The Bretton Woods Committee

No. 6 • APRIL 2023

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)

Deep Dive: Enhancing Market Integrity and Investor Protection in Crypto Asset Markets

By Jonah Crane, Jonathan Everhart, and Antonio Weiss

INTRODUCTION

Crypto market events over the past year demonstrate the risks inherent in an extremely volatile asset class that operates largely outside of existing regulatory frameworks. Turbulence in crypto asset markets in the spring of 2022 led to the collapse of a large algorithmic stablecoin project, which, in turn, triggered a wave of high-profile failures, ultimately including that of FTX, then the world's third-largest exchange. Amid allegations of pervasive fraud, millions of FTX customers were unable to access their crypto assets, and have little recourse in recovering assets that are missing due to mismanagement and malfeasance.

These events have revealed widespread failures in investor protection, risk management, and governance. In response, many policy makers and commentators are calling for more regulatory oversight of crypto asset markets,[1] while others are advocating for further marginalization of crypto assets by keeping them outside the regulated financial system.[2] For its part, the crypto industry has used the FTX collapse to tout the benefits of decentralized finance (known as *DeFi*), whereby market participants maintain custody of their own crypto assets and transact over smart contract–enabled protocols without the overt participation of intermediaries like FTX. At the same time, many in the industry vociferously oppose the regulation of DeFi.

We argue that investor protection and market integrity are foundational public policy goals that should be upheld regardless of whether transactions involve centralized intermediaries or are conducted in a decentralized manner through a web of smart contracts. Since most investment and trading activities in crypto assets closely resemble activities in traditional

[1] Sen. Elizabeth Warren, "Regulate Crypto or It'll Take Down the Economy," *Wall Street Journal*, November 22, 2022.

[2] Stephen Cecchetti and Kim Schoenholtz, "Let Crypto Burn," *Financial Times*, November 17, 2022; Todd H. Baker, "Let's Stop Treating Crypto Trading as If It Were Finance," *The CLS Blue Sky Blog*, November 29, 2022, https://clsbluesky.law.columbia.edu/2022/11/29/lets-stop-treating-crypto-as-if-it-were-finance/.

finance that are regulated, public policy should seek to achieve similar outcomes with respect to crypto exchanges and DeFi.

Crypto assets and the crypto ecosystem have unique characteristics that have resulted in regulatory gaps and made existing regulations difficult to apply.[3] Those gaps should be filled, giving one or more regulators clear authority to oversee crypto asset markets. In addition, regulators and market participants should identify the set of current regulations that cannot easily be applied effectively to crypto assets, and work to propose solutions to ensure that regulatory objectives—including investor protection and market integrity—can be met.

We are not advocating an entirely new regulatory system for crypto assets. That would take too long and increase the risk of abuse from regulatory arbitrage. But changes in technology and market structures mean that simply applying existing regulations to crypto assets may not be sufficient to protect investors and ensure market integrity.

Why regulate at all? Are the critics correct that regulation will bestow legitimacy, compounding the investor harm experienced to date? We doubt the imprimatur bestowed on crypto assets by being brought within the regulatory perimeter will, on its own, make those assets viable. We are still in the midst of an experiment to determine whether and how tokenized value transfer can improve traditional financial intermediation activity.[4] Crypto assets and related businesses may be unable to thrive within a regulated environment and, ultimately, may not facilitate economic activity of social value. But regulators should not base their actions on predictions about the likely outcome of this experiment, and investors should not be exposed to unnecessary risk while the experiment is being run.

IMPROVING INVESTOR PROTECTION AND MARKET INTEGRITY IN CRYPTO PLATFORMS

Investor Protection: Disclosure, Conflicts of Interest, Custody, and Security

Investor protection is a core feature of all well-functioning financial markets. But it has been lacking in many crypto activities and markets because crypto markets have largely operated outside existing investor protection frameworks. The vast majority of token issuers have not complied with the existing registration and disclosure regimes applicable to traditional markets, and few jurisdictions have created bespoke frameworks for crypto platforms.

