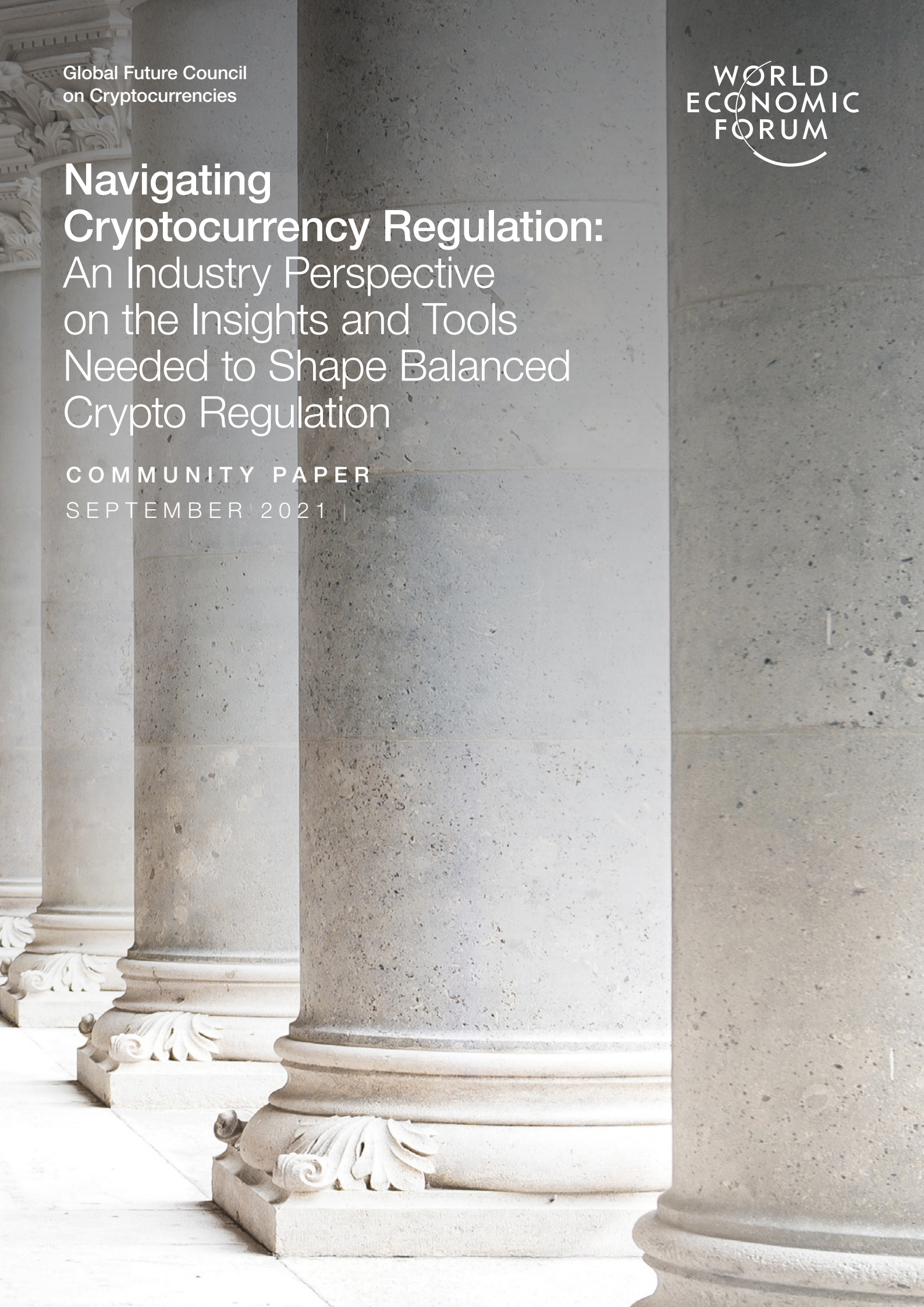


Global Future Council
on Cryptocurrencies

WORLD ECONOMIC FORUM

Navigating Cryptocurrency Regulation: An Industry Perspective on the Insights and Tools Needed to Shape Balanced Crypto Regulation

COMMUNITY PAPER

SEPTEMBER 2021

Images: Getty images

Contents

Executive summary

The technological and economic particularities of cryptocurrencies require prudent regulation that accommodates the characteristics and use cases of cryptocurrency.

Cryptocurrencies and the underlying blockchain technology are becoming a pervasive force in the global economy, affecting everything from cross-border retail payments to interbank transfers. The growing adoption and decentralized nature of cryptocurrencies pose unique and unprecedented challenges for financial authorities, capital markets regulators, consumer protection and privacy bureaus, and tax authorities around the world. However, cryptocurrencies also bring opportunities in terms of leveraging the internet to provide new digital pathways for individuals and micro-, small- and medium-sized enterprises (MSMEs) into the global financial system. Further, cryptocurrencies and underlying blockchains contribute a new paradigm for secure data and value transmission, storage and access. As such, the technological and economic particularities of cryptocurrencies require prudent regulation that accommodates the characteristics and use cases of cryptocurrency.

In simple terms, cryptocurrencies are digital "coins" or "tokens" secured using cryptography. These assets are fully digital; using blockchain or other decentralized ledger technologies (DLTs), they are stored and operate on a decentralized network, with which users can transact directly without the need for a central authority. The assets can be sent instantly at a peer-to-peer (P2P) level, without involving an intermediary such as a bank or central bank. In principle, and in the absence of additional cryptography schemes or failures in security, cryptocurrency transactions are fully traceable and unalterable, and users may remain pseudonymous unless their assets are matched – for example, to a validated know your customer (KYC) file through an exchange.

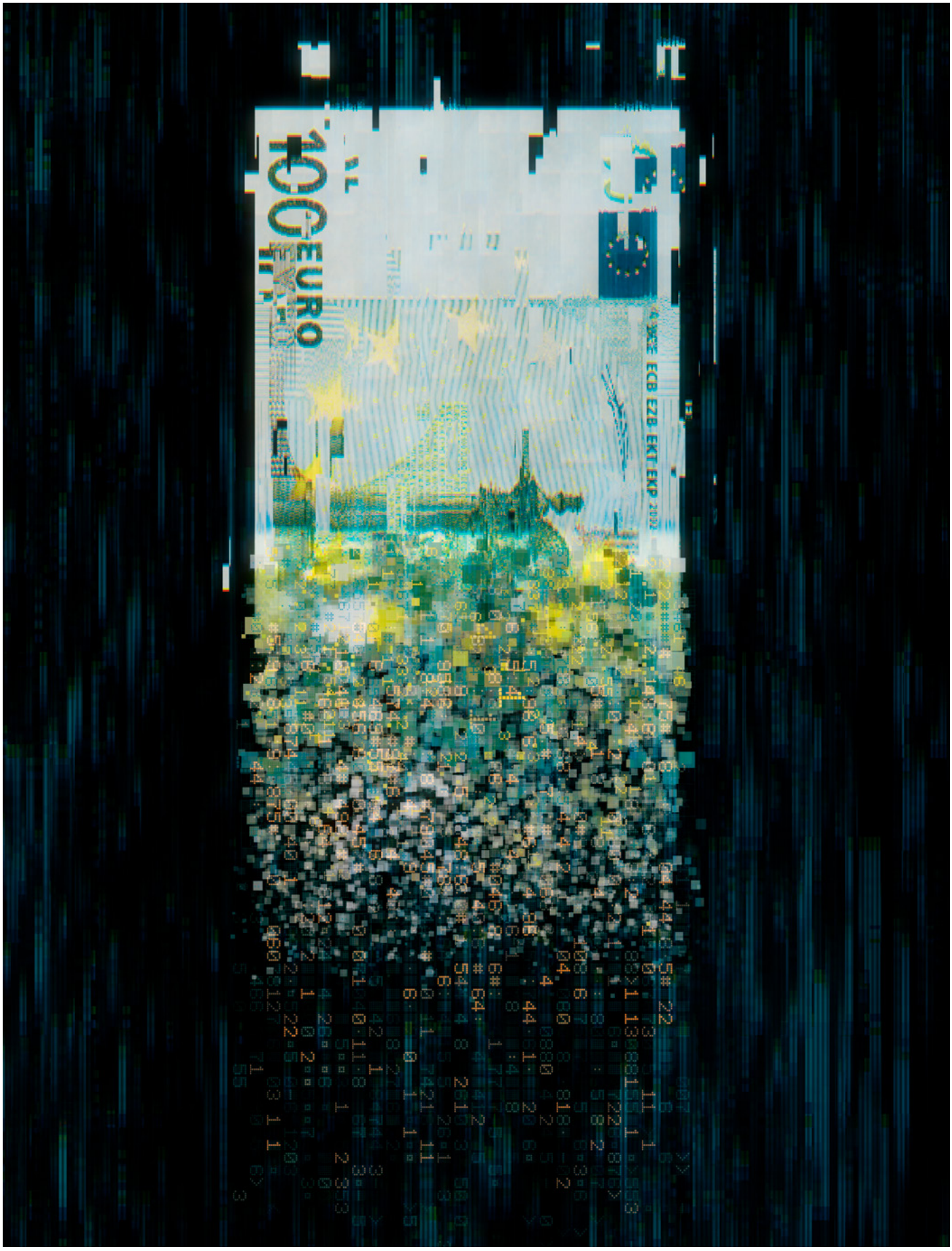
Note: Stablecoins and central bank digital currencies (CBDCs) are outside the scope of this document.

