The Bretton Woods Committee

No. 4 • OCTOBER 2022

This brief is part of a series produced by the Digital Finance Project Team (DFPT) of the Bretton Woods Committee's Future of Finance Working Group (FFWG)

Investor Protection, Market Integrity, and Financial Stability in Digital Finance

By Richard Berner, Douglas Elliott, and Mahesh Kotecha

"Recent developments in the crypto-asset market have again brought urgency for authorities to address the potential risks posed by crypto assets, including stablecoins more broadly. The recent market disruptions, while costly for many, were not systemic events. But they underline the speed with which confidence can be eroded and how volatile crypto assets can be. Such events could become systemic in the future, especially given the strong growth in these markets and the increasing linkages between crypto assets and with traditional finance."[1]

—Sir Jon Cunliffe
Chair of the Committee on Payments and Market Infrastructure, Bank for International Settlements and Deputy Governor for Financial Stability at the Bank of England

INTRODUCTION

This Digital Finance Project Team (DFPT) brief enumerates the legal, regulatory, and supervisory gaps within the crypto ecosystem and examines what is needed to close these gaps. These include actions needed for consumer and investor protection, market integrity, financial stability, and financial crime prevention. Appropriate governance is also critically important; so much so that this topic will be the subject of a separate brief.

In this brief, after reviewing recent developments in crypto-asset markets, we propose some general principles to guide regulation and supervision of these activities globally. We conclude by identifying the key gaps in existing laws, regulations, and supervision.

Examining how the issues and risks associated with crypto differ from those in traditional financial instruments is critical in developing mitigants and solutions that are fit for purpose. While legal and regulatory clarity is needed, filling the gaps also requires care in crafting laws and regulations that address the novel risks in these new activities.

1 See BIS (Bank for International Settlements), "CPMI and IOSCO Publish Final Guidance on Stablecoin Arrangements Confirming Application of Principles for Financial Market Infrastructures," Press Release, July 13, 2022, https://www.bis.org/press/p220713.htm.

RECENT DEVELOPMENTS IN THE CRYPTO-ASSET MARKETS

Some of the risks, challenges, structural limitations, and misaligned incentives in crypto-asset markets have been vividly on display this year, including the following:[2]

- The collapse in the value of some algorithmic stablecoins such as TerraUSD and Luna, and the spillovers this has generated to other types of stablecoins such as Tether
- Sharp price declines and volatility in non-stablecoin (or unbacked) crypto assets[3]
- Freezing of withdrawals from and/or insolvencies of crypto-asset firms such as Celsius
- Regulatory sanctions for failing to register properly and other rule violations

LAWS, REGULATIONS, AND SUPERVISION

While these examples by themselves make a strong case for regulation, it's important to step back and consider why financial regulation is needed.

The key motivations for regulation in finance are to sustain trust between financial counterparties and to align private and public incentives. Specifically, regulation aims to protect investors and consumers from predation or abuse, to promote market integrity, to support the safety and soundness of individual financial firms and the overall financial stability, and to mitigate financial crime.

In that context, it's worth noting that while examples of market volatility, illicit activities, and fraud crowd the recent headlines about the perils of crypto, the need for regulation is much broader. Informed regulation is essential for businesses to grow and thrive. And it is noteworthy that a lack of clear and predictable regulation is often cited as an obstacle to adoption and success by entrepreneurs and other participants in the crypto space.[4]

Promoting the safety and soundness of financial firms and platforms is a critical case in point: It is essential to build trust in them and, in turn, the financial system by ensuring that they will be able to honor their commitments. That's true for both traditional finance (TradFi) and crypto, but, in contrast to TradFi, the crypto-asset ecosystem currently lacks needed structural safeguards. Disciplining mechanisms need to include laws, regulations, supervision, industry standards, and appropriate governance and culture, recognizing that the specifics may need to be adjusted given the different nature of crypto assets and the activities associated with them.

As with TradFi, therefore, to complement regulation and oversight, industry participants should develop standards for conduct and best practices and appropriate governance and culture to enable and promote good risk management. Risk management practices should mirror those in TradFi in terms of desired outcomes, with appropriate adaptations to account for the unique structures and risks associated with crypto activities.

