be an indication of the significant economic value of the underlying technological innovations such as the blockchain, although it might also reflect froth in an environment of stretched valuations.

Cryptos' potential to transform the traditional financial system means the associated challenges are attracting considerable regulatory attention. The focus is twofold: cryptos' possible impact on financial stability and the need to protect vulnerable customers.

The principal challenge is the need for an internationally coherent policy approach, including definitions and jurisdictional perimeters, and in terms of exchanges, prevention of market manipulation and systemic risks. Lending and payment risks, banking, payments and anti-money laundering (AML) risks, tax policy and tax evasion risks, securities fraud and scams, together with cyber security, hacking and privacy risk will all need to be addressed.

> *"But perhaps the most fundamental question is this: in a system where so many new, previously non-financial, players are becoming instrumental in offering financial services, how are we, as financial supervisors, going to ensure that the financial system remains robust and consumers stay safe? How can we make sure that we continue to have the right mandate and effective instruments to ensure that outcome?"*
>
> ***– Steven Maijoor, executive director of supervision, Dutch Central Bank (De Nederlandsche Bank), February 2022.***

The increasing regulatory challenges are exacerbated by the growing public awareness, acceptance and use of cryptos. From the U.S. perspective, research published[1] in November 2021 by Pew Research, a nonpartisan think tank in Washington, reported 16% of respondents saying they personally have invested in, traded or otherwise used cryptocurrencies. Newsweek Magazine cited a survey in January 2022 by the crypto firm New York Digital Investment Group, estimating the total number of Americans who own cryptos at 46 million (about 14% of the population).

In the UK, in June 2021, the UK Financial Conduct Authority published its fourth consumer research publication on crypto-assets ownership[2] which found heightened public interest in, and media coverage of, cryptos, with 78% of adults now having heard of cryptocurrencies. Around 2.3 million now own crypto-assets, up from around 1.9 million in 2020.

The UK regulator also found attitudes have shifted, as cryptocurrencies appear to have become more normalized — fewer crypto users regard them as a gamble (38%, down from 47%) and more see them as an alternative or complement to mainstream investments, with half of crypto users saying they intend to invest more in the future.

In the European Union, as of February 2022, the total market capitalization of crypto-assets is reported[3] as having increased eightfold in the last two years to around 1.5 trillion euros now, although around 1 trillion euros below its peak in November 2021. The suggestion is that crypto-assets are beginning to gain mainstream acceptability, with ownership peaking at 6% of Slovakians and 8% of Dutch nationals reported as owning crypto-assets.

This report is a follow-up to Regulatory Intelligence's "Cryptos on Rise" special report[4] published in 2021. That report highlighted the need for policymakers, regulators and firms all to play their part in ensuring that cryptos are as "safe" as possible, not only in terms of investment risk but also with regards to regulatory certainty and cyber resilience.

The 2022 special report expands beyond cryptocurrencies such as bitcoin. Considering the need to develop a regulatory framework, it investigates other crypto-related instruments, such as central bank digital currencies (CBDCs), non-fungible tokens (NFTs) and stablecoins, and highlights policy work in key countries. It examines some of the misconceptions which persist about cryptos, as well as the ramifications for financial stability and the future of money. It also considers changing structural models for financial institutions emerging from the crypto world, as represented by decentralized autonomous organizations (DAOs).

As with the 2021 report there is a compendium which analyzes the tax, legal and regulatory status of cryptos in various jurisdictions.

1 https://www.pewresearch.org/fact-tank/2021/11/11/16-of-americans-say-they-have-ever-invested-in-traded-or-used-cryptocurrency/
2 https://www.fca.org.uk/publications/research/research-note-cryptoasset-consumer-research-2021
3 https://www.esma.europa.eu/sites/default/files/library/esma50-164-5533_keynote_speech_-_verena_ross_-_keeping_on_track_in_an_evolving_digital_world.pdf
4 https://www.thomsonreuters.com.sg/en/resources/cryptos-on-the-rise.html

Part One – Beyond Bitcoin

Central bank digital currencies

There are some structural similarities between crypto-assets and central bank digital currencies, but CBDCs are best described as the digital equivalent of a country's fiat currency. As a result, they are often seen as an alternative or competitor to cryptos. The most advanced CBDC thus far is China's digital yuan. During the 2022 Beijing Winter Olympic Games athletes, coaches and media made digital payments via smartphone apps, payment cards, or wristbands.

From the crypto regulatory landscape in the compendium of this report, it is apparent that many of the early movers on CBDCs also adopt restrictive stances or outright bans on other cryptos. Prime examples include China, Russia, Iran and Venezuela.

The G7 countries have been deliberately cautious about CBDCs' potential, particularly with regards to retail CBDCs used by the public. The G7 has reiterated that the decision on whether to launch a CBDC is for each country to make, and no G7 jurisdiction has yet done so. In a 2021 survey of central banks[5], the Bank for International Settlements (BIS) found that 86% are actively researching the potential for CBDCs, 60% are experimenting with the technology and 14% are deploying pilot projects.

> *"A CBDC would preserve the coexistence of sovereign and private money in a digital world. This is not an abstract benefit — it is the basis for financial and monetary stability, ensuring competition and efficiency in payment markets. But a CBDC could generate even more benefits for users.*
>
> *It could improve the confidentiality of digital payments. The information contained in electronic transactions can be monetized by private companies, posing a threat to privacy. This risk is further compounded by Big Techs starting to offer financial services and by the rapid development of artificial intelligence. Data protection regulation aims to prevent misuse, but cannot always keep pace with technological innovation, as we have seen in past cases of data breaches and misuse by tech companies."*
>
> ***– Fabio Panetta, member of the executive board of the European Central Bank (ECB), to a panel discussion on CBDCs at the U.S. Monetary Policy Forum, February 2022.***

5 https://www.bis.org/about/bisih/topics/cbdc.htm

Retail CBDC

A retail CBDC would be a digital form of central bank money, denominated in the national unit of account, distinct from electronic reserves (which cannot be accessed by individuals) and physical cash. As a direct liability of the central bank, CBDCs would also be distinct from commercial bank money. If issued, CBDCs, as a form of central bank money, could act as both a liquid, safe settlement asset and as an anchor for the payments system.

Not crypto-assets

The G7 is clear that CBDCs are not crypto-assets. Crypto-assets are not issued by a central bank, can be highly volatile, and are not widely used for payments. CBDCs are fundamentally different from privately issued digital currencies such as stablecoins, which are a liability of private entities that seek to maintain stability in their price (typically in relation to stable assets such as fiat currency). CBDCs can be considered in two parts:

- the CBDC itself, an instrument issued by the central bank that can be transferred as a means of payment or held as a store of value; and
- the wider "ecosystem" in which a CBDC operates, including the supporting infrastructure that allows CBDC balances to be managed and payments made.