Regulators around the world should develop frameworks to responsibly monitor and guide cryptocurrency activity in their jurisdictions, ensuring, among other things, fair market conduct, market competition, the application and enforcement of tax rules, and consumer protection within the parameters of the assets' unique properties, while nurturing the growth of a lucrative cryptocurrency-based economy. At the same time, cryptocurrencies are cross-jurisdictional and, as such, regulatory challenges do not stop at national borders. Regulators should work towards cross-jurisdictional regulatory standards in order to create regulatory clarity, close loopholes and mitigate regulatory arbitrage, while ensuring inclusion of all users is maintained.

Well-designed cryptocurrency regulations have been implemented in many jurisdictions, encouraging crypto-based innovations and efficiencies in finance and commerce, particularly for cross-border transactions. Regulators should look at examples elaborated upon in this guide to bolster their understanding of the parameters and variables that are pertinent to the design of regulatory frameworks.

This regulatory guide from the Global Future Council on Cryptocurrencies reflects the perspectives of a broad cross-section of the cryptocurrency ecosystem and should be used as a tool to assist financial regulators around the world in developing prudent policies, regulations and ideation to mitigate risks and enable opportunities related to cryptocurrencies. In this guide, we address important themes and considerations for the financial regulation of cryptocurrencies, using insights from the leading authorities on blockchain technology and financial regulators navigating these transformations to the global financial and monetary system.

1 Cryptocurrency basics



This section establishes relevant definitions and provides a framework to consider the many issues presented by cryptocurrencies.

1.1 What is a cryptocurrency and a cryptocurrency network?

For the purpose of this guide, a cryptocurrency[1] is a digital non-governmental asset based on a combination of cryptographic algorithms, whose existence and transfer is confirmed and recorded on a ledger that is distributed across a network of independent computers ("validators"). Before the existence or transfer of a cryptocurrency can be recorded on the ledger, the network's validators must reach agreement according to the network's consensus protocol. The decentralized architecture of the validator network is designed to create trust in the absence of a centralized authority, like a government or other central entity. In a decentralized network, multiple entities operate independently under a network-wide shared governance framework, eliminating the single point of failure or control. This architecture reduces the risk of double-spending,[2] while preserving pseudonymity in a transaction. The validators rely significantly (but not exclusively) on cryptography tools to ensure security. For example, cryptocurrency is used as a utility on the network to incentivize (pay) node operators to validate transactions and protect against spam, distributed denial of service (DDoS) and other attacks.[3]

Cryptocurrencies constitute their own unit of account, although, in most cases, the price to acquire a unit is usually quoted in government-based fiat currency. Additionally, most cryptocurrency projects allow for the issuance of account addresses and the transfer of the currency between sender and recipient, without a centralized party and without the need for personal identification typically required by such parties.[4]

There are two types of cryptocurrencies: (1) traditional cryptocurrencies, which are created by a standalone blockchain such as BTC (Bitcoin) and ETH (Ethereum); and (2) cryptocurrencies that are digital representations of other assets such as those backed by fiat currency (sometimes referred to as stablecoins) such as USDC issued by Circle. This paper is focused solely on traditional cryptocurrencies, which are considered to be mathematics-driven protocols.

1.2 What are some characteristics of cryptocurrency networks?

There are currently thousands of different cryptocurrency projects and networks, many with distinct design, architectures and features. While most cryptocurrency projects rely on a distributed ledger system, there are two primary types of "access" permission: (1) permissionless, where networks are open and any entity can participate in terms of sending transactions, reading the history (ledger) of transactions, or participating in transaction verification; or (2) permissioned, where participation in these activities is limited by a governance framework that restricts participation. The focus of this paper is the former, permissionless cryptocurrency. Additionally, the way networks reach "consensus" between participant validators is varied; some use proof of work (e.g. BTC), others proof of stake (e.g. ADA) and other mechanisms.[5]

2 Regulatory considerations

> A clear, constructive and adaptive regulatory environment for cryptocurrencies would lay a foundation for sustainable innovation, competition and transparency, and allow customers and businesses to safely realize the benefits they may offer.

Regulators and policy-makers around the globe are continuously evaluating how best to address the specific and sometimes novel issues posed by cryptocurrencies. Cryptocurrencies have rapidly evolved from expressions of alternative ideals and systems to well-known assets of interest to investors, private firms and, to some extent, nation states. The regulatory landscape for cryptocurrencies continues to evolve as there is increased interest in and usage of the asset class. Building on earlier eras of innovation in distributed computing and cryptography, cryptocurrencies and the underlying blockchains contribute a new paradigm for many kinds of secure data and value transmission, storage and access more broadly. Much like the development of internet communication protocols, the vast potential for its uses and applications is difficult to predict and the technological and economic particularities of cryptocurrencies render it difficult to automatically apply existing legal frameworks and definitions. As such, a clear, constructive and adaptive regulatory environment for cryptocurrencies would lay a foundation for sustainable innovation, competition and transparency, and allow customers and businesses to safely realize the benefits they may offer. As would be expected, significant differences exist in the scope and breadth of regulatory oversight and expectations, especially between jurisdictions. These challenges could be addressed by a greater level of international cooperation and information-sharing between regulatory bodies.

This section explores some of the challenges and concerns that regulators will need to consider and in some cases address as they respond to the growth of cryptocurrencies in their regions.

2.1 Macro-level and multi-jurisdictional risk

At a macro level, the intersection between the use of cryptocurrencies and the role of commercial banks in delivering monetary services across the globe warrants close attention. From a financial regulator's perspective, current cryptocurrency systems appear to lack features that are critical for sovereign monetary regimes in order to manage and control the financial stability of a country. As cryptocurrencies generally lack an adjustable monetary policy, they cannot respond in the same way to monetary and price stability risks due to shocks to demand for cryptocurrency by adjusting the supply. Similarly, shocks to the supply of cryptocurrency are not mitigated by a monetary authority that could otherwise affect demand to stabilize the price. The capacity to access central banks as the lender of last resort (LOLR) is also not present, potentially increasing the possibility of runs in the absence of a central bank function. Lastly, another concern expressed by central banks is that widely adopted cryptocurrency could potentially weaken a country's monetary sovereignty if fewer people use the domestic unit of account. Though there are no current examples of this taking place, central bankers are concerned that this could potentially result in more volatility of domestic prices as the central bank cannot employ monetary policy as effectively.

At the international level, given the cross-border nature of cryptocurrency networks, a key question is who should oversee the markets for cryptocurrencies and financial market infrastructure (FMI) that interact with crypto-assets[6] in payment, settlement and other activities. These potential ecosystem risks lead to fragmentation of solutions and inconsistencies in interpretive guidance that may eventually hurt consumers and investors in the long term. Already, certain cryptocurrency market intermediaries have suffered disruptions with some frequency, most notably the bankruptcy of notable exchange platforms (e.g. Mt. Gox[7]). And, as the Federal Trade Commission (FTC) in the United States reported in May 2021, "Since October 2020, reports [of cryptocurrency theft] have [increased], with nearly 7,000 people reporting losses of more than $80 million."[8]

Importantly, financial institutions must work to understand local regulatory considerations when establishing operations or providing services that support cryptocurrencies. These include issues ranging from licensing requirements to know your customer (KYC), anti-money laundering (AML) and combating the financing of terrorism (CFT) obligations, as well as restrictions on data use and privacy considerations. However, in many countries, third-party intermediaries dealing with cryptocurrencies face an uncertain regulatory environment, and the challenge of global coordination on a future regulatory approach makes the operating environment ambiguous for traditional financial institutions.

Compliance risks

> The pseudonymous and borderless nature of cryptocurrency systems (and the fact that virtually anyone can create a new cryptocurrency and send it to other addresses) raises potential financial integrity risks.

Data evidence shows that illicit activity comprises just 0.34% of all cryptocurrency transactions, which is lower than the incidence of illicit activity in the traditional financial system.[9] However, the pseudonymous and borderless nature of cryptocurrency systems[10] (and the fact that virtually anyone can create a new cryptocurrency and send it to other addresses) raises potential financial integrity risks. In addition, the decentralized nature of cryptocurrency transactions is not dependent on entities on which financial sanctions and embargoes can be imposed via traditional means. As a result, it is difficult for governments and international organizations to enforce financial sanctions or embargoes, but there are several practical ways to address these issues through international cooperation.

In determining who to regulate, national authorities have mainly focused on cryptocurrency market participants and the financial institutions that interact with them. Potential risks to the status and integrity of financial institutions result from their position as the custodian of other people's money. While the issuance and transfer of cryptocurrencies between users are less likely to pass through an intermediary, the interface between cryptocurrencies and the broader economy (as referenced above) will often go through a cryptocurrency exchange or other virtual asset service provider (VASP). In this context, preventive measures, including enhanced customer due diligence (CDD), transaction monitoring and record-keeping, as well as obligations to report suspicious transactions for higher threshold amounts, are already an important component of many national AML frameworks. If applied proportionately in the crypto-ecosystem, alongside new monitoring platforms,[11] they can assist in detecting and deterring instances of money laundering and creating the evidence needed for prosecuting offences.

Lastly, tax record-keeping requirements for cryptocurrencies vary across countries and may reduce the attractiveness of cryptocurrencies as a payment system in the medium term. In many countries, such as the United States and the Netherlands, it is necessary to calculate and report gains and losses on the use, mining and disposition of tokenized assets, including cryptocurrencies. Wallet providers and custodians can facilitate this record-keeping, but the taxpayer is still responsible for accurate reporting and paying any tax owed. Having multiple exchanges with different prices further complicates the problems in regards to record-keeping.

