Legal Studies and
Business Ethics Department
The Wharton School
University of Pennsylvania
600 Jon M. Huntsman Hall
3730 Walnut Street
Philadelphia, PA 19104.6340
215.898.7689 phone
215.573.2006 fax

Kevin Werbach
Liem Sioe Liong/First Pacific Company Professor
Professor of Legal Studies and Business Ethics
Chair, Legal Studies and Business Ethics

Joint Economic Committee

Demystifying Crypto: Digital Assets and the Role of Government

November 17, 2021

Written Statement of Kevin Werbach

Chairman Beyer, Ranking Member Lee, and members of the committee:

Thank you for the opportunity to speak before you today. I am the Liem Sioe Liong/First Pacific Company Professor, and Chair of the Department of Legal Studies & Business Ethics at The Wharton School, University of Pennsylvania. I also direct the Wharton Blockchain and Digital Asset Project. Much of my work involves policy implications of emerging technologies. In the late 1990s, I served as Counsel for New Technology Policy at the Federal Communications Commission. For the Obama Administration, I co-led the review of the FCC for the Transition Team, and then served as an expert advisor to the FCC and National Telecommunications and Information Administration.

For a number of years, blockchain and cryptocurrencies have been a growing focus of my research. I published a book, *The Blockchain and the New Architecture of Trust*, in 2018.[1] Since 2017, I have led workshops bringing together academics, industry legal experts, and regulators from across the federal government, as well as Europe and Asia, to discuss public policy questions around digital assets. My team recently published two reports on decentralized finance in collaboration with the World Economic Forum, *DeFi Beyond the Hype*[2] and *The DeFi Policy-Maker Toolkit*.[3] I created Wharton's blockchain and cryptocurrency course for MBA and

[1] Kevin Werbach, The Blockchain and The New Architecture of Trust (The MIT Press 2018).

[2] Wharton Blockchain and Digital Asset Project, *DeFi Beyond the Hype* (2021), https://wifpr.wharton.upenn.edu/wp-content/uploads/2021/05/DeFi-Beyond-the-Hype.pdf.

[3] World Economic Forum and Wharton Blockchain and Digital Asset Project, *Decentralized Finance (DeFi) Policy-Maker Toolkit* (2021), https://www.weforum.org/whitepapers/decentralized-finance-defi-policy-maker-toolkit.

undergraduate students,[4] and I am academic director of Wharton's forthcoming online executive education program on Economics of Blockchain and Digital Assets.[5]

I. Introduction

You are taking on an important task in seeking to understand the benefits, costs, and regulatory aspects of cryptocurrencies.[6] Blockchain technology, and the decentralized asset ecosystems it enables, could well represent the most important developments in information technology since the internet. Blockchain could be the basis for fundamentally re-wiring the global financial system in beneficial ways, and for re-designing the digital platform economy that impacts the daily life of billions of people.[7] The potential exists to use distributed ledgers and digital assets not only to improve the efficiency of many kinds of transactions, but to make markets more fair, inclusive, open, and transparent.

At the same time, there is no question these same technologies can be—and are—used by criminals, fraudsters, and other bad actors. There are serious risks involved in digital asset-based markets, some of which have already produced large losses for participants. And it is important to distinguish potential from reality. These are still, in many ways, immature technologies. Scalability, security, and interoperability remain huge challenges, especially as adoption grows. There are important questions about energy usage of proof of work networks, which are beyond the scope of this hearing. And blockchain is not the right solution for every problem. In certain situations, blockchains may inspire the incorporation of cryptographic techniques and data structures into fundamentally centralized databases. In others, the traditional architecture is the best one, at least for now.

Finally, while there are many fascinating projects exploring the potential of mechanisms such as decentralized organizations and cryptocurrency payments to enable new kinds of communities, empower individuals, or circumvent authoritarian regimes, the bulk of economic activity around digital assets today is for financial speculation. Holdings of most significant digital assets are highly concentrated, with privileged actors including developers and early investors often

[4] *See* LGST 244x/644x Blockchain and Cryptocurrencies: Business, Legal, and Regulatory Considerations, https://apps.wharton.upenn.edu/syllabi/2019C/LGST644401/.