This wider infrastructure could involve both public and private participants (such as banks, digital wallet providers or other payment entities).

Public policy principles

In October 2021 the G7 published[6] a set of 13 public policy principles for possible future retail CBDCs. Principles 1-8 cover foundational issues and principles 9-13 cover the opportunities. The "foundational issues" are those that any CBDC must demonstrate if it is to command the confidence and trust of users. These include the preservation of monetary and financial stability, the protection of users' privacy, strong standards of operational and cyber resilience, the avoidance of financial crime and sanctions evasion, and environmental sustainability.

The G7 principles also highlight the potential for CBDCs to support safe and efficient transactions. They make it a political priority to harness opportunities and address the monetary and financial stability risks, as well as ensure trust in the financial system. The G7 notes that CBDCs could also advance public policy goals, including digital-economy innovation, financial inclusion and reducing frictions in cross-border payments.

6 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1025235/G7_Public_Policy_Principles_for_Retail_CBDC_FINAL.pdf

A divided UK stance

The UK's stance on CBDC is at best unproven and at worst divided. In January 2022, the parliamentary Economic Affairs Committee published a report which concluded that there is no convincing case for UK to have a CBDC. The committee found that while a CBDC may provide some advantages, it could present significant challenges for financial stability and the protection of privacy.

The committee report[7] builds on a November 2021 joint statement[8] by the Bank of England and HM Treasury, which announced the next steps on the exploration of a UK CBDC. Specifically, the Bank and HM Treasury intend to launch a consultation in 2022 which will set out their assessment of the case for a UK CBDC. The consultation will form part of a "research and exploration" phase and will seek to inform policy development in the next few years.

The committee report adds several challenges and questions to the proposed consultation and evaluation process. The report's findings, however, make it clear that the UK has some way to go before the case has been made for a UK retail CBDC. It also recommends that the UK government and Bank of England take action to shape international standards which suit the UK's values and interests, particularly with regards to privacy, security and operational standards.

> *"The introduction of a UK central bank digital currency would have far-reaching consequences for households, businesses, and the monetary system. We found the potential benefits of a digital pound, as set out by the Bank of England, to be overstated or achievable through less risky alternatives.*
>
> *We took evidence from a variety of witnesses and none of them were able to give us a compelling reason for why the UK needed a central bank digital currency. The concept seems to present a lot of risk for very little reward. We concluded that the idea was a solution in search of a problem."*
>
> ***– Lord Forsyth of Drumlean, chair of the House of Lords Economic Affairs Committee, January 2022.***

The U.S. approach to CBDCs

The potential for a CBDC in the United States took a step forward in February when the findings of a project by the Federal Reserve Bank of Boston and the Massachusetts Institute of Technology (MIT) were released. The project, dubbed "Project Hamilton," achieved its preliminary goals of using emerging technology to deliver, in theory, high-speed transactions within a resilient infrastructure.

7 https://publications.parliament.uk/pa/ld5802/ldselect/ldeconaf/131/131.pdf
8 https://www.bankofengland.co.uk/news/2021/november/statement-on-central-bank-digital-currency-next-steps

Separately, the Federal Reserve Board in January opened debate[9] on the merits of a CBDC. The "white paper" said creating an official digital version of the U.S. dollar could give Americans more, and speedier, payment options, but it would also present financial stability risks and privacy concerns. The paper, however, made no policy recommendations and offered no clear signal about where the Fed stands on whether to launch a CBDC.

The Federal Reserve's Board said it would not proceed with creating a CBDC "without clear support from the executive branch and from Congress, ideally in the form of a specific authorizing law."

Leaders of the Boston Fed/MIT project said the next phase will explore alternative designs and look more closely at other issues such as security and programmability. They will also look at ways to balance privacy issues with concerns about compliance.

"There are still many remaining challenges in determining whether or how to adopt a central bank payment system for the United States," said Neha Narula, director of MIT's Digital Currency Initiative.

In March 2022, the White House issued an Executive Order requiring the government to ensure the responsible development of digital assets and to assess the risks and benefits associated with of creating a central bank digital dollar.

> *"A United States CBDC may have the potential to support efficient and low-cost transactions, particularly for cross-border funds transfers and payments, and to foster greater access to the financial system, with fewer of the risks posed by private sector-administered digital assets. A United States CBDC that is interoperable with CBDCs issued by other monetary authorities could facilitate faster and lower-cost cross-border payments and potentially boost economic growth, support the continued centrality of the United States within the international financial system, and help to protect the unique role that the dollar plays in global finance. There are also, however, potential risks and downsides to consider. We should prioritize timely assessments of potential benefits and risks under various designs to ensure that the United States remains a leader in the international financial system."*
>
> ***– White House Executive Order on Ensuring Responsible Development of Digital Assets, March 2022***

9 https://www.reuters.com/business/fed-lays-out-risks-benefits-cbdc-paper-takes-no-policy-stance-2022-01-20/

Stablecoins

A stablecoin is any cryptocurrency designed to have a stable price, typically through being reserved, backed, or pegged to an underlying asset such as a commodity or currency, or through algorithmic mechanisms to its reference asset. The potential use cases for stablecoins are far-reaching and potentially disruptive to the established banking and payments industries.

Regulators are developing their approach to stablecoins. In October 2021, the international Financial Stability Board (FSB) published[10] a progress report on the implementation of the high-level recommendations with regards to the regulation, supervision and oversight of global stablecoin (GSC) arrangements.

The progress report concluded that "cross-border cooperation and coordination" were the highest regulatory priorities, followed by further work regarding when a so-called stablecoin may be appropriately identified as a GSC.

Hong Kong

Individual jurisdictions are developing their own approaches to stablecoins. The Hong Kong Monetary Authority (HKMA) published a discussion paper[11] on crypto-assets and stablecoins inviting views from the industry and public on the relevant regulatory approach.

The paper, which closed for comments at the end of March 2022, sets out the HKMA's thinking on the regulatory approach for crypto-assets, particularly payment-related stablecoins. The HKMA has considered, among other things, the international recommendations, the market and regulatory landscape locally and in other major jurisdictions, and the characteristics of payment-related stablecoins.

The paper considers five policy options across the entire spectrum, from "no action" to a "blanket ban."

United States

Stablecoins are a likely early crypto priority for U.S. regulators. In November 2021, the President's Working Group on Financial Markets, a government-industry body, released a report on stablecoins[12] that urged Congress to pass new legislation to "fill regulatory gaps."

In the meantime, U.S. market regulators are prepared to play a leading role in stablecoin oversight, Gary Gensler, the chair of the Securities and Exchange Commission (SEC), said in announcing the working group's report.