As referenced above, more could be done at the international level to facilitate the development of appropriate policy responses that align integrity with innovation and inclusivity. Importantly, such global dialogues should encompass a wider diversity of economies and jurisdictional perspectives, particularly smaller countries as well as countries from regions including Africa and the Caribbean, which presently are not part of institutions such as the Financial Action Task Force (FATF) and have minimal representation in the Bank for International Settlement (BIS). As experience is gained, developing international standards supported by best practices from small and larger jurisdictions in different regions could inform more relevant guidance on the most appropriate regulatory responses to the differing risks confronting financial institutions, thereby promoting parity across regions.

Operational risks

The broader acceptance of cryptocurrencies also presents new risks of an operational nature such as the irreversibility of transactions, which is an inherent part of the design of many popular cryptocurrencies.[12] While some networks have developed features to claw back transactions in certain circumstances,[13] the general design of cryptocurrency networks does not allow reversing transactions, as this is a feature to avoid the "double-spend" problem. In these instances, errors in transactions cannot be reversed and, unlike credit cards, customers have no right to reverse the charges if something goes wrong. The finality of transactions is, in many ways, an advantage, but it may create a dependency on the governance and oversight of cryptocurrency systems to ensure that errors or mistakes are addressable in a timely, equitable and auditable manner. Like almost all IT systems, cryptocurrencies are vulnerable to security breaches, and cryptocurrency users face payment system-like risks such as credit risk, liquidity risk and legal risk, just as they do now. Lastly, as with most systems relying on encrypted technology, including many traditional banking systems, cryptocurrencies are vulnerable

to cryptographic risks, the most obvious of which is probably the irrecoverable loss of a private key.

Another important aspect to consider is the definitions of settlement finality and what would legally constitute finality for the variety of cryptocurrency systems (i.e. how that state is determined in a decentralized environment). For example, payment systems in the European Union (EU) need to meet the standards set out in the Settlement Finality Directive (SFD),[14] which guarantees that transfer of assets are irrevocable and final. There are similar standards in most jurisdictions, normally set by the central bank in that country or by the local regulator overseeing payments. A more detailed definition may be required to validate processes and identify the roles and functions of participants in the network, particularly where those networks are unrestricted.

Further work will be needed to define these standards, particularly with respect to how finality would apply to cryptographic assets that rely on consensus mechanisms while understanding that the finality of settlement is a design feature and not a flaw.

2.2 Consumer protection

Consumer protections should be directed at the prevention of unfair, deceptive or abusive practices, and the reduction in harm to end users, including the loss of assets, fraudulent behaviour and cybersecurity risks.

Consumer protection regulations are paramount to safeguard consumer interests and ensure transparent and fair service levels. Regulators can identify which of their consumer protection laws for existing financial products and services are applicable to cryptocurrency products and services. For instance, the responsibilities of a custodian (e.g. VASP) of cryptocurrencies are no different from its responsibilities for other financial instruments: safeguarding customer assets.

Consumer protections should be directed at the prevention of unfair, deceptive or abusive practices, and the reduction in harm to end users, including the loss of assets, fraudulent behaviour and cybersecurity risks. Broadly speaking, the types of concerns and risks to consumers of cryptocurrency products and services will typically be the same as for existing financial services.

Challenges and risks specific to cryptocurrencies and their nature include:

1. The price volatility of cryptocurrency, which constitutes a significant risk to users, as well as merchants accepting cryptocurrencies as a method of payment.

2. The absence of depositor protection. Users can lose savings from many sources such as cryptocurrency price drops, exchange fraud, lost private keys and more.

3. The lack of payment protections due to the irreversibility of transactions.

4. Difficulty establishing accountability towards users due to the decentralized management of cryptocurrencies.

5. Privacy risks stemming from the pseudonymous nature of cryptocurrencies. While pseudonymity hides personally identifiable information, the strings of data representing holders' public key addresses can, with significant effort, be linked back to identifiers, thereby compromising the identity of users and their privacy.

The different ways in which customers may hold crypto-assets also give rise to different consumer concerns. Particularly, self-hosted wallets and allied services, such as decentralized finance (DeFi),[15] which are distinct from custody-based services, require a different approach. With self-hosted wallets, there is no firm holding assets on behalf of a client or "consumer", and consumers are in full control of the asset class. Unlike custody-based services, self-custody wallets are generated by computer protocols and are available to the public directly via the internet. It is incumbent on individual users to understand the interface, security mechanisms, private key management and storage, and the fact that there is no centralized firm involved and there may be no structure to resort to in cases where access to the wallet is lost, for instance. Regulators can make it a point to collect complaints and concerns from the public as well as to provide information publicly about the benefits, best practices and risks of such technology as a matter of public education and resources. Educating the public may be a key aspect in helping address many of the concerns of self-hosted environments. However, consumer protection laws and enforcement actions are unlikely to apply directly given the unique nature of self-hosted technologies. A more detailed explanation of the key aspects of these technologies is provided in the next section.

In conclusion, regulations can help ensure that adequate information is provided to consumers of such financial products, both where firms custody assets on behalf of clients and with platforms that enable self-custody. In countries where cryptocurrencies are not regulated, the government's ability to investigate cases of crypto-related financial crimes would be, in effect, limited due to the fact that the government does not legally recognize cryptocurrencies – the consequence of which might be the loss or theft of such assets.

2.3 Infrastructure-specific issues

This section will unpack concerns surrounding the methods of custody and the importance of interoperability.

Custody and safekeeping of cryptocurrencies

Complex issues such as cybersecurity procedures, operational resilience, storage solutions for underlying assets, and sufficient redundancy are central to most regulatory approaches to cryptocurrency custody regulation.

As mentioned above, the responsibilities of a custodian of cryptocurrencies are similar to its responsibilities for other financial instruments: to safeguard customer assets. However, cryptocurrency is unique in requiring the safeguarding of a private key; this is an additional responsibility that financial services providers in other asset classes do not hold. Ownership of a crypto-asset is reflected in a string of numbers on a distributed ledger, which is accessible by both a public key and a private key. The holder of the private key maintains the agency to perform a transaction involving the crypto-asset. A custodian must implement proper key management practices in order to safeguard the customer's ability to directly dispose of the crypto-asset.

Cryptocurrencies provide the opportunity for self-custody, where customers do not need to use a custodian to hold or manage their crypto-assets. While this provides customers with the maximum ability to express their agency and choice without intermediation, it also introduces significant risk. For example, if a customer loses their private key, they irreversibly lose access to the crypto-assets secured by that private key. As such, most customers opt for custody providers, which act as a fiduciary for the customer and manage or recover a user's keys if they are lost.

Another important difference compared to traditional custody models is the concept of hot and cold wallets (custodial accounts). Hot wallets are connected to the internet, while cold wallets are kept in an offline environment. As hot wallets are connected to the internet, it is faster and easier to trade or spend cryptocurrency – but they may be more vulnerable to online attacks that could increase the risk of stolen funds. Cold wallets are typically not connected to the internet. So, while these may be more secure, they are also less convenient as additional steps are needed to transact. Custody providers should implement a responsible mix of cold and hot wallet strategies to ensure the best user experience and protection.

Given the nascent level of development of the cryptocurrency industry, and especially the custodian arrangements therein, many regulators are assessing which types of custodial solutions are appropriate for the market. Complex issues such as cybersecurity procedures, operational resilience, storage solutions for underlying assets, and sufficient redundancy are central to most regulatory approaches to cryptocurrency custody regulation. Regular verification and certification of compliance typically evaluates the operational, security and technology practices of custody providers. Other considerations include whether custodians: (1) provide custody insurance coverage; (2) have completed either System and Organization Controls (SOC) 1 or SOC 2 audits;[16] and (3) have processes in place to identify and implement technology upgrades when needed.

The concept of private keys is not new in financial services, but in the context of cryptocurrencies they

are synonymous with how custody and clearing services will be supported. For the purposes of this paper, it is assumed that private keys are a technical feature to produce digital signatures. The keys themselves do not constitute the means of safekeeping nor are they essential to legally demonstrating proof of ownership.

As the crypto industry develops, it will be necessary to delve into the difference between more traditional custody models (e.g. the existence of bilateral relationships between the account holder and intermediaries in the custody chain) and the new business models and services that are referenced in the previous paragraphs. For example, from an infrastructure perspective, this could mean that a cryptocurrency custodian does not hold a client's private keys to the underlying assets but instead safekeeps a private key that operates the client's account on their behalf.

Furthermore, as cryptocurrencies continue to gain traction, the existing tools used for custody today will require new technical solutions that incorporate the necessary risk management and controls to prevent the misappropriation of funds. The same can be said regarding aspects such as account structure and asset servicing and their differing functions in a DLT environment.

Mitigating the risks of self-custody

Regardless of how new technologies such as distributed ledgers and self-hosted wallets are deployed, the messaging and reporting of regulated services should adhere, wherever possible and practical, to existing standards.

Self-hosted technologies raise several considerations for companies operating cryptocurrency services. In general terms, cryptocurrency holders using self-hosted technologies have the unilateral ability to access, manage and transfer their holdings and therefore do not need to rely on any financial institution to act on their behalf.

Financial regulators have raised concerns about the prospect of self-hosting due to the nascent development of true non-intermediated transactions and their potential for money laundering (ML) and terrorism financing (TF).[17] For example, the Financial Crimes Enforcement Network (FinCEN) made self-hosted wallets the focal point of its Notice of Proposed Rulemaking released in December 2020.[18] With the stated objective of closing gaps in regulatory obligations to better address the risks associated with virtual currency transactions involving unknown participants, the Proposed Rule requires that service providers collect KYC information when performing transactions involving self-hosted wallets. However, such approaches have been met with criticism by some who say that such data collection erodes existing thresholds of privacy, is practically difficult to enforce and establishes a stricter set of rules than those that apply to cash transactions today.