One important question is whether countries should provide or require a safety net for crypto firms or

---

2 The BIS 2022 Annual Report outlines these: "The Future Monetary System" in *BIS Annual Economic Report*, 75–115 (Basel, Switzerland: BIS, June 21, 2022), https://www.bis.org/publ/arpdf/ar2022e3.htm. The website Web3 Is Going Just Great (https://web3isgoinggreat.com/) provides other examples. See also Jon Cunliffe, "Some lessons from the Crypto Winter" (Speech at Eden Hall, the British High Commissioner's Residence in Singapore, July 12, 2022), https://www.bankofengland.co.uk/speech/2022/july/jon-cunliffe-speech-on-crypto-market-developments-at-the-british-high-commission-singapore; Stephen G. Cecchetti and Kermit L. Schoenholtz, "Crypto Assets and Decentralized Finance: A Primer," *Commentary* (blog), *Money and Banking*, May 13, 2022, https://www.moneyandbanking.com/commentary/2022/5/13/crypto-assets-and-decentralized-finance-a-primer; and Cecchetti and Schoenholtz, "TradFi and Defi: Same Problems Different Solutions," *Commentary* (blog), *Money and Banking*, May 30, 2022, https://www.moneyandbanking.com/commentary/2022/5/29/tradfi-and-defi-same-problems-different-solutions.

3 Federal Reserve Vice Chair Lael Brainard noted the risks of amplification and contagion: "Finally, we have seen how decentralized lending, which relies on overcollateralization to substitute for intermediation, can serve as a stress amplifier by creating waves of liquidations as prices fall." Lael Brainard, "Crypto-Assets and Decentralized Finance through a Financial Stability Lens" (Speech at Bank of England Conference, London, July 8, 2022), https://www.federalreserve.gov/newsevents/speech/brainard20220708a.htm. See evidence of such pro-cyclicality in this activity in preliminary research in Alfred Lehar and Christine A. Parlour, "Systemic Fragility in Decentralized Markets" (Unpublished Paper, June 13, 2022), https://econ.hkbu.edu.hk/eng/Doc/20220616_LEHAR.pdf.

4 See, for example, Liam Akiba Wright, "Coinbase CEO Brian Armstrong Says 'The More Regulation There Is for Crypto, the Better It Is for Coinbase,'" *Cryptoslate*, August 9, 2022, https://cryptoslate.com/coinbase-ceo-brian-armstrong-says-the-more-regulation-there-is-for-crypto-the-better-it-is-for-coinbase/.

activities, as seen in some areas of TradFi. The quid pro quo for the TradFi safety net is supervision and oversight, with transparent reporting to the public. Any contemplation of a crypto safety net should take account of the specific risks and characteristics of the asset or activity, and if established, should include strong safeguards, analogous to those in TradFi, to limit moral hazard.

To understand whether existing financial regulation is fit for purpose for these new activities and ways of doing business, it is important to recognize the similarities and differences between crypto and decentralized finance (DeFi) on one hand, and TradFi on the other.

Many characteristics and risks in DeFi are *similar* to those in TradFi. Among them are

- market, credit, liquidity and contagion risks;
- operational /cyber risks;
- fraud, scams, and illicit activity; and
- opportunities for abuse created by opacity and concentration.

Traditional financial regulation aims to mitigate those risks through disclosure, standards for risk management, firm-level and systemwide resilience built with capital and liquidity requirements, and rules related to firm-level governance and behavior. This is paired with the supervision of financial firms and market infrastructure, deposit insurance, and lender of last resort liquidity provision for those subject to prudential oversight, as well as regular stress testing and recovery and resolution planning for firms that are systemically important. Given the differences between TradFi and DeFi, those tools may need to be adjusted to be fit for purpose in the DeFi arena.

WHAT IS DIFFERENT ABOUT DEFI?