10 https://www.fsb.org/wp-content/uploads/P071021.pdf
11 https://www.hkma.gov.hk/media/eng/doc/key-information/press-release/2022/20220112e3a1.pdf
12 https://www.sec.gov/news/statement/gensler-statement-presidents-working-group-report-stablecoins-110121

Similarly, the federal Financial Stability Oversight Council, chaired by Janet Yellen, Treasury secretary, noted in its annual report[13] in December 2021 that it "will further assess and monitor the potential risks of stablecoins and recommends that its members consider appropriate actions within each member's jurisdiction to address those risks while continuing to coordinate and collaborate on issues of common interest."

Gensler cited similarities between stablecoins and stable value funds and said the SEC and the Commodity Futures Trading Commission (CFTC) "will deploy the full protections of the federal securities laws and the Commodity Exchange Act to these products and arrangements, where applicable."

> ***"will further assess and monitor the potential risks of stablecoins and recommends that its members consider appropriate actions within each member's jurisdiction to address those risks while continuing to coordinate and collaborate on issues of common interest."***
>
> ***– U.S. Financial Stability Oversight Council, December 2021***

The SEC and CFTC are also likely to play an integral role in the oversight of crypto trading platforms or exchanges. Market structure, potential market manipulation, scams and investment and trading activities will be priorities.

Concerns about investor protection have already been voiced by several prominent members of Congress. The SEC and CFTC will also oversee investor protection and overall policing and enforcement, with input from the Consumer Financial Protection Bureau (CFPB).

Some use cases for stablecoins will "trigger obligations under federal consumer financial protection laws, including the prohibition on unfair, deceptive, or abusive acts or practices," said Rohit Chopra, chair of the CFPB.

The CFPB has launched a review of stablecoins' potential to cause harm in three main areas: concentrated market power, systemic risk and consumer abuse.

The banking regulators will play a role in regulating stablecoins because of their potential uses in payments, borrowing, lending and deposit-like functions.

Singapore

The Monetary Authority of Singapore (MAS) has repeatedly cautioned that investing in cryptocurrencies is risky, and unsuitable for retail investors. Cryptocurrency funds are not authorized for sale to retail investors in Singapore.

In December 2019, MAS issued a public consultation seeking views on the interactions between money, e-money and cryptocurrencies, including stablecoins, and the appropriate regulatory treatment for cryptocurrencies, particularly stablecoins.

13 https://home.treasury.gov/system/files/261/FSOC2021AnnualReport.pdf

The consultation sought views on the defining characteristics of e-money and cryptocurrency, considered the potential ability of stablecoins to function as money, and discussed its relevance in the regulatory class of e-money or cryptocurrency.

The differing regulatory priorities for e-money and cryptocurrency services have different implications for how stablecoins would be regulated if placed in either of these categories.

E-money services are regulated for the safeguarding of customers' money, whereas cryptocurrency services are regulated for AML risk, with a disclosure requirement to warn customers of the risk of loss. Other issues were also touched on, such as whether a global stablecoin should be regulated differently from other stablecoins and how the stabilization mechanism should be regulated.

The consultation received mixed views over whether a stablecoin was a single-currency or multi-currency stablecoin and whether there was a claim on the issuer of the stablecoin. There were also varying views regarding whether stablecoins should be treated as a payment instrument or an investment product, depending on the assets backing the stablecoins.

MAS intends to continue its work on reviewing the appropriate regulatory treatment for stablecoins, such as the treatment under different legislation, taking into consideration its practical use and risks, and informed by the continuing work of the international standard-setting bodies.

> *"... another important development is stablecoins. The use of private stablecoins is still limited, partly because of their risks to users. But stablecoins also have features that could make them attractive, for example, in countries with weaker institutions and unstable national currencies, and for cross-border payments. As soon as the conditions are right, things could go very fast. Based on the experience with dollarization in developing countries, we know there is a tipping point beyond which adoption of a new currency increases exponentially. Without regulation, such a steep rise in the use of private stablecoins could pose a threat to financial stability."*
>
> ***– Steven Maijoor, executive director of supervision, Dutch Central Bank (De Nederlandsche Bank), February 2022***

Non-fungible tokens

A non-fungible token (NFT) is a unique digital code stored on a blockchain, a form of distributed or digital ledger. Non-fungible tokens represent rights to the particular asset. The term "non-fungible" distinguishes NFTs from other digital assets that are fungible or interchangeable, such as bitcoin.

The use cases for NFTs are far-reaching as they provide an ability to authenticate virtually anything where there is a need to establish authenticity and ownership. Their popularity thus far has centred on the art and collectibles world — NFTs representing works of art, collectibles, video clips, or other digital media have exploded in price and popularity — but other potential uses include real-estate and auto titles, coupons, transit, or event tickets.

NFTs representing works of art, collectibles, video clips, or other digital media have exploded in price and popularity

NFT and blockchain technology can also be useful in logistics and supply-chain applications, where metadata and timestamps can authenticate and help track the origins and journeys of commodities.

Critics may see the NFT market as yet another speculative bubble, but proponents point to broader applications in other industrial, legal and commercial uses that could be transformative.

The popularity of NFTs has raised concerns that the marketplace could be fertile ground for illicit activities such as scams, cybercrime, price manipulation, or money laundering. Indeed, many are baffled as to why so much money is spent on items that do not physically exist.

NFTs have been noticeably absent from the regulatory policy debate so far. How far financial regulators ultimately attempt to expand the perimeters of their authority — potentially into this new digital art and collectibles world, or even beyond into commercial applications — remains to be seen.

With such broad technological utility and complexity, regulation will be complex and likely to be challenged in courts. It appears obvious that AML requirements should apply in some areas. Another question is whether an NFT is deemed a financial instrument or security. Many legal experts already agree that if an NFT is fractionalized, thus representing partial ownership, or has royalty streams of income associated with it, it will likely be deemed a security and thus subject to regulatory oversight.

European Union

In September 2021, the European Union introduced a proposal to regulate crypto-assets. The Markets in Crypto-Assets Regulation (MiCA), if adopted, will regulate all issuers and service providers dealing with crypto-assets.

NFTs were explicitly excluded from MICA's scope. Article 4 (2) of the draft provides that issuers of "crypto-assets that are unique and non-fungible" do not need to publish or register a white paper for them. MICA does state, however, that fractional NFTs should not be considered unique and would therefore be subject to MiCA.

United States

The United States has yet to issue direct guidance on NFTs as their use cases and potential value remain to be clarified. The structure of NFTs and the intellectual property rights, such as rights to use, copy and display, and whether revenue streams are associated, are just some of the legal uncertainties.