[5] *See* Wharton Executive Education, Economics of Blockchain and Digital Assets, https://www.blockchain.wharton.upenn.edu/.

[6] As described below, I will primarily use the general term "digital assets," because most of the tokens discussed are not intended to be employed as currencies.

[7] Kevin Werbach, Blockchain: The Last, Best Hope for Open Data, NESTA (September 11, 2020), https://www.nesta.org.uk/report/blockchain-last-best-hope-open-data/.

holding a disproportionate share. And there are major questions about market manipulation underlying the entire digital asset trading market.[8]

Let me be clear. These problems do not mean that digital assets should be dismissed, regulated out of existence, or treated as an inherently noxious development. There is real value being created, in many different ways. The twin revolutions of Satoshi Nakamoto's Bitcoin whitepaper and the smart contract technology of Ethereum have unleashed a Cambrian Explosion of experimentation and innovation. Virtually every major firm in financial services, and most other industries, is now looking at where blockchain and digital assets might provide opportunities to do what they do better, or do new things they cannot do today. And this is a global phenomenon.

It is essential for market participants and policy-makers to see both the positive and the negative aspects of digital assets, so that they can set a course to accentuate the benefits while limiting the harms. Regulation and innovation are not necessarily in conflict. In many cases, regulatory action to address abuses and provide clarity to market participants is an important, or even necessary, condition for long-lasting, productive or transformative innovation. This is not to say that all regulation is well-designed or well-implemented. But we have centuries of evidence that unregulated financial markets produce catastrophic boom-and-bust cycles and severe abuses that undermine their welfare-maximizing potential.

A quarter century ago, I served as a member and editor for the White House working group that drafted the *Framework for Global Electronic Commerce*, a seminal report that set out the United States Government's approach to the emerging phenomenon of the internet.[9] I also wrote *Digital Tornado: The Internet and Telecommunications Policy*, a 1997 Federal Communications Commission working paper that explained how the internet would transform the communications sector and identified the regulatory challenges that would pose.[10] The steps taken by the U.S. Government in the late 1990s facilitated the incredible growth of the digital economy. However, what is important to understand is that the policy adopted then was not that the internet should be a totally unregulated space, or that the harms it brought should be disregarded because of its benefits. While the *Framework* opposed "undue restrictions" on e-commerce, it also identified the need for a "predictable, minimalist, consistent and simple legal environment for commerce."[11] That is what you, and other policy-makers, should be seeking today for cryptocurrencies and digital assets.

---

[8] *See* John M. Griffin and Amin Shams, *Is Bitcoin Really Untethered?*, 75 J. of Finance 1913 (2020); Jacob Silverman, *Is Tether Just a Scam to Enrich Bitcoin Investors*?, New Republic (Jan. 13, 2021), https://newrepublic.com/article/160905/tether-cryptocurrency-scam-enrich-bitcoin-investors.

[9] *See* President William J. Clinton and Vice President Albert Gore, Jr., *A Framework for Global Electronic Commerce* (1997), https://clintonwhitehouse4.archives.gov/WH/New/Commerce/.

[10] *See* Kevin Werbach, *Digital Tornado: The Internet and Telecommunications Policy* (1997), https://www.fcc.gov/reports-research/working-papers/digital-tornado-internet-and-telecommunications-policy.

[11] *See Framework for Global Electronic Commerce* (1997), *supra* note 8.

The central thesis of my book is that blockchain is not the end of trust; it is a new, decentralized form of trust. It is a scary thing to exchange your dollars for a currency issued by no one, or to buy a virtual asset whose value is represented on a decentralized network, or to devote your time and energy to a community whose rules are enforced entirely through software executing automatically on a blockchain. The success or failure of the blockchain economy, or Web 3 as some would prefer, depends on trust. What government does—and doesn't do—will play a significant role in shaping that trust.