Five key characteristics differentiate DeFi from TradFi:

1. ***Pseudonymity:*** Crypto protocols like bitcoin facilitate the use of pseudonyms for privacy—to shield participants' identity. Transacting in bitcoin and/or creating a bitcoin wallet generates an alphanumeric address that allows sending or receiving bitcoin; only the address (not the identity of the owner) is visible on the blockchain. In TradFi, explicit identification is required by law.
2. ***Transparency:*** Unlike in TradFi, where customer transactions are not published, crypto protocols publish all transactions—albeit with only an address rather than an ID. Although an ID can be linked to an address in some cases, masking tools have been developed to make transactions difficult to trace.
3. ***Lack of legal recourse:*** Crypto protocols lack inherent property rights enforcement, so if your wallet is drained, it is just like losing cash on the street.
4. ***Entity-free transactions:*** Crypto intentionally does not associate transactions with an intermediating entity (excluding validators in protocols like proof of work or proof of stake).
5. ***Irreversibility:*** Transaction errors in crypto cannot be corrected automatically, and because payments are final when transacted, clearance and settlement aren't relevant. So a fat-finger error (typing 10,000 instead of 1,000) is typically not correctable absent human intervention and cooperation from both parties to the transaction.

Those characteristics pose a variety of challenges for regulation. Among them are the following:

- TradFi regulations/laws are ***entity-based***—they focus on firms and people (and, to some extent, markets)—but DeFi is ***activity-based***, so behavior can't be (easily) overseen except through connections to traditional finance, such as the on- and off-ramps used to convert sovereign currencies or bank deposits into crypto or back again.
- ***Regulatory uncertainty*** is currently pervasive and that may undermine trust, facilitate abuse, and discourage use.
- Regulation tends to be embedded in *static rules*, but DeFi is ***dynamic and evolving rapidly***. For instance, a non-fungible token (NFT) may start out as a simple piece of art and later be fractionalized and used as collateral.

- Crypto is ***footloose***—geographic location and jurisdiction are generally unknown and irrelevant, but laws and regulations are locationally specific. Supervision, if needed, and enforcement are thus more challenging than for traditional finance.
- Regulators and supervisors lack expertise and capacity—there is a severe shortage of proper ***staffing and skills*** for crypto onboarding (registration), supervision, and enforcement that is exacerbated by the rapid changes in technology and venues.
- To a greater extent than TradFi, crypto can be used to evade laws and regulations—the pseudonymity, frequent lack of an entity controlling transactions, and the global nature of digital assets mean that crypto is well suited for those who wish to circumvent regulations, including cross-border capital controls, or to engage in illicit activities.

PRINCIPLES

As has been emphasized in earlier DFPT briefs, innovation that meets consumer, investor, and business needs is presumably the raison d'être for the technology and concepts behind crypto/DeFi activities. Equally, as Brief I asserts, we seek "a legal and regulatory regime that promotes safety and resilience while allowing the new technologies and business models to develop and experiment, succeed, or fail."[5] Allowing experimentation and failure should promote the assessment of the benefits, costs, and risks associated with the innovation and the new business models the innovation enables.

Specifically, the following principles are fundamental to meeting that goal:

1. Laws and regulations should support ***responsible*** innovation. Risks should be well managed, but the goal should not be to drive risk to zero.
2. "Same activity, same risk, same disclosure, same mitigation/outcome"[6] will reduce uncertainty and help level the playing field and reduce regulatory arbitrage.
3. Technology-***independent*** objectives, technology-***specific*** tools: regulators should focus on the ***outcomes*** of any particular technology or application and be agnostic about the underlying technology itself.

GUIDELINES

Likewise, some practical guidelines should facilitate translating those principles into actions:

1. Set appropriate standards to protect investors and users and the broader economy and financial system.
2. Use the existing framework and tool kit if they are fit for purpose.
3. Identify gaps and fill them efficiently.

WHAT NEEDS TO BE REGULATED AND WHY?