The important first step is to ensure that all crypto asset market activities are brought within the jurisdiction of appropriate regulator(s). Once that is accomplished, *how* should the crypto asset market be regulated? Regulation should be designed to ensure that investors receive meaningful disclosure about the risks of their investments, are generally treated fairly in the marketplace, and can trust that their assets are being held safely and securely on their behalf.

Disclosure

A core tenet of investor protection is clear disclosure of all material information related to the investment. Many crypto assets do not pose especially novel challenges in this respect—there is typically a core team of developers or promoters who issue tokens to fund the development of a project, with investors betting, in essence, on its success. Applying traditional disclosure requirements to certain crypto assets, including some of the largest such as bitcoin and ether, will require clarifying who the issuer is and what information is material to investors in those crypto assets. For example, the so-called tokenomics of a

[3] For example, tokenized assets enable instantaneous settlement between market participants without the need for account-based settlement through central securities depositories or securities settlement systems. Similarly, existing US Securities and Exchange Commission regulations necessitate the use of transfer agents and require such agents to have the ability to unilaterally amend the official registry.

[4] See Deepika Sharma, Natalya Thakur, Dawn Fitzpatrick, Michael Kruse, and Adam Schneider, "Emerging Digital Finance Ecosystem and Positive Use Cases" (June 2022), Bretton Woods Committee, https://www.brettonwoods.org/sites/default/files/documents/Brief_II_Revised_Final.pdf.

given project or the way in which on-chain governance will be managed are likely to be important but do not fit neatly within existing disclosure requirements.

Nevertheless, these disclosure issues can be solved with some creativity. For example, Christopher Brummer has proposed leveraging technical information widely available to sophisticated participants in crypto asset markets and coupling that with simple, easy-to-read disclosures that draw on long-standing consumer protection principles.[5]

Conflicts of Interest

The structural differences driven by the technical manner in which crypto assets are traded, custodied, and cleared, as well as the vertically integrated organizational structures of the largest crypto asset platforms, are more challenging. All of the large so-called centralized crypto asset trading platforms (e.g., Coinbase, Binance, and previously, FTX) offer a suite of services, including brokerage, trading, order matching, custody, clearing and settlement, lending, and proprietary trading / market making. In traditional securities and derivatives markets, many of these individual functions must be conducted by different entities, each subject to its own set of standards and regulations.

The shortcomings of the current regime have been exemplified by FTX. FTX's affiliated hedge fund, Alameda Research, was the exchange's largest market maker and, unbeknownst to other exchange participants, received an effectively unlimited line of credit from FTX. Even if Alameda hadn't appropriated FTX customer funds, its preferred role at the exchange undermined the integrity of the FTX operation.

The operators of platforms such as Coinbase provide brokerage services to enable retail participants to access their platforms directly. These operators also manage proprietary trading desks that provide liquidity on their platforms and can take the other side of customer trades. Centralized crypto platforms also typically provide custodial services for their customers' assets.

In traditional retail markets, brokerage activities are separated from exchange activities, with brokers obligated to ensure "best execution" for their customers and to segregate and safeguard customer funds. An important question for policy makers is whether the nature of crypto assets *requires* a more integrated market structure. For example, Coinbase asserts that providing instantaneous settlement requires all transactions to settle either on-chain or on the books of the platform. This necessity, in turn, requires each platform to limit access to a single brokerage because brokers must provide custodial services, and having more than one custodian on a platform would prevent instant settlement.[6]

If policy makers do allow more integrated market structures, they will need to ensure that core investor protections are maintained across all of the key functions involved in transactions. Even prior to the collapse of FTX, SEC Chair Gary Gensler was skeptical that investors could be adequately protected if custody and trading operations remained under one roof.[7]

Safeguarding of Customer Assets

FTX also provides a spectacular example of misuse of customer funds. FTX appears to have failed even to accurately track customer assets, let alone segregate and safeguard them as would be required under any effective regulatory framework. Customers reportedly sent $8 billion to Alameda accounts, and Alameda gained control of billions more in customer assets pursuant to a secret and essentially unlimited "credit line" from FTX.