II. Regulation of Digital Assets

A. Development of Digital Asset Markets

The digital asset sector has seen extraordinary growth over the last decade. Within the last year alone, cryptocurrency market capitalization has grown fivefold, from $578 billion in November 2020 to $3 trillion in November 2021.[12] Daily trading volume far exceeds $100 billion.[13] There is now a thriving industry of decentralized applications (DApps) enabled through blockchains in a plethora of industries, from finance services to supply chains to fine art. DApps are created using smart contracts, which are a form of software code that executes immutably according to its specified parameters on a blockchain network.

The underlying blockchain market is developing rapidly as well.[14] Bitcoin (BTC) is the oldest and most valuable digital asset, still preeminent in payments and trading, but until recently the Bitcoin network did not offer robust capabilities for DApps.[15] Ethereum, whose native Ether (ETH) token is the second most valuable, is the most popular platform for smart contract and DApp development, especially for decentralized finance (DeFi). Today, Ethereum handles more

[12] *See* Yvonne Lau, *Cryptocurrencies hit market cap of $3 trillion for the first time as Bitcoin and Ether reach record highs*, Fortune (Nov. 9, 2021), https://fortune.com/2021/11/09/cryptocurrency-market-cap-3-trillion-bitcion-ether-shiba-inu/.

[13] Patricia Kowsmann and Caitlin Ostroff, *$76 Billion a Day: How Binance Became the World's Biggest Crypto Exchange*, Wall Street Journal (Nov. 11, 2021).

[14] I focus here on public permissionless blockchains. There are also permissioned networks and consortia built on platforms such as R3 Corda and Hyperledger Fabric. These are important in the enterprise blockchain market, but generally do not create platforms for third-party DApps and publicly accessible cryptocurrencies.

[15] A recent upgrade, Taproot, increases Bitcoin's capability to support smart contracts. There are also platforms built on top of Bitcoin, such as RSK and Stacks, which offer some of this functionality. *See, e.g.,* Arijit Sarkar, *BREAKING: The Bitcoin network welcomes Taproot soft fork upgrade*, Cointelegraph (Nov. 14, 2021).

than a million transactions daily.[16] Over the past twelve months, it has settled more than $6 trillion in transactions.[17]

There are, however, several competing public blockchain networks that claim to improve on Ethereum's functionality, including Solana, Algorand, Avalanche, DFinity, Tezos, EOS, Hedera Hashgraph, and Cardano. Some of these are gaining real developer traction and user adoption due to Ethereum's current performance limitations and high transaction ("gas") costs. And there are many more cryptocurrencies than blockchains; more than ten thousand, in fact.[18] This is because it is easy to create a virtual "token" on top of a smart contract blockchain, leveraging the underlying network security but providing different functionality. The number of tokens has doubled since last year,[19] and the trend is toward further growth.[20]

Of the $3 trillion market value of digital assets, about half is Bitcoin and one-fifth Ether.[21] The term "cryptocurrency" is sometimes limited to tokens that can effectively serve as money, and sometimes limited to the native asset of a blockchain network. The general term "digital assets," or in some international regulatory contexts, "virtual assets," encompasses all such tokens cryptographically secured on a blockchain ledger. Beyond payments, tokens can represent voting rights, for example, for members of a Decentralized Autonomous Organization (DAO) in the form of governance tokens. Other use cases include stablecoins, which can be pegged to less volatile fiat currency or other assets, and Non-Fungible Tokens (NFTs), which can represent anything from tickets that give access to events, to ownership of digital land or unique collectible artworks to even characters in games and digital identities.

Decentralization is a fundamental attribute of blockchains and digital asset or smart contract-based markets. What makes a blockchain different from a traditional database is that no central actor can issue, block, or change transactions on their own. Decentralization is a powerful force for both freedom and economic efficiency. It's the reason this country has thrived with a political system that gives every citizen a vote in electing our government, and an economic system driven by the self-interested actions of independent market participants. However, a more

---

[16] *See* Ethereum Daily Transactions Chart, https://etherscan.io/chart/tx.

[17] *See* Samyuktha Sriram*, Ethereum Settles Over $6 Trillion In Transactions In Last 12 Months*, Benzinga (Oct. 5, 2021), https://www.benzinga.com/markets/cryptocurrency/21/10/23234548/ethereum-settles-over-6-trillion-in-transactions-in-last-12-months.