Regardless of how new technologies such as distributed ledgers and self-hosted wallets are deployed, the messaging and reporting of regulated services should adhere, wherever possible and practical, to existing standards. In the current fragmented ecosystem, with initiatives making use of different protocols and differing technologies, a commonality of rules and standards could significantly help with the adoption and use of cryptocurrency services. However, it should not do so at the expense of innovation and the improper use of data as it relates to privacy. The public and private sectors should work together to find solutions that could give rise to a successful approach.

The importance of technical and jurisdictional interoperability

In addition to the advantages already mentioned, standardized rules can also encourage a higher level of interoperability across the cryptocurrency ecosystem and with legacy systems that will improve competition, drive up levels of participation, and increase inclusion, market liquidity and the development of new services and financial products. For example, industry standards and protocols will help ensure smooth interactions between market participants and their service providers. Similarly, recognized standards for interfaces (e.g. application programming interfaces and market gateways) will encourage interaction between participants that use these systems.

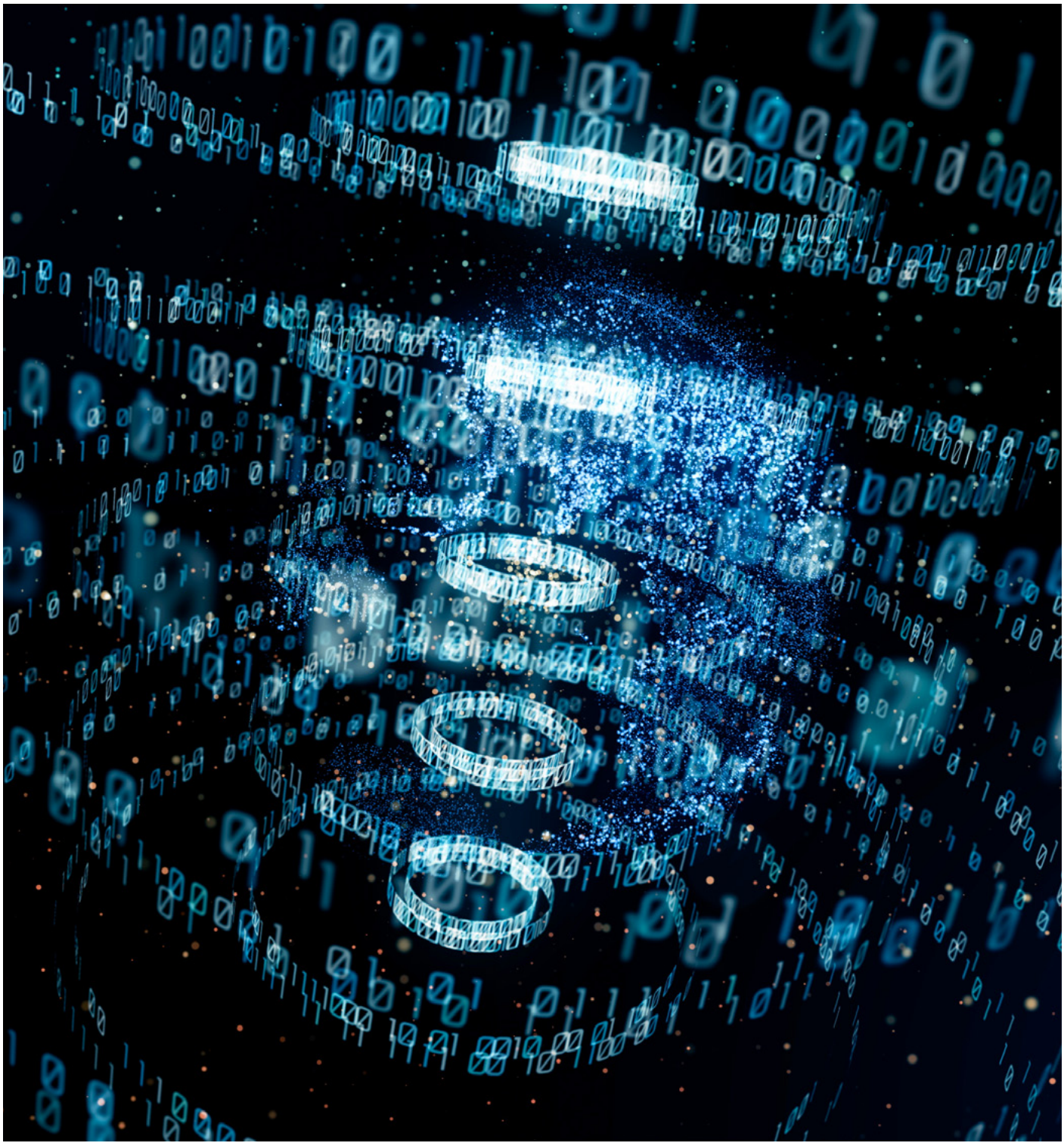
The interoperation of cryptocurrency ecosystems with legacy systems also entails jurisdictional overlap among multiple authorities. This overlap of jurisdictions and authorities increases the regulatory complexity, further underscoring the need for domestic and international cooperation, not only in achieving technical interoperability but in attaining jurisdictional interoperability in the treatment of cryptocurrencies across systems and borders.

2.4 Key takeaways and guiding principles

A lack of clarity on both the definitions of safekeeping (custody) and settlement finality will have ramifications for market participants and their providers. A standardized approach with a shared understanding of equivalence and recognition between jurisdictions will be highly desirable for the long-term adoption and development of the market. The messaging and reporting of regulated services should also adhere, wherever possible, to existing standards. In the current fragmented ecosystem, commonality of rules and industry standards could help significantly with the adoption and use of cryptocurrency services.

It is likely that, over time, access methods will change. Clients may choose to connect directly to systems via new applications, and the custody function itself will evolve. The role of the financial institution in a DLT network will need to ensure customer asset protection, position management and record-keeping in the same way that they do for fiat currencies and the myriad financial products that are based on them. It will also need to facilitate dispute mechanisms in relation to transactions, provide asset-protection insurance and deal with network outages, just as it does today.

3 Regulatory opportunities for inclusion and innovation



While there are potential regulatory risks that should be addressed when considering cryptocurrencies, there are also potential benefits, including increased payment efficiencies, broader financial inclusion, and innovation in digital identification and programmability.[19] This section elaborates upon them.

3.1 De-risking and its global implications

Over the past decade, despite the widespread availability of mobile and other technologies to increase financial access, de-risking[20] decisions have increased in the financial sector and have consequently reduced the number of financial services available to populations in the affected jurisdictions, often smaller countries with younger financial markets. According to the World Bank, cost and benefit considerations and concerns about AML/CFT risk are one of the main drivers of de-risking. Bank de-risking refers to the decision by financial institutions to terminate or restrict business relationships with other financial institutions in another jurisdiction to avoid, rather than manage, risk.[21] At stake are the potential risks of money laundering and terrorist financing that stem from relatively weaker AML/CFT controls as reported in particular jurisdictions. This has especially affected remittance companies and local banks in certain regions of the world, particularly emerging markets.[22]

Unfortunately, the process of de-risking paradoxically generates new risks as more people are forced to use informal and other means to access basic financial services such as payments and savings. Globally, it is estimated that more than 1.7 billion adults are counted as "unbanked" and lack access to even a basic savings account.[23] More than a billion people would not be able to satisfy prevailing KYC requirements for opening a bank account or accessing the formal economy because of a global identity gap. In the same vein, de-risking could have widespread effects on access to crypto-assets globally.

Though financial inclusion and exclusion are driven by a wide range of factors that vary by jurisdiction, it's clear that certain regulatory requirements can create new barriers to financial inclusion. Therefore, as regulators design frameworks for cryptocurrencies, they should explore opportunities to limit de-risking and align compliance with inclusion.

3.2 Addressing financial inclusion and exclusion

The impact of regulation on those who are already financially excluded should be an important consideration in the development of new policies and rules on cryptocurrencies. The challenge facing regulators is that many of the most widespread financial rules, such as the Bank Secrecy Act, were created before the current range of technologies – such as public blockchains, digital currencies and financial integrity capabilities – that exist today. Regulators have an opportunity to carefully decide how to approach the risks, novelties and advantages of new financial technologies such as cryptocurrencies and avoid reinforcing the precedent of systematically excluding vulnerable populations that are "unbanked" in the first place. As an example, in East Africa, it was found that having a more inclusive and innovative approach to KYC (e.g. "tiered-KYC"[24]) and proportionate AML/CFT compliance requirements based on transaction sizes are at the root of the success for mobile money platforms, such as M-Pesa in Kenya.[25]

The open-source software code that underpins cryptocurrencies, self-hosted wallets and distributed ledger technologies creates new opportunities as well as potential barriers for financial inclusion. Although it is too early to know if cryptocurrencies can meaningfully address financial inclusion in a manner that is unique or superior to pre-existing solutions or centralized technology infrastructure, some examples of the unique potential of cryptocurrencies for financial access include:

Self-hosted wallets

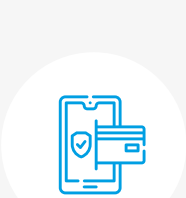
These have the potential to provide a pathway to financial inclusion, reducing reliance on informal cash transfer networks and providing much greater transparency on value flows into and around high-risk environments in which untraceable cash-based transactions are widespread.

Public blockchain-based payments

Cryptocurrencies and related tokens can be used by public institutions and international organizations for aid, relief and remittance corridors. They can be targeted to specific geographies and jurisdictions as well as to white-labelled addresses to help ensure taxpayer and donor proceeds do not inadvertently contribute to unintended consequences such as corruption, bribery and fraud, especially in complex environments.