1. ***Stablecoins:*** Unless they are backed 1:1 by very low-risk assets (e.g., central bank reserves or short-dated sovereign debt) or appropriately overcollateralized, stablecoins will not be completely stable and the chance of a run under stress will be unacceptably high. This is why the President's Working Group recommended limiting stablecoin issuance to insured depository institutions, where it would be treated like bank deposits (i.e., private money). The UK and some in the US Congress are considering other ways of ensuring stability (see Box 1).
2. ***Other crypto assets:*** Not only can the prices of unbacked crypto assets fluctuate significantly, there is often limited or no built-in recourse for retail holders if they are lost through error or theft.

5 William C. Dudley and Carolyn Wilkins, "State of Play in Crypto Markets: Opportunities and Dangers" (BWC Digital Finance Project Team Brief I, April 2022), https://www.brettonwoods.org/article/bwc-digital-finance-project-team-brief-i.

6 Agustín Carstens, "A Level Playing Field in Banking" (Speech at the Institute of International Finance Board of Directors Dinner, Zurich, January 21, 2018), https://www.bis.org/speeches/sp180130.htm; Brainard, "Crypto Assets."

Box 1. Regulation of stablecoins: Proportionate to the risks*

The collapse in the value of some algorithmic stablecoins such as TerraUSD and Luna has undermined trust in other stablecoins. But there are a wide variety of stablecoins with very different risks. Thus, regulation should eschew a one-size-fits-all approach and instead have regulations that are appropriate for the risks. For example, a stablecoin that is backed 1:1 by central bank reserves will, all else equal, be less risky than a stablecoin backed by commercial paper or dependent on algorithmic backing. In the same vein, scale matters. If stablecoins grow to be systemically important, runs and "breaking the buck" could lead to instability in the broader financial system. In this case, the regulatory bar needs to be higher to mitigate such risks.

To distinguish among the types and risks of stablecoins, the Basel Committee on Banking Supervision has proposed a two-part classification framework to assess the risks to banks' crypto-asset exposures based on the principle of "same risk, same activity, same treatment."†

Japan's parliament recently passed a bill on stablecoins, defining them as a form of digital money. Such stablecoins must be linked to the yen or other legal tender and thus guarantee holders the right to redeem them at face value. In order to ensure that, the law requires that stablecoins only be issued by licensed banks, registered money transfer agents, and trust companies.‡

The following criteria distinguishes the different types of stablecoins and indicates what regulatory approach might be appropriate:

Backing	
Fiat currency	**Explicitly backed "payment stablecoins"** §, ¶ Require disclosure of (1) the nature, level, and composition of assets backing targeted redemption value; (2) whether there is full or partial backing; and (3) whether there is contingent support. For issuers of "payment stablecoins," require prudent resources and reporting standards that are proportional to the quality/risk of the stablecoins' backing. Require issuers to disclose their identities and be subject to appropriate regulatory oversight. Some propose that issuers of "payment stablecoins" could be regulated as insured depository institutions (e.g., under a "Federal Stablecoin Platform") with de facto backing of bank reserves.** However, others have noted that deposit insurance backing may not be necessary when there is 1:1 backing by central bank reserves with enough capitalization that the issuer has adequate resources to honor its obligations.
Crypto or algorithms	**Algorithmic or other stablecoins without explicit (fiat currency) backing** Require (1) a clear explanation of the risks involved in the methodology utilized to sustain a stable value; (2) assurance by independent validators about the robustness of its application; and (3) overcollateralization maintenance.

* The President's Working Group recommended limiting stablecoin issuance to insured depository institutions, where it would be treated like bank deposits. US Department of the Treasury, "President's Working Group on Financial Markets Releases Report and Recommendations on Stablecoins," Press Release, November 1, 2021, https://home.treasury.gov/news/press-releases/jy0454. See also G7 Working Group on Stablecoins, Investigating the Impact of Global Stablecoins (Basel, Switzerland: BIS, October 2019), https://www.bis.org/cpmi/publ/d187.pdf and BIS, "CPMI and IOSCO."

† Basel Committee on Banking Supervision, *Second Consultation on the Prudential Treatment of Cryptoasset Exposures* (Basel, Switzerland: BIS, June 30, 2022), https://www.bis.org/bcbs/publ/d533.htm.