There is no direct state regulatory framework or guidance on NFTs, but several states, including New York and Louisiana, which do have virtual currency regulations could attempt to hold NFTs under their purview.

A spokesperson for the NYSE said, however, that it has no immediate plans to launch cryptocurrency or NFT trading.

The U.S. Treasury's anti-money laundering arm has yet to issue guidance specific to NFTs but has published general guidance related to how the Bank Secrecy Act and related regulations relate to virtual currencies that might apply to NFTs.

Established financial services firms and venues are getting into NFTs. In February 2022, the New York Stock Exchange filed an application to register the term "NYSE" for a marketplace for NFTs, appearing to take a step closer to setting up an online trading place for cryptocurrencies and NFTs.

If the NYSE launches a new marketplace, it will compete with SuperRare, Rarible and NFT marketplace OpenSea, which was valued at $13.3 billion after its latest private funding round.

A spokesperson for the NYSE said, however, that it has no immediate plans to launch cryptocurrency or NFT trading.

The NYSE minted its first set of NFTs in April 2021 commemorating the first trades of six "notable" listings.

Hong Kong

Investors in Hong Kong have shown considerable interest in NFTs. Projects have been launched at a steady pace, attracting enthusiastic bidders. Bricks and mortar marketplaces such as Sotheby's and Christie's have auctioned NFTs to buyers in Hong Kong, either as standalone items or as add-ons to luxury items such as watches, as well as facilitating bidding for locally produced NFT art.

NFT activity in Hong Kong has been further buoyed by regulatory uncertainty in mainland China. Financial authorities there have yet to clarify whether a recently implemented ban on all cryptocurrency transactions includes producing, selling or trading NFTs. As a result, some Chinese digital art and entertainment creators have turned to Hong Kong to issue NFTs.

The Securities and Futures Commission (SFC) has stated that virtual assets fall within the legal definition of securities or derivatives and are therefore subject to local securities laws. Cryptocurrency trading platforms such as Binance have withdrawn from Hong Kong after receiving written warnings from the SFC. The regulator's move to assert jurisdiction over platforms suggests that it firmly considers virtual assets, such as cryptocurrencies and tokens that function as securities, to fall within its jurisdiction.

The natural next question is whether financial regulators will also consider NFTs as a class of virtual assets that fall within their jurisdiction. They have yet to issue regulations specifically concerning NFTs, although recent legislative developments in Hong Kong have tended to apply certain regulatory requirements, such as anti-money laundering and counter-terrorist financing rules, to all classes of virtual assets.

Part Two – Oversight in a crypto world

Financial stability and regulatory challenges

The identification, monitoring and management of risks continue to concern and on occasion confound regulators and firms alike. The challenges include operational and financial integrity risks from crypto-asset exchanges and wallets, investor protection, and inadequate reserves and inaccurate disclosure for some stablecoins. Moreover, in emerging markets and developing economies, the advent of crypto can accelerate what the IMF has badged "cryptoization"— when these assets replace domestic currency and circumvent exchange restrictions and capital account management measures.

Financial stability

The FSB raised[14] potentially serious concerns about financial stability in a recent paper. Given the international and diverse nature of the crypto-asset markets, it has advocated that regulatory authorities prioritize cross-border and cross-sectoral cooperation. Financial stability risks could escalate rapidly, and the FSB is clear that a "timely and pre-emptive evaluation of possible policy responses" is required.

The need for policymaking pre-emption and cooperation is seen as increasingly urgent as, while crypto-assets account for only a small portion of overall financial system assets, they are growing rapidly. Direct connections between crypto-assets and systemically important financial institutions and core financial markets are rapidly evolving, opening the door to the potential for regulatory gaps, fragmentation or arbitrage.

A lack of consistency

The cross-sector, cross-border nature of cryptos limits the effectiveness of national approaches. Countries are adopting different strategies, and existing regulations may not allow for national approaches that comprehensively cover all elements of these assets. Importantly, many crypto service providers operate across borders, making the task for supervision and enforcement even more difficult.

14 https://www.fsb.org/wp-content/uploads/P160222.pdf

> *"If we can harness the benefits of digital technology, we may hope to see a more democratized, even more inclusive, financial sector. But there are serious risks that investors will be subject to misinformation, and that the lines between regulated and unregulated products become blurred."*
>
> ***– Verena Ross, chair of the European Securities and Markets Authority, February 2022***

A particular challenge is a lack of consistency between, or absence of, definitions related to new technology applications. There are also legal and jurisdictional questions to be resolved. As an example, the U.S. CFTC and the courts have established that bitcoin is a commodity. The banking regulators see cryptos as a form of payment subject to their purview. The SEC, as the lead U.S. financial services regulator, however, sees things differently.

U.S. Executive Order and SEC take steps toward crypto regulation

In March 2022, the White House issued an Executive Order which emphasized the importance of digital assets and the need for coordination and cooperation between government departments, agencies and regulators. The Order said, "We must reinforce United States leadership in the global financial system and in technological and economic competitiveness, including through the responsible development of payment innovations and digital assets."

The Order took a holistic approach to addressing risks and harnessing the potential benefits of digital assets. It emphasized six key priorities: consumer and investor protection, financial stability; illicit finance; U.S. leadership in the global financial system and economic competitiveness; financial inclusion; and responsible innovation.

New proposed rules from the SEC related to alternative trading systems (ATSs) have raised speculation in the crypto industry that the regulatory expansion could include blockchain and cryptocurrency platforms.

The proposal does not specifically reference cryptocurrencies or blockchain. However, a reference to "communication protocol systems" could apply to trading venues of all types, such as unregulated platforms according to several attorneys.

The rule proposal[15] announced in January 2022 may have come as a surprise to the crypto and blockchain industries, some elements of which perceived it as an early shot in what will be a long and complex regulatory battle.

Alternative trading systems are SEC-regulated electronic trading systems that match orders for buyers and sellers of securities. Trading in U.S. government securities on such platforms

15 https://www.sec.gov/rules/proposed/2022/34-94062.pdf

has grown significantly in recent years. The level of regulatory oversight and investor transparency at these venues has not matched similar platforms for corporate bonds or equity securities.

The proposed rules are intended to protect investors and enhance cybersecurity in ATSs that trade U.S. Treasury securities. They expand on a similar 2020 proposal under Jay Clayton, former SEC chair.

"It modernizes the rules related to the definition of an exchange to cover platforms for all kinds of asset classes that bring together buyers and sellers," Gensler said, alluding to the expansiveness of the proposal.

"It modernizes the rules related to the definition of an exchange to cover platforms for all kinds of asset classes that bring together buyers and sellers," Gensler said, alluding to the expansiveness of the proposal.