Universal access to financial services

While global transaction fees average 6.38% for remittances,[26] the UN Sustainable Development Goals (SDGs) call for universal access to financial services, and lowering of the average cost of sending remittances to less than 3% by 2030.[27] In some cases where remittance corridors remain very expensive and innovative fintech solutions have not entered, cryptocurrency (including stablecoins[28]) could offer a means of rapid and lower-cost remittances.



Cryptocurrency-based P2P payments

Although mobile money networks offer P2P payments by drawing on the expansive user base and assets of telecom networks to issue mobile minutes that are redeemable for actual cash, cryptocurrency-based P2P payments do not require a business or firm as an intermediary. Especially in contexts with limited or no financial institution presence, self-custody wallets and internet-native financial contracts such as those provided by DeFi can allow for the transaction of value without banking institutions.

There are also critical risks associated with cryptocurrencies for the financially underserved. As with any technology, there are trade-offs and limitations. The major risks are as follows:

- Users, especially those with low levels of financial and technological literacy, may not fully understand the risks associated with cryptocurrency and may consequently be exposed to adverse circumstances. Cryptocurrencies and their derivative technologies take a variety of forms and need to be defined appropriately to help users and communities understand them properly.
- Self-hosted wallets, which carry the risk of forgotten or stolen private keys, put consumers at high risk of losing their funds. Technical failures could also lead to lost funds.
- As cryptocurrencies are not held at regulated financial institutions and are not subject to depositor insurance protection, funds held in these assets are at greater risk of loss.
- The pseudonymity of cryptocurrencies creates privacy risks for consumers due to the visibility of transactions on a public ledger and the potential of linking this information to a personal identifier.
- Cryptocurrency-based transactions require digital device ownership. While mobile phone penetration is growing,[29] there is still a substantial device accessibility gap particularly among low-income populations and women.
- Additionally, the extent to which cryptocurrency-based P2P payments meaningfully supports

financial inclusion in a manner that does not increase the risk of illicit activity or harm to the financially vulnerable is yet to be determined.

By understanding the nuances of cryptocurrencies and their infrastructure, regulators can decide how to balance the risks and benefits in a more concrete way as well as develop approaches to mitigating risks. As regulators design frameworks for cryptocurrencies, there are opportunities to align compliance with inclusion by using the technological advantages of cryptocurrency networks and learning from past mistakes in order to achieve a more balanced approach, particularly in high-risk jurisdictions.

3.3 Digital identity

The ability of cryptocurrencies to move and store value quickly without intermediation may also create risks to financial integrity, including money laundering and terrorism financing. Some regulators have demonstrated that new digital identity technologies[30] can enable effective, risk-based AML/CFT regimes. Several countries have integrated national digital identity programmes with tiered KYC and/or other electronic know your customer (eKYC) regulations to enable compliant, remote customer onboarding consistent with certain global guidelines such as the FATF recommendations.[31] These include Bangladesh (Porichoy and two-tiered eKYC), India (UIDAI and eKYC), Nigeria (BVN and three-tiered eKYC), Singapore (NDI and eKYC), Ukraine (Diia), United Arab Emirates (UAE PASS) and Sierra Leone (NDIP and eKYC).[32]

For regulators applying FATF's risk-based approach to digital identity systems, there are two issues to address: (1) understanding the assurance levels of the digital identity system's main components to determine if it is a reliable, independent source of information; and (2) making a broader, risk-based determination of whether, given its assurance levels, the digital identity system provides an appropriate level of reliability and independence in regards to the potential ML, TF, fraud and other illicit financing risks at stake. Digital identity solutions can be evaluated on the basis of whether they appropriately address both of the FATF issues in order to support compliant remote authentication and onboarding for the enablement of cryptocurrency services. An additional consideration is whether they allow access rights to inherit these assets in the event of death.

3.4 Key takeaways and guiding principles

Regulators should seek to balance the material risks of cryptocurrencies (which in some cases are not significantly different from conventional financial services) with the potential benefits and regulatory opportunities. There is an opportunity not only to eliminate critical risks to end users and financial integrity through adequate regulatory coverage, but to increase financial access through careful regulation. Of particular focus should be the issues of de-risking, financial inclusion and digital identity in providing a new means of addressing the policy goals of payment integrity and inclusion.

4 Global regulatory approaches

Regulators all over the world are grappling with the best way to regulate the growing cryptocurrency industry. This section explores the different approaches of individual jurisdictions and the guidance from international bodies. For ease of reference, it will also present in a visual and objective manner which countries and regions are taking a more or less progressive approach to the subject.

4.1 Categories of regulatory approaches

Regulators could take different approaches to the design of a regulatory framework. Certain approaches may potentially be combined and/or vary over time depending on the objectives of the regulators in that specific market. We have outlined four general approaches.

1. **"Wait and see" approach:** A "wait and see" regulatory approach implies not issuing specific regulation on the nascent industry in order to allow for its development. It usually combines existing laws and regulations with close monitoring, which leads to the timely development of a regulatory framework that addresses potential attendant risks. It ultimately seeks to avoid affecting innovation before it has even taken off, but remains attentive and ready to act if and when required to preserve stability, among other needed variables. A good example is Brazil, where, despite the non-existence of crypto-specific laws or regulations issued by the financial authority, cryptocurrency entities can operate based on pre-existing laws and regulations applicable to the financial sector.

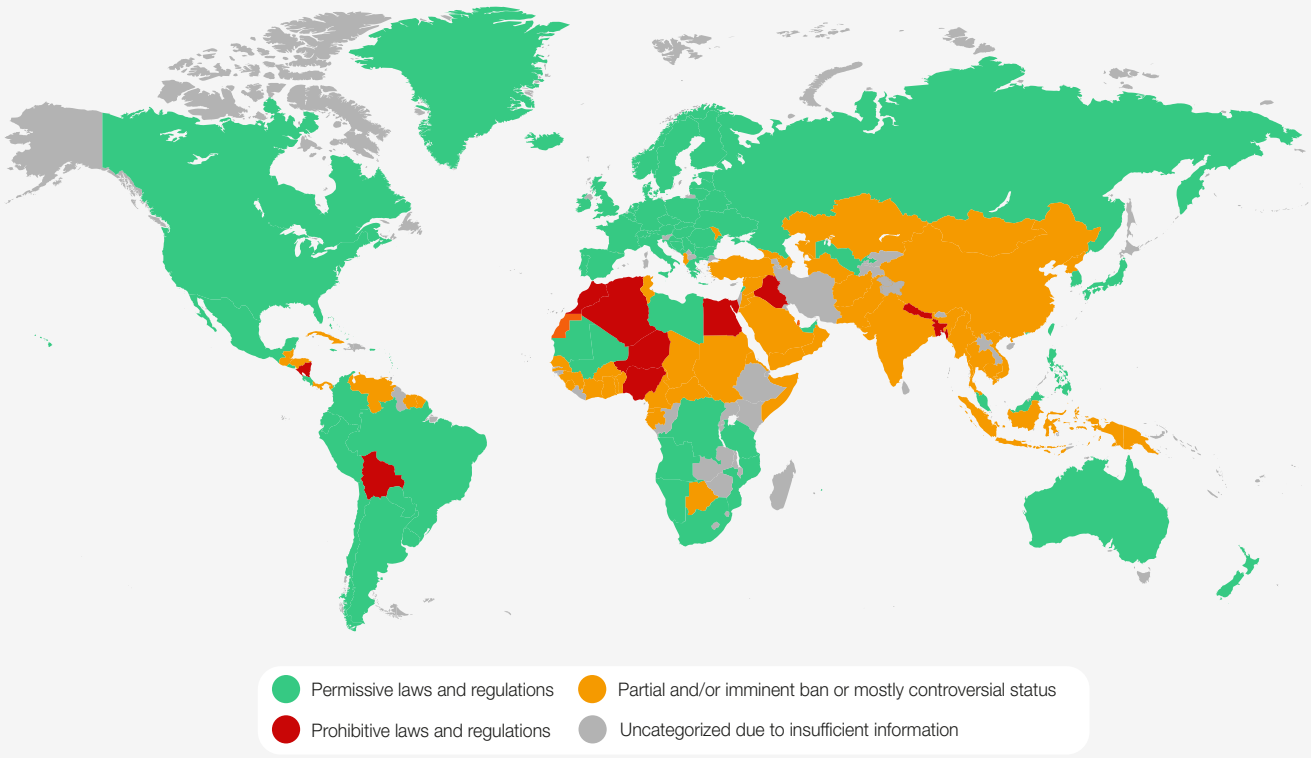
2. **Public-private partnership approach (balanced/risk-proportionate approach):** The public-private partnership or balanced/risk-proportionate approach entails a collaborative engagement between policy-makers, regulators and the private sector in order to work together through task forces and/or innovation hubs on the design and implementation of laws and regulations that aim to develop an inclusive and innovative financial system. Under this approach, regulators tend to develop a better understanding of the innovators and adapt quickly to the fast-paced nature of the environment, while businesses tend to adjust more quickly to regulators' concerns to protect the reputational integrity and value of the ecosystem. For example, Singapore and the European Union have opted for a balanced approach.[33] The Monetary Authority of Singapore (MAS) is taking a collaborative, risk-proportionate approach to blockchain, and has launched a regulatory sandbox where fintechs, banks and regulators work together. In addition, the MAS has developed a payments service framework to ensure AML compliance for companies involved in the dealing or exchange of virtual currencies.[34] The European Central Bank formed a task force on distributed ledgers and launched a joint research project with the Bank of Japan; and the European Commission launched the EU Blockchain Observatory Forum to gather information from EU members on use cases, and engage experts and practitioners before formulating concrete policies.[35]

3. **Comprehensive regulatory approach:** The comprehensive regulatory approach involves designing and implementing a specific regulation that would govern activities conducted by the regulated entities. This could typically comprise licensing requirements, such as reporting and AML/CFT obligations, in order to provide financial services and foreign exchange restrictions for cross-border transfers, among others. Examples include Switzerland, Japan and New York, USA. At the level of the EU, the Markets in Crypto-Assets (MiCA) Regulation will provide Europe-wide regulations for crypto-assets.[36]

4. **Restrictive approach:** The restrictive approach implies imposing more broad restrictive measures that affect the market generally. This may be based on a more conservative or precautionary view and/or may derive from a specific market experience or event. Countries that have proposed bans due to concerns about fraud and AML/CFT risks include Turkey, India and Nigeria, among others. Such determinations are within the purview of the respective nation states. However, adopting definitive legislation at an early stage and in a broader manner may be premature and affect innovation which could be of the interest of the nation states.[37]

4.2 Legal status of cryptocurrencies around the world

FIGURE 1 **Legal status of cryptocurrencies**[38]



This map visually represents the approach taken by most countries to the regulation of cryptocurrencies as of September 2021.