‡ See Taiga Uranaka and Yuki Hagiwara, "Japan Passes Stablecoin Bill That Enshrines Investor Protection," *Bloomberg*, June 2, 2022, https://www.bloomberg.com/news/articles/2022-06-03/japan-passes-stablecoin-bill-that-enshrines-investor-protection#xj4y7vzkg.

§ *Payment stablecoins* is the term used in the bill proposed by Senators Lummis and Gillibrand called the Responsible Financial Innovation Act. Ropes & Gray, "Lummis-Gillibrand Digital Asset Bill—Key Takeaways," News Alert, June 7, 2022, https://www.ropesgray.com/en/newsroom/alerts/2022/06/Lummis-Gillibrand-Digital-Asset-Bill-Key-Takeaways.

¶ In the UK, the Financial Policy Committee has set out its expectation that stablecoins used as money-like instruments in systemic payment chains should meet standards equivalent to commercial bank money in relation to stability of value, robustness of legal claim, and ability to redeem at par in fiat. See Financial Policy Committee, *Financial Stability in Focus: Cryptoassets and Decentralised Finance* (London: Bank of England, March 2022), https://www.bankofengland.co.uk/financial-stability-in-focus/2022/march-2022.

** See Howell Jackson, Timothy G. Massad, and Dan Awrey, "How We Can Regulate Stablecoins Now—Without Congressional Action" (Hutchins Center Working Paper 76, Brookings Institution, Washington, DC, August 16, 2022), https://www.brookings.edu/research/how-we-can-regulate-stablecoins-now-without-congressional-action/.

3. ***Trading venues and exchanges:*** Volatility and dysfunction in underlying crypto assets have triggered runs on these platforms and investors have been denied access. They are also subject to operational/cyber risks that can erode market integrity, trigger runs, and endanger investors. Potentially significant conflicts of interest must also be monitored.
4. ***Custodians and wallets:*** Crypto custodians are also subject to runs and to cyber/operational risks.
5. ***DeFi:*** The opacity in DeFi can facilitate exploitation or fraud, resulting in undisclosed conflicts of interest and market manipulation. That this might occur through the autonomous execution of smart contracts makes it difficult for investors and regulators to identify responsible parties and obtain redress.

CRITICAL POTENTIAL GAPS AND HOW TO FILL THEM

Consumer and investor protection: Four key gaps in consumer and investor protection in crypto assets need to be addressed: (1) adequate disclosure, (2) suitability safeguards, (3) cryptocurrency issuer soundness, and (4) digital IDs and Know Your Customer (KYC) enforcement.

Disclosure: In order to weigh risks against opportunities, consumers and investors need strong disclosure of all pertinent risk factors, similar to disclosure in TradFi. Crypto platforms should be required to provide clear and timely disclosure of their key risk factors, risk management processes, the nature and risks of their sponsors, and mechanisms for recourse and remedies on failed or disputed transactions.

Suitability standards: Standards to ensure that high-risk assets can only be purchased by those who understand their risks and are able to absorb potential losses. For example, regulators might limit the acquisition of and risk disclosure for algorithmic stablecoins—or any high-risk asset—to accredited investors and qualified institutional buyers.[7]

Cryptocurrency issuer soundness: As noted above, ensuring the safety and soundness of crypto firms is essential to limiting the potential for losses.[8] While crypto's characteristics will make implementation a challenge, reporting standards should be analogous to those in TradFi for issuers of backed and unbacked crypto assets, as well as for entity identification, limits on ownership concentration, and disclosure of potential conflicts of interest to help forestall "51 percent attacks"[9] and other events that could unfairly disadvantage minority parties.

KYC and digital IDs: Anonymity or pseudonymity can facilitate money laundering and illicit activity, undermine trust in crypto assets, and frustrate tax collection.[10] Global compliance with KYC and anti–money laundering (AML) protocols is thus more challenging than in TradFi, underscoring the complementary need for digital identity across jurisdictions. Proper, secure digital IDs can both protect the privacy of and validate parties to transactions. Unfortunately, agreement on how to achieve both goals in the United States is still lacking.[11] The World Bank is assisting many countries to develop digital IDs under

---

7 In the UK, the Financial Conduct Authority is setting out proposals for strengthening the suitability and disclosure regime for high-risk assets. See Financial Conduct Authority, "Strengthening Our Financial Promotion Rules for High-Risk Investments, Including Cryptoassets" (Consultation Paper CP22/2, January 2022), https://www.fca.org.uk/publication/consultation/cp22-2.pdf.