– Gary Gensler, Chair U.S. SEC

The 650-page document raised about a dozen significant issues, according to Hester Peirce, an SEC commissioner. Peirce cited[16] a reach to "currently unregulated communication protocol systems" and noted that the proposal "goes well beyond government securities, or even fixed-income securities; key parts of the proposal affect trading venues that make any type of security available for trading."

Critics have said the proposal could include wallets, block explorers that allow users to call smart contracts, and other market participants including virtually every blockchain-based application. The proposal considers definitions such as "orders" "trading interests," and "communication protocol systems" in place of "exchanges."

Crypto advertsing

Supervisory approaches to the advertising of cryptos to retail investors vary considerably among jurisdictions.

UK

In February 2022, the UK FCA updated its prohibition[17] on the retail marketing, distribution and sale of crypto-asset derivatives and crypto-asset exchange-traded notes. The UK is also consulting on further potential restrictions.

United States

Crypto advertising in the United States is big business. When celebrity Kim Kardashian was paid to ask her 250 million Instagram followers to speculate on crypto tokens by "joining the Ethereum Max Community," she disclosed that her post was an advertisement. She did not, however, have to disclose that Ethereum Max — not to be confused with the cryptocurrency

16 https://www.sec.gov/news/statement/peirce-ats-20220126
17 https://www.handbook.fca.org.uk/handbook/COBS/22/6.pdf

ethereum — was a speculative digital token created a month before, one of hundreds of such tokens that fill the crypto-exchanges.

On television, meanwhile, potential retail investors in cryptos can watch movie stars pitch them in prime-time slots during major sporting events. Sporting venues have been re-named after crypto trading platforms, most notably Crypto.com, which paid $700 million for the naming rights of the Staples Center, home of the NBA's Los Angeles Lakers, for a 20-year term. During the 2022 Super Bowl, four cryptocurrency commercials aired. A one-minute advertisement costing nearly $14 million, which featured nothing more than a floating QR code, drove more than 20 million hits to Coinbase's landing page within one minute, according to Bitcoin Magazine.

Regulators in the United States have thus far focused their attention and enforcement efforts on unregistered securities offerings, and fraudulent scams. However, with investor protection and risk disclosures as core tenets, stricter advertising regulations surrounding cryptos are likely inevitable.

Spain

The Spanish securities regulator (CNMV) said in January that would begin to regulate rampant advertising of crypto-assets, including by social media influencers, to ensure investors are aware of risks. New regulations[18] set out requirements for the content and format of promotional messages for crypto-asset campaigns.

Advertisers and companies that market crypto-assets will have to inform the CNMV at least 10 days in advance about the content of campaigns targeting more than 100,000 people.

In November 2021, the CNMV scolded soccer star Andres Iniesta after he promoted the cryptocurrency exchange platform Binance on his Twitter and Instagram accounts, telling him that he should be thoroughly informed about cryptocurrencies before making any investment in them or recommending others to do so.

Singapore

The Monetary Authority of Singapore in January published guidelines[19] "discouraging" cryptocurrency trading by the general public and giving effect to MAS' expectations that cryptocurrency service providers should not promote their services to the general public in Singapore.

Russia

Also in January 2022, Russia's central bank proposed to ban the use and mining of cryptocurrencies on Russian territory, citing threats to financial stability, citizens' wellbeing

18 https://cnmv.es/DocPortal/Legislacion/Circulares/Circular_1_2022_EN.pdf

19 https://www.mas.gov.sg/-/media/MAS-Media-Library/regulation/guidelines/PSO/ps-g02-guidelines-on-provision-of-digital-payment-token-services-to-the-public/Guidelines-on-Provision-of-Digital-Payment-Token-Services-to-the-Public-PS-G02.pdf

and its monetary policy sovereignty. Russia has argued for years against cryptocurrencies, saying they could be used in money laundering or to finance terrorism. It eventually gave them legal status in 2020 but banned their use as a means of payment.

The Russian central bank stated that speculative demand primarily determined cryptocurrencies' rapid growth and that they carried characteristics of a financial pyramid, warning of potential bubbles in the market, threatening financial stability and citizens. The bank has proposed to prevent financial institutions from carrying out any operations with cryptocurrencies and said mechanisms should be developed to block transactions aimed at buying or selling cryptocurrencies for fiat currencies. The proposed ban would include crypto exchanges.

> The DFSA advises consumers and potential investors to exercise caution and undertake due diligence to understand the risks involved when buying crypto-assets. Risks include:
>
> - **Fraud** — Criminals often use crypto-assets and new technology to perpetrate fraudulent schemes by misleading customers as to the nature of the product on offer and "take the money and run" shortly after the token is issued. Also, fraudsters may entice customers by touting crypto-assets as an investment or an "opportunity" to get into a cutting-edge space without any real benefit behind the offer.
> - **Volatility** — Crypto-asset valuation and pricing can be difficult because of volatility and lack of real underlying assets, and holders may suffer significant losses if the price of the crypto-asset drops quickly.
> - **Liquidity** – Illiquid or flat market structures can make it hard to sell or trade crypto-assets. It may also be difficult to exit the market and "cash out."
> - **Information** — Information may be missing, inaccurate, incomplete and unclear with respect to the project and associated risks. Documents may be technical and require additional knowledge to understand the characteristics of the crypto-assets and what the holder is (not) getting.
> - **Money laundering** — Crypto-asset platforms commonly rely on complex infrastructures using several entities (spanning across jurisdictions) to transfer funds and/or execute payments. This can mean that AML/CTF compliance, supervision and enforcement may not be effective.
>
> Consumers should exercise caution when dealing with crypto-asset entities, unless they are sure that the entities are properly regulated, to be protected against financial misconduct or wrongdoing."
>
> ***– Extract from Dubai Financial Services Authority statement on crypto-assets, November 2021.***

Trust

Trust is a particular challenge with regards to the increasingly widespread use of cryptos, especially as cryptos are seen to be eroding or replacing existing monetary norms such as fiat currency.

Policymakers are beginning to consider the possible economic and regulatory ramifications of the adoption of digital currencies, together with the potential impact on the international monetary system.

> *"My main message today is simple: the soul of money belongs neither to a Big Tech nor to an anonymous ledger. The soul of money is trust. So, the question becomes: which institution is best-placed to generate trust? I will argue that central banks have been and continue to be the institutions best-placed to provide trust in the digital age. This is also the best way to ensure an efficient and inclusive financial system to the benefit of all."*
>
> ***– Agustín Carstens, general manager of the Bank for International Settlements, January 2022.***

Trust is primarily needed to maintain the societal conventions regarding the use of money. Part of that convention is that central banks provide, and critically are seen to provide, an open, neutral, trusted and stable platform. Private companies use their ingenuity and dynamism to develop new payment methods and financial products and services. This combination has been a powerful driver of innovation and welfare. The successful symbiosis cannot be taken for granted, however, and some recent developments may threaten money's essence as a public good, if taken too far.