To the extent they are regulated, crypto platforms are typically treated as a form of payment services

[5] Christopher J. Brummer, "Disclosure, Dapps and DeFi," *Stanford Journal of Blockchain Law & Policy* 5:2 (June 2022).

[6] See Coinbase, "Petition for Rulemaking—Digital Asset Securities Regulation" (July 21, 2022), available at US Securities and Exchange Commission, https://www.sec.gov/rules/petitions/2022/petn4-789.pdf.

[7] "Prepared Remarks of Gary Gensler on Crypto Markets" (US Securities and Exchange Commission, April 4, 2022), https://www.sec.gov/news/speech/gensler-remarks-crypto-markets-040422.

business.[8] Such businesses are generally required to "safeguard" customer funds and comply with anti–money laundering laws. However, the requirements on these businesses to safeguard customer funds often do not match the specificity or rigor of analogous requirements applicable to capital markets intermediaries, such as the use of third-party custodians; moreover, the investment restrictions for customer funds are often lax for payment services businesses. Even the New York Department of Financial Services, which is widely considered the most rigorous U.S. state regulator and adopted a bespoke crypto licensing regime in 2014, only recently issued guidance expressly requiring crypto firms under its jurisdiction to segregate customer funds from corporate funds.[9]

As noted by Jay Clayton and Tim Massad, former chairs of the US Securities and Exchange Commission (SEC) and Commodity Futures Trading Commission (CFTC) respectively, the absence of traditional market regulation for crypto trading in the United States means "investor protection rests on state laws written for the telegraph era that are woefully inadequate, particularly when trading and leverage are present."[10]

A notable exception is Japan, where the Financial Services Agency adopted regulations specifically applicable to crypto exchanges, including requirements to segregate customer funds and to safeguard them by maintaining 95 percent in "cold" storage (i.e., storage devices not connected to the internet) and thus not available for immediate transfer. Moreover, the exchanges are required to "self-insure" for the loss of any customer assets held in "hot" (internet-connected) storage and to undergo annual audits.[11] Japan's regulations came in response to two major hacks of Japanese exchanges—Mt. Gox in 2014 and Coincheck in 2018. Customers of FTX Japan reportedly regained access to their assets, albeit over two months following the parent company's failure.

Market Integrity

The global nature of crypto asset trading—across multiple exchanges and jurisdictions with different regulatory frameworks—creates ample opportunity for market manipulation. This is especially true for the thousands of less-liquid tokens.

Crypto markets have been marked by a broad array of scams and fraud. Many crypto assets have been the subject of "pump-and-dump" schemes, reminiscent of the penny stock scams prevalent in the late days of the dot-com bubble, and similar scams known as "rug pulls," in which token creators and protocol developers withdraw a large number of tokens before other participants can (sometimes because they are prevented by the code from doing so). Analysis of global blockchains reveals rampant wash trading both within and across a number of trading platforms, calling into question the true level of liquidity and the legitimacy of price discovery in many crypto asset markets.[12] The vertically integrated nature of crypto trading platforms has also created the perception (and, in some cases, legal allegations[13]) of insider trading.

Crypto asset platforms have instituted the use of forensic tools to identify potentially manipulative behavior. But the robustness of these efforts varies across platforms and has not been tested and verified by independent third

[8] For example, money services businesses operating in the United States must register with the Financial Crimes Enforcement Network (FinCEN) and comply with anti–money laundering (AML) regulations. They typically must also receive money transmission licenses from most states. In the UK, crypto asset businesses are required to register with the Financial Conduct Authority (FCA), principally for the purpose of complying with AML and countering the financing of terrorism (CFT) laws.

[9] New York Department of Financial Services, "Guidance on Custodial Structures for Customer Protection in the Event of Insolvency" (January 23, 2023), https://www.dfs.ny.gov/industry_guidance/industry_letters/il20230123_guidance_custodial_structures.

[10] Jay Clayton and Timothy Massad, "How to Start Regulating the Crypto Markets—Immediately," *Wall Street Journal*, December 4, 2022.