8 Some unscrupulous promoters engage in so-called *rug pulls*, in which they take in money and then just vanish.

9 An attack on a blockchain by a group of miners controlling over 50 percent of a network's mining *hashrate*—the sum of all computing power dedicated to mining and processing transactions—is called a "51 percent attack." See Griffin Mcshane, "What Is a 51% Attack?" *CoinDesk*, October 12, 2021, https://www.coindesk.com/learn/what-is-a-51-attack/.

10 For example, a bitcoin user typically only needs to specify the destination addresses and the amounts to be transferred. A special piece of software, called a wallet, then decides the (often multiple) addresses from which to send bitcoins to cover a given amount the user wants transferred. A clustering algorithm can group a user's (i.e., a sender's) wallet addresses together. But a user can easily and deliberately conceal the connections between different addresses by making sure that no two addresses used are ever used again in the same transaction. See Igor Makarov and Antoinette Schoar, "Blockchain Analysis of the Bitcoin Market" (NBER Working Paper Series, No. 29396, p. 8, Cambridge, Massachusetts, October 2021), https://www.nber.org/papers/w29396.

11 See Frank Hersey, "US Congressmen Reintroduce Sweeping Digital ID Bill," *Biometricupdate.com*, July 2, 2021. https://www.biometricupdate.com/202107/us-congressmen-reintroduce-sweeping-digital-id-bill.

its ID4D project, though much work is still ahead.[12] Thus, an interim solution is needed until robust and broadly implementable digital IDs are available.

Financial stability: The Global Financial Crisis showed that the so-called *macroprudential* measures are needed to mitigate threats to financial stability of the whole financial system. These can arise when shocks expose systemic vulnerabilities; for example, because one or more firms are so important that their material distress or failure would trigger systemic consequences or because a pervasive activity or systemically relevant market becomes dysfunctional.

Although none of the digital asset businesses or activities are yet of systemic importance, they could grow to be so in the future.[13] And their characteristics create substantial uncertainty about when that threshold may be reached.

The judgment about whether a business or activity was systemic would presumably be based on several factors, including connections with the traditional financial system, importance in payments, leverage of important participants, and the exposure of household wealth. For example, if stablecoins became systemically important for payments, disruptions in their value could lead to payments dysfunction and spillovers to the broader financial system. When such activities have been judged to be systemic, a higher standard of regulation and supervision would be appropriate. This might be similar to the higher capital and liquidity, stress test, and resolution requirements to which traditional financial firms are subject when they are deemed to be systemic.

Of course, authorities cannot and should not simply apply macroprudential *banking* regulation directly to these entities and activities. Instead the principle of "same activity, same risk, same disclosure, same mitigation/outcome" should guide laws, regulations, and supervision for these activities. Substantial further development of the analytical, empirical, and legal foundations for these activities is warranted.

Financial crime: Global financial systems can be exploited by criminals who finance illicit activities, such as human trafficking, transactions for illegal substances, and theft. Terrorism financing is a related challenge. While global KYC/AML rules exist, they are porous. And the pseudonymity of crypto and the fact that not all crypto platforms are subject to KYC/AML regulations make crypto vulnerable to such illicit activity.

The need to strengthen KYC/AML regimes is critical in both DeFi and TradFi. Authorities understand the need to extend the rules to virtual assets and virtual asset service providers (VASPs). Strengthening the FATF guidelines[14] proposed for these instruments and enhancing enforcement of existing rules will be an important first step.