In a speech[20] entitled "Digital currencies and the soul of money," Agustín Carstens, general manager of the Bank for International Settlements, offers three plausible scenarios for the future of money:

1. Big Tech stablecoins compete with national currencies and also against each other, fragmenting the monetary system.
2. The elusive promise of crypto and decentralized finance, or "DeFi," which claims to offer a financial system free from powerful intermediaries but may deliver something very different.
3. The realization of the vision of an open monetary and financial system that harnesses technology for the benefit of all.

20 https://www.bis.org/speeches/sp220118.htm

Carstens is an advocate of the third scenario, with an ideal of incumbent financial institutions, Big Techs and new innovative entrants all competing in an open marketplace that guarantees interoperability, building on central bank public goods. This is also the goal of the BIS Innovation Hub[21].

Gatekeeping the gatekeepers — big tech and banking licenses

The growing interconnectedness between the traditional financial system and cryptos is demonstrated by the potential for, and the implications of, Big Tech firms and other digital asset firms taking stakes in or owning banks and financial services companies.

In January 2022, a paper by the Bank for International Settlements' Financial Stability Institute assessed[22] the benefits and risks of extending banking licenses to Big Techs and fintechs. The findings are based on publicly available licensing requirements in seven jurisdictions covering Asia, Europe and North America.

The paper compares the merits of bank ownership by tech firms in relation to ownership by commercial or industrial non-financial companies (NFCs).

> ***The perceived benefits of allowing tech firms to operate with a banking license are "compelling but require scrutiny."***
>
> ***– January 2022, Bank for International Settlements' Financial Stability Institute***

The perceived benefits of allowing tech firms to operate with a banking license are "compelling but require scrutiny," the paper says. Unburdened by legacy infrastructure, tech firms can offer superior technology and user-friendly apps that may allow them to reach more consumers and perform various aspects of the banking business (onboarding, deposit-taking, lending, payments) more efficiently than incumbents, including commercial or industrial NFCs that may own banks.

Collectively, their technology-centric approach to the delivery of financial services is expected to advance some authorities' broader goals of fostering financial inclusion, promoting competition and delivering better outcomes for society. Nevertheless, as part of the authorization process — and subsequently through continuing supervision — authorities need to examine the ability and willingness of tech firms to deliver on their stated objectives.

A particular policy concern is whether the risks of allowing tech firms to own banks can be offset through licensing requirements without undermining the potential benefits they bring to consumers. Policy responses may differ across countries, but they are likely to be guided by three main considerations: the policy priorities of each jurisdiction; the inherent risks posed across and within each group of tech firms; and the applicability of the existing licensing regime in addressing the risks of tech-owned banks.

21 https://www.bis.org/about/bisih/about.htm
22 https://www.bis.org/fsi/publ/insights39.pdf

Warning from history

The UK has a stark warning for policymakers regarding the risks associated with non-financial services owners or controllers of banks, in a report on the Co-operative Bank's failure in 2013. The report[23] by Sir Christopher Kelly, which considered the events leading to the Co-operative Bank's capital shortfall, highlights lessons relevant to the policy debate on tech firms owning or controlling banks or other financial services firms.

It found that mistakes had not stemmed from regulatory grey areas or misinterpretations of risk, regulation or compliance. Rather, the Co-operative Group's board lacked the skills, knowledge or understanding required to manage a bank. It did not know what management information to expect, did not understand the role of the regulator and fundamentally did not understand banking.

The potential relevance to, say, a Big Tech owning a bank is clear. In the words of Kelly, "one of the most surprising features of this whole episode is that the board seemed unaware of its limitations."

Policymakers will need to ensure there is credible deterrence inherent in the approach to tech firm bank ownership and specifically that any senior manager who is unaware of or ignores their regulatory responsibilities will be vulnerable to investigation and sanction.

The potential relevance to, say, a Big Tech owning a bank is clear. In the words of Kelly, "one of the most surprising features of this whole episode is that the board seemed unaware of its limitations."

– Sir Christopher Kelly, Report of the independent review into the events leading to the Co-operative Bank's capital shortfall, April, 2014

23 https://assets.ctfassets.net/5ywmq66472jr/3LpckmtCnuWiuuuEM2qAsw/9bc99b1cd941261bca5d674724873deb/kelly-review.pdf

Decentralized autonomous organizations

The blockchain-based economy has spawned a new structure of financial institution called the "digital autonomous organization." This type of organization, based on computerized "smart contracts" recorded on a blockchain, raises significant issues regarding governance and accountability.

Decentralized autonomous organizations

The emergence of decentralized autonomous organizations (DAOs) represents a revolutionary change in the ways people and businesses can organize. DAOs leverage blockchain technology and are decentralized models of control and governance. They are characterized by transparency, clarity of rule, and process-driven decisions, primarily using smart contracts on distributed ledgers. Once a DAO has been established, via a blockchain, participants take ownership of its token, which allows them to participate in the system. Token holders can propose changes, and can vote on those changes, with the subsequent actions being taken "leaderlessly." There are no chief executives, chief financial officers or chief technical officers, only code and community.

Close to 5,000 DAOs have been formed to date, and this is expected to grow exponentially. Many involve pooling digital money together to purchase assets, both physical and digital. ConstitutionDAO was established seven days prior to the auctioning of one of the 11 remaining copies of the U.S. Constitution. The intent was to purchase and house it at a protected public location. Participants in the DAO contributed money in ETH (Ethereum token), raising $45 million. Separately, the AssangeDAO raised $53 million for the criminal defense of Julian Assange. These are just two examples of how quickly DAOs can be created, and of how powerful they can be.

Central to a DAO is transparency. Anyone can see which individual (wallet address) owns tokens. Tokens allow for people to vote on proposals. Anyone can create a proposal. Simply stated, and in an ideal setting, it is egalitarian. One challenge to the model, however, is its democratic nature which can make DAOs overly deliberate and result in a slower process compared with more traditional organizations.

The regulatory landscape for DAOs is nearly non-existent at the state level. Wyoming, which has led the United States on regulation for blockchain and cryptocurrency, recently codified rules for DAOs residing in the state. A DAO could, therefore, be created under the laws of the State of Wyoming. No other state enables this yet. Further, there is a movement afoot for corporations in the cryptocurrency sector to dissolve and become DAOs. With potentially hawkish regulation on the horizon for cryptocurrency, DAOs, by their very nature, are code-based, self-running, leaderless entities running via a decentralized network, which permits actions based on how users interact under brassbound, predefined rules. Theoretically, under the current regulatory landscape there is nothing the law can do about such an entity. A corporation converted to a DAO would no longer be in control of the platform, which reverts to a completely new decentralized model, unlike anything regulated currently.