[18] According to coinmarketcap there are more than 14,000 cryptocurrencies. *See* CoinMarketCap, https://coinmarketcap.com/ (visited Nov. 12, 2021).

[19] *See* CoinMarketCap, https://coinmarketcap.com/.

[20] On the Ethereum blockchain the number of new addresses is increasing daily. *See* Ethereum Unique Addresses Chart, https://etherscan.io/chart/address.

[21] *See* Top 100 Cryptos by Market Cap, OnChainFX, https://onchainfx.com/ (visited Nov. 12, 2021).

decentralized system is not always better; nor is it always desirable. And we don't have a rigorous language for describing what "more decentralized" means in any event.

I would urge you to ignore the simplistic characterizations of blockchains and digital assets as necessarily creating a zero-sum competitor to existing firms, industries, or even governments. We heard this with the internet too. Yet the *New York Times*, JP Morgan, AT&T, and Microsoft are still here, albeit changed in important ways. And of course, the United States of America is still here. The choice we face is not blockchain vs. traditional software, nor is it Bitcoin vs. the U.S. dollar. It is the question of what kind of blockchain-enabled and digital asset-powered future we will experience, and how this new world will interact with and, in some ways, transform the old one.

B. The Regulatory Landscape

Broadly speaking, cryptocurrencies raise three major categories of regulatory consideration:

1. Consumer/investor protection
2. Financial crime
3. Macroprudential and monetary policy

Consumer/Investor Protection

The first category relates to concerns about fraud, market manipulation, deception, information asymmetries, hacks, and excessive or hidden risk. The basic financial regulatory response to these concerns is the registration, disclosure, and market surveillance regime of the 1933 and 1934 Securities Acts. Outside of financial services, agencies such as the Federal Trade Commission take actions against unfair or deceptive trade practices, and the Department of Justice pursues those who defraud consumers or investors. There have been numerous cases where digital asset market participants have been defrauded, had funds stolen, or have suffered catastrophic losses because they took risks they did not understand or could not withstand.

Financial Crime

The digital asset market today is still small relative to the universe of financial asset classes. However, this market is no longer small in absolute terms. The attributes that make cryptocurrencies valuable for legitimate uses also make them attractive for criminals, money launderers, sanctioned nations, terrorists, and others who are appropriately excluded from the global financial system. Over the past decades, a sophisticated national and global regime of anti-money-laundering and countering the financing of terrorism (AML/CFT) rules, as well as industry compliance practices, have been put into place. While highly imperfect, these mechanisms serve important objectives.

Macroprudential and Monetary Policy

Finally, as the size of digital asset markets increases, and instruments such as stablecoins and central bank digital currencies become a greater component of the monetary system, financial policy makers will need to consider them in assessments of systemic risk. They may also need to take into account the impacts that privately issued digital assets have on nations' ability to exercise monetary policy, a topic that has already been raised in connection with Facebook's Libra (now Diem) proposal.[22]

Enforcement Challenges

In the cryptocurrency sector, there are two main problems in applying established rules. The first is categorization difficulty. The securities regulation regime depends on classification as a security or investment contract, for example. Applying the *Howey* and *Reves* frameworks in the digital asset context can be challenging. The second is that blockchain networks are decentralized, global, and typically reference participants through addresses not inherently associated with real-world identities. These factors create practical enforcement challenges even when there are clear cases of harms. Regulators also need to consider the magnitude of harms relative to benefits of unconstrained experimentation, the balance between case-by-case *post hoc* enforcement and prospective rules, as well as whether to take action against those who actively facilitate but may not directly commit violations.

C. U.S. Regulatory Activity[23]

Federal digital asset regulation in the U.S. to date has involved a number of agencies and offices: the Financial Crimes Enforcement Network (FinCEN), Office of the Comptroller of the Currency (OCC), and Internal Revenue Service (IRS) in the Treasury Department, the Securities and Exchange Commission (SEC), the Commodity Futures Trading Commission (CFTC), and the Federal Deposit Insurance Corporation (FDIC). There has also been activity in a number of states, and several bills introduced in recent sessions of Congress, which I will not cover here.