Green indicates countries that have more permissive laws and regulations. This would encompass the first three approaches described in the topic above: i.e. the "wait and see" approach, public-private partnership approach and comprehensive regulatory approach. Red covers the countries opting for more prohibitive laws and regulations, as described in the last approach mentioned above: i.e. the restrictive approach. Orange relates to countries that have been adopting partial and/or imminent bans or those whose situations are more controversial.

For a more in-depth look at how these approaches might apply at the country level, we have compared the approaches taken by 11 distinct countries across South America, the Caribbean, Europe, Asia, the Middle East and Africa. It is hoped this will provide context on how jurisdictions might evaluate the elements they need to consider in regulating cryptocurrencies.

TABLE 1 | **Country-level comparison of regulatory approaches to cryptocurrency**

	Recognition and definition of crypto-assets	Adoption of FATF Travel Rule	Taxation	Country-level impact
United Kingdom	The Financial Conduct Authority (FCA) policy statement PS19/22 (2019) provides guidance on crypto-assets and the applicable regulatory regime for each type. Rule PS20/10 (2020) prohibits the sale of investment products that reference cryptocurrencies to retail clients.	The FCA requires custodian wallets and crypto exchanges to register according to the 5th EU AML Directive published in 2018.	Her Majesty's Revenue and Customs (HMRC) set forth guidance in 2018 that a capital gains tax may apply to the sale, exchange, use (for payment), transfer and donation of crypto-assets.	The UK's regulations relying on early-stage consultations have resulted in less regulatory uncertainty and a more conducive policy environment for cryptocurrency.
Singapore	The Monetary Authority of Singapore (MAS) passed the Payment Services Act (2019), which licenses and regulates payment service providers. It regulates cryptocurrency-based payments and payment service providers as "digital payment tokens" (DPT) and "digital payment token services".	The PSA (2019), through Notice PSN02 requires crypto-currency service providers to adhere to AML/CFT compliance measures per FATF guidance.	The Inland Revenue Authority of Singapore's (IRAS) guidance on the tax treatment of crypto-assets establishes that individuals/businesses who hold DPT as a long-term investment face no capital gains tax. However, businesses that buy and sell DPT are required to pay taxes on their profit.	Singapore's supportive approach to cryptocurrency, as illustrated by the MAS helping crypto businesses set up in Singapore, has enabled Singapore to grow into a burgeoning crypto-economy, with 43% of Singaporeans owning cryptocurrency.
Switzerland	The Swiss Parliament passed the Federal Act on Adaptation of Federal Law to Developments in the Technology of Distributed Electronic Registers (2020), which sets forth an expanded framework for regulating blockchain and DLT based on the token taxonomy in the ICO guidelines (2018).	The AML Act (2020) requires blockchain businesses to verify customer ID and report it to the Money Laundering Reporting Office, abiding by the FATF guidance.	The Swiss Federal Tax Administration (FTA) has set out guidance on the tax treatment of cryptocurrencies, which establishes that private wealth generated from cryptocurrencies does not incur taxes. However, income earned from mining and trading are subject to taxation. As of February 2021, the canton of Zug is accepting tax payments in cryptocurrency.	Early guidelines and acts for cryptocurrencies reduced the legal uncertainty such that cryptocurrency businesses have been able to emerge.

	Recognition and definition of crypto-assets	Adoption of FATF Travel Rule	Taxation	Country-level impact
Japan	The Payment Services Act (Act 59/2009) and its Amendment (Act 50/2020) characterizes cryptocurrencies as crypto-assets. The act, enforced by the Financial Services Agency (FSA), regulates crypto-asset exchanges and custody services.	The Payment Services Act requires compliance with global AML/CFT such as those recommended by FATF. Additionally, the Act on Prevention of Transfer of Criminal Proceeds (2018) was amended to require crypto businesses to verify customer IDs and report suspicious transactions to the authorities.	In 2017, the National Tax Agency ruled that profit earned through the sale or use of cryptocurrency is considered miscellaneous income. Additionally, inheritance tax will be imposed on the estate of a deceased individual who held crypto-assets.	Japan's move to establish a regulatory framework for cryptocurrencies much earlier than most countries has led to the proliferation of regulated crypto exchanges and custody services in the country.
United Arab Emirates	In 2018, the Abu Dhabi Global Market (ADGM) released the first set of regulations in the UAE for cryptocurrencies. In 2020, the Central Bank of the United Arab Emirates (CBUAE) and the Securities and Commodities Authority (SCA) released crypto regulations through guidance and decision.	The Financial Services Regulatory Authority (FSRA) Guidance (2018) and SCA Decision (2020) prescribe the AML/CFT requirements for abiding by the FATF guidance, and the necessary controls and scope of AML/CTF, respectively.	There is no regulation or guidance on the taxation of cryptocurrencies in the UAE.	Regulatory certainty from the financial free zones and the federal regulator has resulted in an increasing number of crypto businesses setting up in the UAE.
Bermuda	The Companies (Initial Coin Offering) Regulation (2018) and Amendment, followed by the Digital Asset Issuance Act (2020) provide the framework of digital asset issuance. The Digital Assets Business Act (2018) regulates their businesses.	The Bermuda Monetary Authority put forth AML/anti-terrorist financing (ATF) guidance in Sector-Specific Guidance Notes for Digital Assets, to be followed in conjunction with the main Guidance Notes for AML/ATF applicable to regulated financial institutions.	Digital assets do not incur income capital gains, withholding or other taxes. Digital asset transactions are generally exempt from the foreign currency purchase tax of 1%.	Bermuda's open regulatory framework has lowered the barriers to entry for crypto-asset businesses. As such, Bermuda has emerged as a regional fintech hub. At present, nine leading fintechs have registered in the country to take advantage of the favourable rules on crypto-assets.

	Recognition and definition of crypto-assets	Adoption of FATF Travel Rule	Taxation	Country-level impact
Brazil	No specific regulations have been issued for cryptocurrencies, but the existing regulations for the financial sector provide a framework for cryptocurrency businesses.	The current set of AML/CFT laws and regulations, especially Brazil Ordinary Law No. 9613/98, are being applied extensively and comprehensively, and apply to businesses dealing with cryptocurrencies.	The tax authorities have issued specific instructions for stating ownership of cryptocurrencies such as information on bitcoin holdings and capital gains in the case of sale of bitcoin, as well as transactions above a certain amount. General capital gains rules apply to cryptocurrency transactions.	Despite the absence of crypto regulation, cryptocurrency innovations have emerged in Brazil. However, the existence of specific crypto regulations would create the necessary legal security for the growth of crypto businesses.
China	The Civil Code (2020) recognizes cryptocurrency as inheritable property. However, China has banned cryptocurrency exchanges and mining operations.	Since China has prohibited virtual asset activities, many AML/KYC requirements remain inapplicable, as specified in FATF's 2020 Report.	Income earned from the purchase and sale of "virtual currencies" is considered taxable income for individual income tax computed under "property transfer income".	Despite its legal recognition of cryptocurrencies, they are greatly restricted. China is placing more emphasis on central bank digital currency, namely the digital yuan, which is currently in development. Therefore, the place of privately issued cryptocurrencies in China is uncertain.
India	In 2018, the Reserve Bank of India (RBI) prohibited entities from dealing with crypto-related businesses. This order was struck down by the Supreme Court of India in March 2020.	There is no regulation implementing the FATF's Travel Rule for cryptocurrency service providers.	No regulation or guidance has been issued for the taxation of cryptocurrencies.	The absence of crypto regulation and the ensuing regulatory uncertainty is a hurdle for innovation in the industry. However, in May 2021, it was reported that the government may form a committee to regulate cryptocurrencies.

Nigeria	The Central Bank of Nigeria (CBN) and Securities and Exchange Commission (SEC Nigeria) have not yet regulated cryptocurrencies, but have recommended since 2017 that financial institutions do not deal in crypto, nor hold the accounts for crypto exchanges. However, the SEC and CBN have agreed to "collaborate and conduct research with a view to finding ways of regulating the cryptocurrency market".[39]	Although crypto exchanges are unregulated, CBN (2017) requires banks to ensure their clients follow appropriate KYC/AML procedures.	Nigeria describes cryptocurrency as an intangible asset other than goodwill, and does not levy any taxes on cryptocurrencies.	Nigeria's approach to the regulation of cryptocurrencies has created uncertainty for developers and SMEs within Nigeria, along with those attempting to do business within the market. The recent focus on collaboration has created some optimism that useful engagement can create regulatory certainty.
South Korea	The Government of South Korea has maintained its stance of warning about the speculative nature of investment in digital assets since its Emergency Meeting on Digital Currencies (2018).	The Act on Reporting and Using Specific Financial Transaction Information (2021) requires VASPs to interoperate their customers with real-name bank accounts and report doubtful transactions.	The Ministry of Strategy and Finance announced that they would impose a 20% tax on income earned from renting and transferring digital assets from January 2022.	South Korea's cautious position on cryptocurrencies and the related businesses has restricted crypto innovation.