The SEC is reportedly looking into true DAOs such as Uniswap, which operates in the decentralized finance (DeFi) sector as a decentralized exchange (DEX) and is a code-based organization that matches buyers and sellers of cryptocurrency. One area of focus is lending pools, where users will provide their assets for other users to trade, which produces healthy yields, just as banks provide interest on assets. This may fall into the Howey Test investment contract realm.

Governments' and regulators' understanding of DAOs is embryonic, but this area is bursting with potential, and there is a real need for a regulatory framework.

– Joe Raczynski, technologist and futurist, manager of technical client management at Thomson Reuters.

Financial crime

One could be forgiven for thinking that participants in crypto markets are the "cool kids" who are taking exciting investment risks in a brave new financial world. On the other side of the coin, regulators are increasingly concerned about the risks to vulnerable customers.

Financial crime

There is also concern that crypto firms can, and are, being used as conduits for facilitating financial crime. Many such firms, if not most, are outside the regulatory perimeter and have often found stepping into the regulated world challenging. One example of this is Binance, which has suffered multiple setbacks in its attempts to become regulated in several jurisdictions.

> *"The FCA currently has a limited role in registering UK-based crypto-asset exchanges for anti-money laundering purposes. Exchanges can be used to launder the proceeds of crime and we must contribute to the global effort to address financial crime by demanding that businesses with a UK presence meet the necessary standards. While some of the business which have applied to us have shown evidence of adequate systems and controls, many others fell well short of acceptable standards, and many have withdrawn their applications as we have scrutinized them. The state of those firms ignoring the requirement to register with us or which have moved off-shore to avoid registration could be even worse."*
>
> ***– Charles Randell, chair of the UK Financial Conduct Authority and the Payment Services Regulator, September 2021***

New research shows that decentralized finance (DeFi) protocols in particular are becoming an increasingly significant route for money launderers. The January 2022 update[24] from data provider Chainalysis reported that $8.6 billion worth of cryptocurrency was laundered in 2021 — a figure that has fluctuated from $6.6 billion in 2020 to $10.9 billion in 2019.

The 2021 figure represents a 30% increase in money laundering activity compared with 2020, although, as the update points out, "such an increase is unsurprising given the significant growth of both legitimate and illicit cryptocurrency activity in 2021." Chainalysis also notes that the numbers only account for funds derived from "cryptocurrency-native" crime. This refers to cyber-criminal activity such as darknet market sales or ransomware attacks in which profits are virtually always derived in cryptocurrency rather than fiat currency. It is more difficult to measure how much fiat currency derived from offline crime — traditional drug trafficking, for example — is converted into cryptocurrency to be laundered.

24 https://blog.chainalysis.com/reports/2022-crypto-crime-report-preview-cryptocurrency-money-laundering/

The U.S. Department of Justice (DOJ) announced recently that it had seized a record $3.6 billion in bitcoin tied to the 2016 hack of digital currency exchange Bitfinex and had arrested a husband-and-wife team on money laundering charges.

The couple allegedly conspired to launder 119,754 bitcoin stolen after a hacker broke into Bitfinex and initiated more than 2,000 unauthorized transactions. DOJ officials said the transactions at the time were valued at $71 million in bitcoin, but with the rise in the currency's value, the value now is more than $4.5 billion. Bitfinex said in a statement it was working with the DOJ to "establish our rights to a return of the stolen bitcoin."

This showed that cryptocurrency was "not a safe haven for criminals," said Lisa Monaco, deputy attorney general.

In another high-profile example last year, former partners and associates of the ransomware group REvil[25] caused a widespread gas shortage on the U.S. East Coast when it used encryption software called DarkSide to launch a cyber attack on the Colonial Pipeline. The DOJ recovered some $2.3 million in cryptocurrency ransom that Colonial paid to the hackers just days later.

Cases like these demonstrate that the DOJ "can follow money across the blockchain, just as we have always followed it within the traditional financial system," said Kenneth Polite, assistant attorney general of the DOJ's Criminal Division. This showed that cryptocurrency was "not a safe haven for criminals," said Lisa Monaco, deputy attorney general.

Transparency

Overall, cyber-criminals have laundered more than $33 billion worth of cryptocurrency since 2017, with most of the total over time moving to centralized exchanges. For comparison, the UN (United Nations) Office on Drugs and Crime estimates that between $800 billion and $2 trillion of fiat currency is laundered each year — as much as 5% of GDP worldwide, whereas money laundering accounted for just 0.05% of all cryptocurrency transaction volume in 2021.

The biggest difference between fiat and cryptocurrency-based money laundering is that, due to the inherent transparency of blockchains, it is much easier to trace how criminals move cryptocurrency between wallets and services in their efforts to convert their funds into cash.

For the first time since 2018, centralized exchanges did not receive most of the funds sent by illicit addresses, taking in just 47%. Instead, the illicit funds were routed through DeFi protocols, which received 17% of all funds sent from illicit wallets in 2021, up from 2% the previous year. That translates to a 1,964% year-over-year increase in total value received by DeFi protocols from illicit addresses, reaching a total of $900 million in 2021. Mining pools, high-risk exchanges and mixers also saw substantial increases in value received from illicit addresses.

25 https://www.reuters.com/technology/exclusive-governments-turn-tables-ransomware-gang-revil-by-pushing-it-offline-2021-10-21/

The increasing concern about DeFi was highlighted in 2021 when the U.S. Treasury Department's Office of Foreign Assets Control (OFAC) sanctioned Suex and Chatex, two DeFi "gateway services" that regularly laundered funds from ransomware operators, scammers, and other cyber criminals.

> *"One of the novel features of DeFi platforms is that visibility and verification of identities of counterparties is not required. Although some platforms have recently introduced know-your-customer (KYC) verification requirements, these are not always necessary for the platforms to function, even though such requirements are required by law in most jurisdictions. In addition, some third-party service providers offer additional privacy-enhancement (or even law evasion) techniques for DeFi users. It can therefore be difficult to trace transactions, increasing the risk of these platforms attracting illegal activities, money laundering, terrorist financing, or circumventing sanctions restrictions."*
>
> ***– Financial Stability Board's update on the assessment of risks to financial stability from crypto-assets, February 2022.***

In a different vein, HM's Revenue & Customs in the UK is reported to have seized NFTs for the first time in February 2022 as part of a fraud investigation.

That said, the Belgian financial services regulator reported[26] that fraud linked specifically to cryptocurrencies fell 11% between 2020 and 2021.