[11] See Tomoko Amaya, "Regulating the Crypto Assets Landscape in Japan," Financial Services Agency of Japan (December 7, 2022), https://www.fsa.go.jp/en/news/2022/20221207/01.pdf.

[12] See, e.g., Lin William Cong, Xi Li, Ke Tang, and Yang Yang, "Crypto Wash Trading" (updated July 2021), available at https://cornell.app.box.com/s/htavb95jr18s6ftd38jigg4l6jeaicjd. Wash trading generally refers to trades in which a market simultaneously purchases and sells the same asset, often to create the impression of trading activity.

[13] Matthew Goldstein and David Yaffe-Bellany, "Ex-Coinbase Employee and 2 Others Charged with Insider Trading of Crypto Assets," *New York Times*, July 21, 2022, https://www.nytimes.com/2022/07/21/business/insider-trading-crypto-coinbase.html.

parties. Moreover, in the absence of voluntary reporting, it is not possible for blockchain analytics providers to match on-chain activity with off-chain transaction data in order to detect potentially manipulative behavior.

Regulatory authorities should require crypto asset platforms to employ real-time monitoring and forensic tools to identify potentially manipulative activity, including activity that takes place across platforms, and to sanction market participants that engage in such activity. DeFi protocols that facilitate entirely on-chain activity without identity verification of participants will be a particular challenge. The anonymous nature of the transactions under such protocols will require sophisticated analysis to identify coordinated trading or the use of multiple accounts to mask an individual's activities.

Security

Both investor protection and market integrity are undermined by the vulnerability of crypto asset platforms and wallets to code exploits and cyber attacks. Flaws or bugs in code are regularly exploited, putting investors' assets at risk. In 2022 alone, roughly 200 exploits led to $3.8 billion in losses. Cross-chain "bridges," developed to enable trading in a specific crypto asset across multiple blockchains, have proven particularly vulnerable. Ronin Bridge was hacked for $625 million in March 2022, and BSC Token Hub was exploited in October 2022, the latter act leading to the creation and withdrawal of 2 million BNB (the native token of Binance, the world's largest exchange) and $570 million in losses. In total, nearly $9 billion has been stolen from crypto networks.[14]

In addition to hacks and exploits, crypto markets have been disrupted by outages in underlying blockchains,[15] flash events on individual exchanges,[16] "fat finger" trades,[17] and cut-and-paste errors.[18] Traditional institutions and exchanges are not immune from these kinds of events, but they have established mechanisms to deal with them, such as trading halts and agreed-upon standards for reversing "clearly erroneous" transactions.

Both hacks and trading halts increase the risks to investors in global markets, where a coordinated resumption of trading is not possible and where transactions are typically irreversible. As discussed in further detail below, attempts to address major hacks have been hindered by an industry that subscribes to the ethos "code is law."

Crypto asset trading platforms and critical intermediary functions should be subject to rigorous information security risk management standards and should adopt business continuity and disaster recovery plans designed to minimize disruptions and protect customers. Platforms could be required to impose minimum security standards, including security audits, on tokens before listing them. These standards should largely mirror those applied to existing traditional financial market participants and, similarly, should be subject to examination by supervisory authorities.

The private sector could also be used to provide complementary security assurances. For example, "bug bounties" could be used to help ferret out vulnerabilities in smart contract code. The industry could also fund research and development to harden security and improve resilience of open-source software.[19]

[14] Based on crypto asset valuations at the time of the theft. When converted to valuations as of December 17, 2022, those losses are approximately $46.5 billion. See https://www.comparitech.com/crypto/biggest-cryptocurrency-heists/.

[15] Danny Nelson, "Solana Halted by Bug Linked to Certain Cold Storage Transactions," *CoinDesk*, June 1, 2022, https://www.coindesk.com/tech/2022/06/02/solana-halted-by-bug-linked-to-certain-cold-storage-transactions/.

[16] Nick Baker, "Bitcoin Crashed 87% on Binance's U.S. Exchange Due to Algo Bug," *Bloomberg*, October 21, 2021, https://www.bloomberg.com/news/articles/2021-10-21/bitcoin-appears-to-crash-87-on-binance-in-apparent-mistake#xj4y7vzkg .