Risks of over-regulation and under-regulation

The above map and table reveal the range of approaches countries are taking and could take to the regulation of cryptocurrencies. Indeed, cryptocurrencies present new and quite complex governance challenges. They are also challenging considering their speculative nature and potential impact on financial stability and macroeconomic growth. These differing regulatory approaches, which vary from total risk-aversion to governmental endorsement, present different obstacles and consequences for consumers, industry and innovation, as well as government.

Both over-regulation and/or under-regulation should be avoided. Over-regulation, such as early-stage costs for licensing requirements, tax burdens or very strict foreign exchange controls, may suffocate innovation efforts. Conversely, there are also risks to taking an under-regulation approach. For instance, failing to address ML, TF, fraud and ransomware risks could lead to significant losses to consumers (as covered in the consumer protection section), businesses and investors, in addition to potential financial stability risks.

It should also be noted that, in view of the digital and global reach of cryptocurrencies, both scenarios – over-regulation and under-regulation – may also imply regulatory arbitrage. As different jurisdictions develop regulatory approaches to the cryptocurrency industry at different paces, innovators may gravitate to jurisdictions with more favourable, transparent and reliable regulatory regimes.

Therefore, the regulatory model for cryptocurrencies should be proportionate and risk-based. This includes clarity of regulatory expectations for the industry and the potential impact on competition, innovation and financial inclusion.

The approach should also consider and reflect international discussions and collaboration through standard-setting bodies to support harmonization of treatment as far as is feasible, as exemplified by the United Kingdom's consultation with industry and stakeholders on a regulatory approach for crypto-assets and stablecoins.[40]

4.3 Guidance from international bodies

In addition to country-level approaches, the positions taken by international bodies on cryptocurrencies are critical and have significant ramifications for country-level adoption and regulations, as well as global regulatory and operational interoperability. As standard-setting bodies, they have an important role to play in building an enabling environment for the effective use of cryptocurrencies and setting the foundation for consistency across jurisdictions in the treatment of cryptocurrencies.

International bodies recognize the opportunities and challenges that the cryptocurrency architecture presents to the global economy. For the purposes of this paper, five global organizations/institutions have been identified that have been instrumental in shaping the dialogue on the regulation of cryptocurrencies from different perspectives.

The Financial Action Task Force (FATF) has examined and provided recommendations for a risk-based approach to regulating cryptocurrencies aimed at preventing money laundering and terrorism financing activities using cryptocurrencies. To this end, it has extended its Travel Rule obliging cryptocurrency service providers to obtain, hold and exchange information about beneficiaries and originators of cryptocurrency transfers. It also monitors the implementation of these rules by way of a 12-month review. This has led to increased focus on AML/CFT risks associated with cryptocurrencies and the development of technological solutions addressing these issues. Uneven implementation of the recommendations has also resulted in issues relating to jurisdictional arbitrage.[41]

The Financial Stability Board (FSB) has analysed cryptocurrencies from the lens of financial stability. In a 2019 report, the FSB reported that cryptocurrencies do not pose a risk to financial stability, with a caveat that the topic of regulatory approaches and potential gaps and the question of increased global coordination be kept under review. It, therefore, highlighted the need for vigilant monitoring systems, taking into consideration the rapid development of new products and services.[42]

The Basel Committee on Banking Supervision (BCBS) is working on developing policy frameworks pertaining to risks and rewards due to the increased exposure of banking systems to cryptocurrencies. For this purpose, it has released a public consultation. Categorizing cryptocurrencies such as bitcoin as Group 2 crypto-assets, which are being considered as higher-risk assets due to their volatility and opacity, has led to a conservative, prudential treatment of such cryptocurrencies.[43]

The Organisation for Economic Co-operation and Development (OECD) released a report in 2020 focusing on the issue of taxation of cryptocurrencies. The report served as a cross-country comparison of the tax treatment of cryptocurrencies across the main tax types, i.e. income, consumption and property taxes. It highlighted challenges such as the nature of cryptocurrencies (decentralized protocols), valuation difficulties and hybrid characteristics in taxing cryptocurrencies. It also considered the challenges posed by emerging issues such as forking, stablecoins, central bank digital currencies (CBDCs), the evolution of consensus mechanisms and DeFi, among others. Advocating the need for clear guidance by countries on the tax treatment of cryptocurrencies and other crypto-assets, the OECD also emphasized the need to review/adapt such guidance frequently. With the aim of ensuring tax transparency, it is also working on designing a tax-reporting framework for cryptocurrencies and the income derived from their sale.

The International Organization of Securities Commission (IOSOC) is focused on protecting investors, ensuring that markets are fair, transparent and efficient, and reducing systemic risk. While recognizing that cryptocurrencies may facilitate capital formation and financial inclusion, it has warned against the risks arising from using/investing in cryptocurrencies. It has, therefore, focused on promoting education among retail investors in this regard.[44]

In sum, international institutions have been working on analysing various risks relating to cryptocurrencies. The major risks that these guidelines seek to address pertain to money laundering, terrorism financing, risks to retail investors, risks to the stability of the banking/financial system and taxation of cryptocurrencies. In order to minimize these risks, international bodies recommend the following:

1. *Need for regulatory certainty*: Clarity in the regulatory status of cryptocurrencies will allow the ecosystem to grow and promote innovation, thus harnessing the benefits of cryptocurrencies while mitigating the risks arising from them.

2. *Developing a coordinated approach*: Given the cross-border nature of the crypto ecosystem, countries should coordinate and collaborate with each other and with international standard-setting bodies to avoid issues of jurisdictional arbitrage.

3. *Taking a risk-based approach*: The crypto ecosystem should be regulated commensurate to the risks posed. This involves countries assessing the various risks posed by cryptocurrencies and proactively focusing on mitigating them.

4. *Evolving agile frameworks*: Keeping in line with the rapid pace of development in this space, countries should follow agile frameworks, such that they can be monitored and reviewed on an ongoing basis. As an example, while in the initial years the focus of international guidelines were the intermediaries that had emerged in the crypto space (exchanges, custodians, brokers etc.), today, with developments in decentralized protocols, new consensus mechanisms and stablecoins/CBDCs, international bodies have been working towards analysing risks relating to those spheres as well.

These international recommendations highlight the need to evolve regulatory certainty, domestically and globally, through a coordinated approach, with the aim of promoting uniformity and clarity while minimizing the potential risks arising from cryptocurrencies.

4.4 Key takeaways and guiding principles

The main takeaways revealed by the approaches being taken by different jurisdictions on the treatment of cryptocurrencies and the guidance coming from international bodies are as follows:

1. Regulation of cryptocurrencies is an evolving and global challenge, which is primarily being dealt with on a country level but is also of importance to international bodies and regulators.

2. Although certain countries are taking a more reactive approach, others are making more efforts to create a better regulatory environment for the development of cryptocurrency businesses, while also establishing frameworks to limit malicious activities and financial stability risks.

3. Over-regulation or under-regulation can lead to regulatory arbitrage as players seek to establish businesses in more advantageous jurisdictions. It should be noted, however, that this does not mean entities are necessarily looking for more deregulated jurisdictions. Actually, large venture capitalists (VCs) and institutional players are usually looking for jurisdictions that will allow more clarity and security for the development of their businesses. As such, a balanced approach to regulation is necessary across jurisdictions.

Within the context explored and weighing the risks and opportunities therein, we are confident that the observance of the following guiding principles shall be of interest to regulators:

1. *Banning is not necessarily efficient*: Considering the decentralized governance model of most cryptocurrencies, and the particular circumstances surrounding their existence and transfer, a legal ban will not necessarily imply the end of the activities surrounding them.

2. *Promoting an environment of legal certainty is a positive sign*: The enablement of frequent communication between regulators, the markets and the consumers, alongside the creation of more precise and clear rules, promotes an environment of legal certainty, which is commonly understood as a positive sign for investors and businesses.

3. *Regulating while allowing for innovation is best*: Efforts should be made to allow innovation. However, regulators should find an appropriate balance between encouraging innovation and mitigating its risks. This requires an enabling yet robust regulatory environment that minimizes any potentially negative macroeconomic impacts.

Conclusion

This report provides industry perspective to regulators on the development of prudent regulation for cryptocurrencies. Regulators should draw on this report's analysis and expert insights across several themes related to cryptocurrency regulation, including:

1. The characteristics of cryptocurrencies and the underlying blockchain technology

2. Cryptocurrencies' incongruence with traditional financial regulation and associated risks to the financial system

3. Key challenges and considerations for regulating cryptocurrency activity

4. Current best practices for regulation and examples from forward-looking regulatory regimes

Cryptocurrencies will continue to gain traction in the global economy across retail and institutional use cases, as individuals, businesses and banks adopt cryptocurrencies for investment, payment and an array of other utilities. They touch every aspect of financial activity and regulation, including market conduct, taxation rules and consumer protection.