Cryptos are undoubtedly being used in financial crime, but it still appears that, for instance, cryptocurrencies are substantially less likely to be used for money laundering than fiat currency. That said, the war in Ukraine has raised further questions and concerns about the potential for cryptos to be used in the avoidance of, or non-compliance with, sanctions.

> *"While most virtual currency activity is licit, virtual currency remains the primary mechanism for ransomware payments, and certain unscrupulous virtual currency exchanges are an important piece of the ransomware ecosystem. The United States urges the international community to effectively implement international standards on anti-money laundering/countering the financing of terrorism (AML/CFT) in the virtual currency area, particularly regarding virtual currency exchanges."*
>
> ***– FinCEN Updates Ransomware Advisory: OFAC Sanctions Two Ransomware Operators and a Virtual Currency Exchange Network for the Kaseya Incident and Laundering Cyber Ransoms, November 2021.***

26 https://www.fsma.be/en/news/fraudulent-online-trading-platforms-53-cent-increase-reports

The way forward

Policymakers are all-too aware of the need for a coherent approach to cryptos. "Global crypto regulation should be comprehensive, consistent and coordinated," according to the IMF.

Specifically, the international regulatory framework should provide a level playing field along the activity and risk spectrum. The IMF believes this should have the following elements:

- Crypto-asset service providers that deliver critical functions should be licensed or authorized. This would include storage, transfer, settlement and custody of reserves and assets, among others, as with existing rules for financial service providers.
- Requirements should be tailored to the main use cases of crypto-assets and stablecoins.
- Authorities should provide clear requirements on regulated financial institutions concerning their exposure to and engagement with crypto.

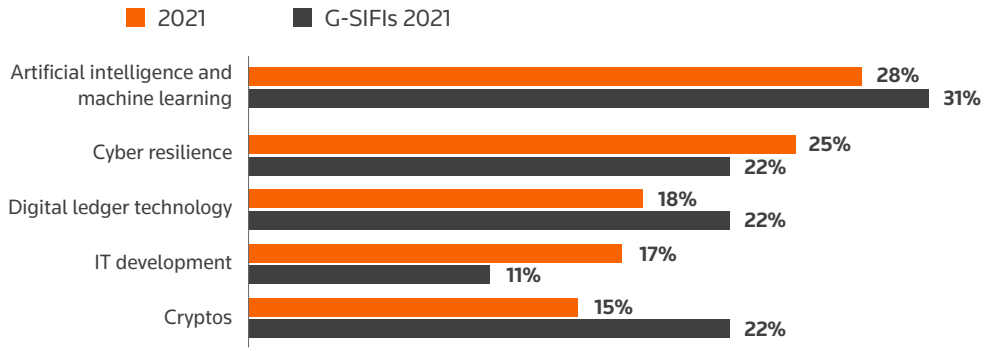
> *"As the financial sector transforms, the stakes — and gains — from cooperation are high. As financial regulators and supervisors, we have a responsibility to make sure that we can continue to deliver on our mandate to safeguard financial stability. We want no holes in the global financial safety net, however much it gets stretched and reshaped."*
>
> ***– Steven Maijoor, executive director of supervision, Dutch Central Bank (De Nederlandsche Bank), February 2022***

Firms and their risk and compliance officers must engage with policymakers and regulators to ensure the best possible supervisory approach. Fast-moving digital transformation and adoption, even in limited terms, of innovative new technology, products and solutions will require skill sets to keep pace.

In addition to crypto, respondents to Regulatory Intelligence's Fintech, regtech and role of compliance report for 2022[27] highlighted a swath of other technological skills, including artificial intelligence and machine learning, cyber resilience and digital ledger technology, as being future knowledge requirements for risk and compliance functions.

27 https://legal.thomsonreuters.com/en/insights/reports/fintech-regtech-and-the-role-of-compliance-in-2022/form?gatedContent=%252Fcontent%252Fewp-marketing-websites%252Flegal%252Fgl%252Fen%252Finsights%252Freports%252Ffintech-regtech-and-the-role-of-compliance-in-2022

Figure 1: **What skills do you see risk and compliance needing in the future?**



Source: Thomson Reuters 2022

A positive and transformative force?

Cryptos have huge potential to be a positive and transformative force for the future of financial services. The point was made in a November 2021 speech[28] by Carolyn A Wilkins, an external member of the Financial Policy Committee at the Bank of England.

Wilkins said she saw crypto-assets as the bedrock of the emerging financial ecosystem. The opportunities and risks extend well past the crypto-assets themselves to encompass a rapidly expanding range of financial services, from lending to insurance, she said. The future of this new frontier will depend critically on the regulatory response to these new activities and how fast the traditional financial system modernizes, and there will need to be major investment in domestic and cross-border payments, as well as digital governance, she said.

Tipping point

In many countries, cryptos appear to be at a legal and regulatory tipping point. Concerns about financial stability and vulnerable customers, together with the apparently persistent misperceptions about financial crime, are driving policymakers to consider significant action. Policymakers must, however, balance these considerations with the benefits which could be derived from the more widespread adoption of cryptos.

Other countries, meanwhile, are welcoming cryptos with seemingly few regulatory concerns. Cryptos' borderless nature makes this even more challenging, as is evidenced by the near-overnight relocation of miners and crypto firms out of China. Most countries are reluctant to stifle innovation, but it would be politically unacceptable to deliberately risk either wholesale financial stability or widespread retail customer detriment.

There is an urgent need for a coherent approach to the regulation and oversight of cryptos; otherwise, there is a danger that they will fail to achieve their potential, and the world will lose the considerable benefits they could bring.

28 https://www.bankofengland.co.uk/speech/2021/november/carolyn-a-wilkins-keynote-speaker-at-autorite-des-marches-financiers-annual-meeting

Thomson Reuters Institute

The Thomson Reuters Institute brings together people from across the legal, corporate, tax & accounting and government communities to ignite conversation and debate, make sense of the latest events and trends and provide essential guidance on the opportunities and challenges facing their world today. As the dedicated thought leadership arm of Thomson Reuters, our content spans blog commentaries, industry-leading data sets, informed analyses, interviews with industry leaders, videos, podcasts and world-class events that deliver keen insight into a dynamic business landscape.

Visit **thomsonreuters.com/institute** for more details.

About the authors

SUSANNAH HAMMOND

Susannah Hammond is Senior Regulatory Intelligence Expert for Thomson Reuters Regulatory Intelligence 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.

TODD EHRET

Todd Ehret is a Senior Regulatory Intelligence Expert for Thomson Reuters Regulatory Intelligence. He has more than 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.

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.

Scan the QR code for more information

THOMSON REUTERS®