THE CHALLENGE OF ACHIEVING A LEVEL GLOBAL REGULATORY PLAYING FIELD

Crypto—and digital finance generally—is footloose and can potentially operate globally without being domiciled in a particular jurisdiction. In contrast, traditional finance generally requires a financial institution to be locally identified, incorporated, and/or regulated. Ensuring compliance by crypto asset platforms with risk-management requirements and other standards endorsed by global standards setters such as the

12 ID4D is supporting 49 countries and shaping more than US$1.5 billion in financing for the implementation of digital ID and civil registration ecosystems in 35 of the countries. See ID4D, "The ID4D Initiative," About Us, World Bank, https://id4d.worldbank.org/about-us.

13 See, for example, Financial Stability Board, *Assessment of Risks to Financial Stability from Crypto-Assets*, February 16, 2022, https://www.fsb.org/2022/02/assessment-of-risks-to-financial-stability-from-crypto-assets/; Board of Governors of the Federal Reserve System, *Financial Stability Report* (Washington, DC, May 2022), https://www.federalreserve.gov/publications/files/financial-stability-report-20220509.pdf; Brainard, "Crypto Assets;" and Pablo D. Azar, Garth Baughman, Francesca Carapella, Jacob Gerszten, Arazi Lubis, JP Perez-Sangimino, David E. Rappoport, Chiara Scotti, Nathan Swem, Alexandros Vardoulakis, and Aurite Werman, "The Financial Stability Implications of Digital Assets" (Finance and Economics Discussion Series 2022-058, Board of Governors of the Federal Reserve ,Washington, DC, July 2022), https://www.federalreserve.gov/econres/feds/files/2022058pap.pdf.

14 FATF (Financial Action Task Force), *Virtual Assets and Virtual Asset Service Providers: Updated Guidance for a Risk-Based Approach* (FATF, Paris, October 2021), https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf

International Organization of Securities Commissions (IOSCO), the Committee on Payments and Market Infrastructures (CPMI),and the Basel Committee on Banking Supervision is thus a major challenge.

That challenge is more complicated across borders (e.g., for stablecoins) as some jurisdictions may promote regulatory arbitrage and a race to the bottom similar to TradFi activities in less regulated offshore financial centers. Analogously, remedies could include restrictions on those crypto activities that originate in poorly regulated jurisdictions (such as those on offshore banking booking centers for KYC from the Organisation for Economic Co-operation and Development [OECD]). This may require innovations in cyber-blocking technologies, new monitoring and sanctions mechanisms across national jurisdictions, selective waivers of sovereign immunities to allow international examinations and enforcement where necessary, and international coordination.

CONCLUSION

This brief has assessed crypto/DeFi risks and examined how to fill regulatory gaps and provide the necessary mitigants to promote responsible innovation. Global legal and regulatory consistency is needed in order to build trust, promote a level playing field, and limit the regulatory arbitrage to which crypto and DeFi are especially prone. While such activities aren't currently consequential enough to threaten financial stability, they could be in the future. For this reason alone, authorities should begin developing appropriate legal and regulatory frameworks at both the national and the global levels to mitigate the potential vulnerabilities of these activities. The goal must be to ensure that, in the long run, the costs of such activities won't outweigh their benefits.

Future of Finance Working Group

CO-CHAIRS: William C. Dudley and Afsaneh Beschloss

Digital Finance Project Team

CO-LEADS: William C. Dudley and Carolyn Wilkins

Daniela Bassan, Richard Berner, Bill Coen, Larissa Delima, Douglas Elliott, Anthony Elson, Jonathan Everhart, Diana Farrell, Dawn Fitzpatrick, Daniel Gleizer, Daniel Goldman, Michael Greenwald, Sarah Hirsch, Greg Johnson, Mahesh Kotecha, Teresa Kong, Michael Kruse, Kay Lazidis, Caitlin Long, Sultan Meghji, Marsha Vande Berg, Jonathan Padilla, William Papp, Franco Passacantando, Daniel Runde, Jason Schenker, Adam Schneider, Deepika Sharma, Andrew Slack, Heather Smith, Lynn Thoman, Kunal Thakur, Natalya Thakur, Tomicah Tillemann, Peter Tomozawa, Antonio Weiss, Benjamin Weiss

THE BRETTON WOODS COMMITTEE

1701 K St NW #950, Washington, DC 20006

www.brettonwoods.org