[17] Paul Vigna, "Tether's $5 Billion Error Exposes Crypto Market's Fragility," *Wall Street Journal,* July 16, 2019, https://www.wsj.com/articles/tethers-5-billion-error-exposes-crypto-markets-fragility-11563280121 .

[18] "Cut-And-Paste Error Destroys $36M in Crypto, Eroding Trust in Blockchain" *PYMNTS,* May 6, 2022, https://www.pymnts.com/cryptocurrency/2022/cut-and-paste-error-destroys-36m-in-crypto-eroding-trust-in-blockchain/.

[19] The Bitcoin Security Initiative, launched in 2021 by the MIT Digital Currency Initiative and supported by a number of private sector market participants, funded several core developers over a multiyear period to "improve the robustness of the bitcoin protocol."

IS DEFI THE ANSWER?

The collapse and malfeasance at FTX has caused many to advocate for greater adoption of DeFi. Indeed, the value of crypto assets held in noncustodial wallets increased significantly in the wake of FTX's bankruptcy. The argument is that centralized exchanges have been demonstrated to be the weak link in the crypto world. Given this reality, why not double down on decentralization? This line of reasoning, however, is not persuasive. While decentralized protocols may hold out promise as the underlying rails to support tokenized value transfer, DeFi is not exempt from the challenges in building trust among investors.[20] When DeFi is used to replicate traditional financial market functions, it will have to solve the same investor protection and market integrity problems as centralized intermediaries.

In certain respects, DeFi does address some of the core vulnerabilities that enabled the types of fraud evident at FTX. In DeFi, participants manage their own private keys via noncustodial wallets, thus avoiding the risk that a centralized platform will commingle and potentially misappropriate customer assets, as happened at FTX. The absence of vertically integrated platforms may also reduce the potential for conflicts of interest. However, there is no mechanism to ensure the safety and security of the noncustodial wallets or the code used to operate the decentralized exchanges and other applications used to transact in DeFi. Users are left to fend for themselves and face information asymmetries as daunting and consequential as those that investors in corporate securities, for example, would face in the absence of disclosure requirements. Can investors really be expected to read and understand the code underlying each piece of software with which they interact? If regulation is not extended to DeFi, who is accountable for ensuring that investors' funds are protected against hacks or rehypothecation?

The core investor protection and market integrity challenge in DeFi boils down to a simple question: What happens if something goes wrong?

Smart contracts—the "instructions" that enable transactions to be executed on blockchains—operate deterministically. That is, contracts will execute the task they are programmed to execute when they are triggered. However, smart contracts cannot be programmed to address all (or even many) states of the world. (The glib joke about smart contracts is that they are neither "smart" nor "contracts.") Unexpected and unforeseeable events occur constantly in financial markets,[21] making it impossible for even relatively simple smart contracts to remain robust over time amid changing circumstances. Moreover, smart contracts typically rely on inputs from various external data sources referred to as "oracles"—asset prices, weather events, etc. DeFi markets can easily be gamed where such oracles are vulnerable to manipulation.

Traditional markets rely on a combination of tools to address errors and unforeseen events. Market participants who suffer harm can seek recourse from intermediaries, regulators, and ultimately the legal system. Transactions can be canceled or reversed if deemed to be erroneous (e.g., "fat finger" trades) or otherwise invalid. Market participants who engage in dishonest or fraudulent behavior or violate principles of fair dealing can be held accountable.

DeFi seeks to replace trust in institutions and legal recourse with trust in code, an approach sometimes called "code deference."[22] DeFi participants are expected to defer to the outcome even when the code turns out to have been flawed or hacked. In February 2020, for example, a trader made $1 million on DeFi trading protocol bZx by manipulating an oracle. This type of exploit is analogous to manipulation of financial benchmarks, such as LIBOR. LIBOR manipulation is clearly illegal,

[20] See "TradFi and DeFi: Same Problems, Different Solutions," *Money & Banking* (blog), May 30, 2022, https://www.moneyandbanking.com/commentary/2022/5/29/tradfi-and-defi-same-problems-different-solutions.