The unique characteristics of cryptocurrencies that drive their adoption also make them difficult and, in some cases, impractical to regulate. Specifically, the decentralized nature of cryptocurrencies allows them to be transacted at a peer-to-peer level, across-borders, without intermediaries. In addition, holders of cryptocurrency are often pseudonymous, unless they have gone through a KYC process with a regulated exchange or financial institution product, for example. Existing financial regulations for a fiat-based economy are inadequate to monitor and guide cryptocurrency activity in the financial system; they are also insufficient to protect the financial system from key risks, such as fraud, money laundering and the irreversibility of erroneous transactions.

It is integral that regulators develop tailored regulatory frameworks that create an environment conducive to the adoption of cryptocurrencies and development of crypto-based commerce, alongside mechanisms to protect the integrity, security and stability of the financial system and its actors. Prudent regulation requires an in-depth understanding of the blockchain technology that underpins cryptocurrencies, and its power to revolutionize the global financial system. Cross-jurisdictional cooperation and government-industry collaboration are essential to a pragmatic global regulatory environment for cryptocurrencies.

Contributors

The Global Future Council on Cryptocurrencies would like to extend its sincere thanks to the regulators, policy-makers and central bankers who contributed their insights and perspectives to this guidance document. The feedback received from these authorities spanning multiple continents was instrumental to developing a guide that could speak to regulators in countries that are in the preliminary stages of understanding and decision-making, as well as those much more advanced in the process. Written from an industry perspective with objective feedback from decision-makers, it serves as a practical resource for formulating regulatory approaches to cryptocurrency.

Subject leads

Gabriel Abed
Ambassador of Barbados to the United Arab Emirates and Chairman, Abed Group, Barbados

Alpen Sheth
Senior Technologist, Financial Innovation, Mercy Corps Ventures, USA

Denelle Dixon
Chief Executive Officer, Stellar Development Foundation, USA

Rosine Kadamani
Regulatory LATAM, Stripe, Brazil

Co-authors

Vansa Chatikavanij
Director, Digital Assets Asia, Thailand

Matthew Davie
Chief Strategy Officer, Kiva, USA

Jose Fernandez da Ponte
Vice-President, General Manager Blockchain, Crypto and Digital Currencies, PayPal, USA

Brad Garlinghouse
Chief Executive Officer, Ripple, USA

Yusuf Hussain
Head of Risk, Gemini, USA

Paul Maley
Managing Director, Global Head of Securities Services, Deutsche Bank, United Kingdom

Sebastian Serrano
Chief Executive Officer, Ripio, Argentina

Council manager

Clarisse Awamengwi
Project Specialist, Blockchain and Digital Assets, World Economic Forum

Reviewers

Marwan Al Zarouni
Chief Executive Officer, Dubai Blockchain Center, United Arab Emirates

Arushi Goel
Project Specialist, Data Policy and Blockchain, World Economic Forum

Mariana Gomez de la Villa
Program Director, Distributed Ledger Technology, ING, Netherlands

Nadia Hewett
Project Lead, Data for Common Purpose Initiative, World Economic Forum

Kibae Kim
Project Fellow, Centre for the Fourth Industrial Revolution, World Economic Forum

Ashley Lannquist
Project Lead, Blockchain and Digital Currency, World Economic Forum

Sheila Warren
Deputy Head, Centre for the Fourth Industrial Revolution Network, World Economic Forum

Endnotes

1. As yet, there is no unique or official definition of cryptocurrencies, though international bodies are making significant efforts in reaching a common view of the concept. You may consult these resources for a more in-depth explanation of cryptocurrencies: Houben, Robby and Snyers, Alexander, *Cryptocurrencies and Blockchain: Legal Context and Implications for Financial Crime, Money Laundering and Tax Evasion*, European Parliament, 2018; World Economic Forum, *Cryptocurrencies: A Guide to Getting Started,* 2021 (links as of 4/8/21).
2. Double-spending is a situation in which the same token can be spent more than once. Fundamental cryptography offers tools to prevent double-spending while maintaining transaction anonymity.
3. More information about the architecture of Bitcoin and Ethereum, and on the relevance and potential of these projects, can be explored in the educational content made available by specialist and educator Andreas Antonopolous through his books and videos. A general framework on Bitcoin is also provided in Kadamani, Rosine, *Panorama Bitcoin*, Blockchain Academy, 2021.
4. Identity documentation may still be required to fight against illicit activity. However, it is not required for the technical transfer of cryptocurrency.
5. Please note that these are liable to change as networks change their mining and governance mechanisms.
6. "Crypto-assets" and "cryptocurrencies" are used interchangeably in this report.
7. Frankenfield, Jake, *Mt. Gox*, *Investopedia*, 26 March 2021 (link as of 4/8/21).
8. *Consumer Protection Data Spotlight*, *Federal Trade Commission,* May 2021 (link as of 4/8/21).
9. *The 2021 Crypto Crime Report*, Chainalysis, 2021 (link as of 4/8/21).
10. *EBA Opinion on Virtual Currencies*, European Banking Authority, 11 August 2014 (link as of 4/8/21).
11. As an example, see *Chainalysis KYT*, Chainalysis (link as of 4/8/21).
12. He, Dong et al., *Virtual Currencies and Beyond: Initial Considerations,* IMF Staff Discussion Notes, SDN/16/03, January 2016 (link as of 4/8/21).
13. See van der Hoeven, Tyler, *Using Protocol 17's Asset Clawback*, Stellar, and *Assets*, Algorand (links as of 4/8/21).
14. *The Use of DLT in Post-Trade Processes: Advisory Groups on Market Infrastructures for Securities and Collateral and for Payments,* European Central Bank, April 2021 (link as of 4/8/21).
15. For more on decentralized finance and its opportunities and risks that should drive policy-making, see the *Decentralized Finance (DeFi) Policy-Maker Toolkit*, World Economic Forum, June 2021 (link as of 4/8/21).
16. *SOC for Service Organizations: Information for Service Organizations*, AICPA (link as of 4/8/21).
17. *12-Month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers*, Financial Action Task Force (FATF), June 2020 (link as of 4/8/21).
18. *Proposed Rule: Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets*, Financial Crimes Enforcement Network (FinCEN), 23 December 2020 (link as of 4/8/21).
19. Lee, Alexander, *What Is Programmable Money?*, Board of Governors of the Federal Reserve, 23 June 2021 (link as of 4/8/21).
20. Ibid.
21. *De.risking*, Council of Europe (link as of 4/8/21).
22. *De-risking in the Financial Sector*, World Bank, 7 October 2016 (link as of 4/8/21).
23. *The Global Findex Database 2017*, World Bank (link as of 4/8/21).
24. *KYC Innovations, Financial Inclusion and Integrity in Selected AFI Member Countries*, Alliance for Financial Inclusion, March 2019 (link as of 4/8/21).
25. *Overcoming the Know Your Customer Hurdle: Innovative Solutions for the Mobile Money Sector*, GSMA, 2019 (link as of 4/8/21).
26. *Remittance Prices Worldwide Quarterly*, World Bank, March 2021 (link as of 4/8/21).
27. #Envision2030 Goal 10: Reduce Inequalities, United Nations (link as of 4/8/21).
28. For more on stablecoins, see Arner, Douglas et al., *Stablecoins: Risks, Potential and Regulation*, BIS Working Papers, No 905, Bank for International Settlements, November 2020 (link as of 4/8/21).
29. *The Mobile Economy 2020*, GSMA, 2020 (link as of 4/8/21).
30. Examples include *Kiva Protocol* and *X-Road* (links as of 4/8/21).
31. *Digital Identity*, FATF, March 2020. In 2020, FATF issued specific guidance on the use of digital identity and related verification methods noting, specifically, that remote identification "may even be lower risk [for ML/TF purposes]" than in-person verification. This guidance applies to all regulated financial institutions, including virtual asset service providers (link as of 4/8/21).

32. See *Kiva Protocol*, *X-Road*, *UAE PASS*, *Diia* (links as of 4/8/21).
33. International Finance Corporation, *Blockchain Governance and Regulation as an Enabler for Market Creation in Emerging Market*, EMcompass, Note 57, September 2018 (link as of 4/8/21).
34. *A Guide to Digital Token Offerings*, Monetary Authority of Singapore (MAS), May 2020 (link as of 4/8/21).
35. Ibid; *EU Blockchain Observatory and Forum* (link as of 4/8/21).
36. *Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and Amending Directive (EU) 2019/1937*, European Commission, 24 September 2020 (link as of 4/8/21).
37. Ibid.
38. The classifications are based on assessments of available information. Where information was insufficient to make a determination, countries have been marked as "uncategorized due to insufficient information". The map is designed for simplicity and objectivity, but more complexity may apply in certain cases. Therefore, despite the categorizations given herein, the treatment of cryptocurrencies across jurisdictions remains highly nuanced. You may provide feedback on this regulatory heat map by emailing blockchain@weforum.org.
39. Announced at a virtual lecture attended by a Council member.
40. *UK Regulatory Approach to Crypto-Assets and Stablecoins: Consultation and Call for Evidence*, HM Treasury, 7 January 2021 (link as of 4/8/21).
41. *Second 12-Month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers*, FAFT, July 2021 (link as of 4/8/21).
42. *Crypto-Assets: Work Underway, Regulatory Approaches and Potential Gaps*, Financial Stability Board, 31 May 2019 (link as of 4/8/21).
43. BIS, *Prudential Treatment of Crypto-Assets Exposures*, Consultative Document, Basel Committee on Banking Supervision, June 2021 (link as of 4/8/21).
44. IOSCO, *Investor Education on Crypto-Assets*, The Board of the International Organization of Securities Commission, December 2020 (link as of 4/8/21).

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744
contact@weforum.org
www.weforum.org