[21] Eric Onstad, "LME Forced to Halt Nickel Trading, Cancel Deals, after Prices Top $100,000," *Reuters*, March 8, 2022, https://www.reuters.com/business/lme-suspends-nickel-trading-day-after-prices-see-record-run-2022-03-08/.

[22] For a description of "code deference" and a discussion of its limits, see Andrew Hinkes, "The Limits of Code Deference," *The Journal of Corporation Law* (forthcoming), prepublication version (July 19, 2021) available at SSRN, https://ssrn.com/abstract=3889630.

and institutions have paid significant fines for manipulatory conduct, but the crypto community vigorously debated whether the bZx exploit was illegal or just a case of a trader "outsmarting" poorly designed code.[23]

In many ways, the concept of trust reflected in DeFi's "code is law" ethos is directly at odds with the way trust is maintained in traditional markets and the fundamental way ordinary people tend to think about trust. Code deference is essentially a new version of "caveat emptor."[24] That doctrine resonates in the crypto community but has been abandoned in most markets, especially retail markets, because it tends to *undermine* trust.

The DeFi community does not yet have robust solutions for basic and common challenges, such as how to handle mistaken or clearly erroneous trades, or compromised oracles. There are many flaws with the way traditional markets manage the tools that are used to maintain trust, but by constantly adapting and developing new rules and institutions, policy makers and market participants have largely been successful in developing a financial system able to withstand many types of adverse shocks.

Because DeFi generally does not involve legally identifiable counterparties, questions have also arisen about how legal or regulatory obligations might be enforced. In a recent case, the US Commodity Futures Trading Commission (CFTC) sued Ooki DAO[25] (successor to bZx, target of the oracle exploit described above) for offering unregistered derivatives products. However, it is unclear whether the CFTC has a cognizable legal theory by which it can hold liable the token holders, who are ultimately responsible for how the platform operates.

No code is flawless, and no complex financial market will be robust to all surprises. DeFi will have to develop governance at the protocol level and across the industry to be able to respond effectively to events like those described above and find ways to provide recourse to harmed investors and ensure accountability for those who violate principles of fair dealing. Caveat emptor is not a basis on which to build a large market of retail investors and will not be acceptable to policy makers.

Moreover, policy makers will almost certainly not accept the exemption of DeFi from regulatory standards—the opportunity for regulatory arbitrage is too great. Indeed, the CFTC's case against Ooki DAO arose because the unincorporated association had been organized as the successor to bZx to carry out essentially the same business. In addition, the CFTC and US Department of Justice recently brought parallel civil and criminal actions against a trader for manipulating the price of the native token on Mango Markets, a DeFi protocol.[26] In the press release announcing the case, the CFTC's head of enforcement emphasized that DeFi will be held to the same standards as traditional commodities markets: "The CEA [Commodity Exchange Act] prohibits deception and swap manipulation, whether on a registered swap execution facility or on a decentralized blockchain-based trading platform."[27]

Intermediaries that interact with DeFi will be required to ensure that their own activities are consistent with regulatory expectations, and DeFi protocols that mimic traditional financial activity should be expected to adhere to the regulations that apply to such activity. To date, centralized intermediaries have tended to align themselves with DeFi—perhaps out of sincere sympathy for the crypto ethos or, perhaps, to signal alignment with

[23] Liam Frost, "Was the $1 Million DeFi Hack Illegal or Not?," *Decrypt,* February 25, 2020, https://decrypt.co/es/20512?amp=1. Some DeFi projects have arranged compensation for victims of exploits, but such compensation is discretionary. See, e.g., Ezra Reguerra, "Platypus Finance Creates Compensation Portal for Users Following $9.1 Million Exploit," *Cointelegraph*, March 1, 2023, https://cointelegraph.com/news/platypus-finance-creates-compensation-portal-for-users-following-9-1m-exploit; Sam Reynolds, "DeFi Protocol Ankr to Reimburse Users Affected by $5M Exploit," *CoinDesk*, December 2, 2022, https://www.coindesk.com/markets/2022/12/02/defi-protocol-ankr-exploited-for-over-5m/.

[24] SEC v. Zandford, 535 U.S. 813 (2002). See also Caroline Crenshaw, "Statement on DeFi Risks, Regulations, and Opportunities," *The International Journal of Blockchain Law* 1 (2021) (to quote Crenshaw, "DeFi participants' current 'buyer beware' approach is not an adequate foundation on which to build reimagined financial markets").

[25] CFTC v. Ooki DAO (formerly d/b/a bZeroX CAO), N.D. Cal. (SF Division).

[26] CFTC v. Eisenberg, Case No. 23-cv-00173 (SDNY).

[27] Commodity Futures Trading Commission, "CFTC Charges Avraham Eisenberg with Manipulative and Deceptive Scheme to Misappropriate Over $110 Million from Mango Markets, a Digital Asset Exchange" (CFTC Release Number 8647-23, January 9, 2023).

the "community." As crypto platforms become subject to more comprehensive regulation, however, the gap between their compliance obligations and those applicable to DeFi may become large enough to cause the centralized platforms to advocate for a level playing field.

Ultimately, DeFi is unlikely to remain outside the regulatory perimeter. And the transition is likely to be jarring for those who believe that laws and regulations can be replaced by trustless markets where code reigns supreme.

CONCLUSION

Centralized intermediaries should be brought within existing regulatory frameworks as quickly as possible, with the goal of achieving the same investor protection and market integrity objectives that apply to traditional finance. Where they exist, regulatory gaps should be filled. When crypto asset activities mirror existing financial market activities, existing regulations should presumptively apply. However, regulation should focus on outcomes. When differences in crypto and DeFi activities and market structure would benefit from a different regulatory approach, regulators should be open to adapting regulations to find new, more appropriate means of achieving the same outcomes—as they have for decades.

Ensuring investor protection and market integrity in crypto asset markets will require addressing the dominant business models and market structures that have arisen in those markets and recognizing the inherent limitations in DeFi.

The highly integrated business models of centralized intermediaries operating in crypto markets have led to enormous conflicts of interest. In traditional markets, functions such as brokerage, trading, and custody are independent precisely to avoid such conflicts.

DeFi holds out the promise of transacting without the need to rely on such conflict-ridden intermediaries. However, DeFi's "code is law" regime is rigid and, therefore, fragile. In the absence of regulatory standards and oversight, as well as legal recourse and accountability, DeFi will be incapable of providing the investor protection and market integrity that are hallmarks of well-functioning markets. DeFi is unlikely to flourish as long as caveat emptor is the law of the land.

What will remain of the decentralized utopia envisioned by much of the DeFi community once regulatory standards, governance, and legal recourse are introduced for the protection of investors? That, too, is an experiment with an uncertain outcome.

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

Kofi Appenteng, Daniela Bassan, Richard Berner, Joe Brocato, Marcus Burnett, Bill Coen, Thierry Déau, Larissa Delima, William Dudley, Douglas Elliott, Anthony Elson, Amara Enyia, Jonathan Everhart, Diana Farrell, Dawn Fitzpatrick, Samim Ghamami, Daniel Gleizer, Michael Goldfarb, Michael Greenwald, Sarah Hirsch, Greg Johnson, Zennon Kapron, Elaine Khoo, Chan Kok Seong, Teresa Kong, Mahesh Kotecha, Michael Kruse, Caitlin Long, Rory MacFarquhar, Jesse McWaters, Sultan Meghji, Helena Ooi, Jonathan Padilla, William Papp, Franco Passacantando, Frankie Phua, Daniel Runde, Jason Schenker, Adam Schneider, Deepika Sharma, Raisa Sheynberg, Andrew Slack, Heather Smith, Suan Teck Kin, Natalya Thakur, Kunal Thakur, Lynn Thoman, Tomicah Tillemann, Peter Tomozawa, Marsha Vande Berg, Antonio Weiss, and Benjamin Weiss

THE BRETTON WOODS COMMITTEE
1701 K St NW #950, Washington, DC 20006
www.brettonwoods.org