FinCEN classifies virtual currencies as "money" for transmission purposes and in 2020 proposed a rule that would impose recordkeeping, reporting, and customer identity verification requirements on large virtual currency transactions.[24] Recent FinCEN actions have built on the

[22] Ryan Browne**,** *Here's why regulators are so worried about Facebook's digital currency*, CNBC.com (September 19, 2019), https://www.cnbc.com/2019/09/19/heres-why-regulators-are-so-worried-about-facebooks-digital-currency.html.

[23] This subsection is adapted from testimony I gave this summer to a legislative hearing before a committee of the Pennsylvania State Assembly on July 19, 2021.

[24] Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets, 85 FR 83840 (Dec. 23, 2020) (to be codified at 47 C.F.R. pts. 1020, 1022).

precedent of the $110 million fine against the exchange BTC-e in 2017.[25] In addition, FinCEN's enforcement focus has noticeably extended to penalties against individual persons. A pair of prominent enforcement actions have targeted over-the-counter exchange activities by individuals who failed to register with FinCEN, implement an anti-money laundering program, and institute a reporting regime.[26] One of the actions included related criminal proceedings for money laundering of illicitly obtained bitcoin funds.[27]

Similar to FinCEN, the CFTC maintains a broad conception of its regulatory authority—if an active futures market exists for a digital asset, it is within the CFTC's purview. The CFTC has plainly stated that it has standing to regulate bitcoin and other virtual currencies in futures or options contracts, as well as any transactions involving margin financing or fraud.[28] Self-certifications of both the CME and CBOE, as well as a 2018 suit, legitimized this authority.[29] The CFTC has issued three order filings in 2021, including a $6.5 million monetary penalty against the exchange Coinbase for an alleged wash trading scheme.[30]

The SEC's framework for analyzing digital assets is based on the longstanding *Howey* test for classifying securities.[31] A 2018 statement by then Corporation Finance Director Bill Hinman stated that Bitcoin and Ether were sufficiently decentralized that they did not appear to meet the requirements of securities classification at this time.[32] A second functional prong developed following a pair of no-action letters issued by the SEC. The agency has indicated that when a

---

[25] *In the Matter of BTC-E a/k/a Canton Business Corp. & Alexander Vinnik, Assessment of Civil Money Penalty*, FinCEN (July 26, 2017), https://www.fincen.gov/sites/default/files/enforcement_action/2020-05-21/Assessment%20for%20BTCeVinnik%20FINAL2.pdf.

[26] *See* Press Release, U.S. Dep't of Just., '*Bitcoin Maven' Sentenced to One Year in Federal Prison in Bitcoin Money Laundering Case* (July 9, 2018), https://www.justice.gov/usao-cdca/pr/bitcoin-maven-sentenced-one-year-federal-prison-bitcoin-money-laundering-case; *see also In the Matter of Eric Powers*, FinCEN (Apr. 18, 2019), https://www.fincen.gov/sites/default/files/enforcement_action/2020-05-21/Assessment%20Eric%20Powers%20Final%20for%20Posting%2004.18.19.pdf.

[27] Judgment, *United States v. Theresa Lynn Tetley*, No. 17-cr-00738 (C.D. CA 2018), https://storage.courtlistener.com/recap/gov.uscourts.cacd.695757/gov.uscourts.cacd.695757.45.0_1.pdf.

[28] *See In the Matter of Coinflip Inc.*, CFTC (Sept. 17, 2015), https://www.cftc.gov/sites/default/files/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfcoinfliprorder09172015.pdf.

[29] *See CFTC v. McDonnell*, 287 F. Supp. 3d 213 (E.D.N.Y. 2018); *see also* Press Release, CFTC, *CFTC Statement of Self-Certification of Bitcoin Products by CME, CFE and Cantor Exchange* (Dec. 1, 2017), https://www.cftc.gov/PressRoom/PressReleases/7654-17.

[30] *See* Press Release, CFTC, *CFTC Orders Coinbase Inc. to Pay $6.5 Million for False, Misleading, or Inaccurate Reporting and Wash Trading* (Mar. 19, 2021), https://www.cftc.gov/PressRoom/PressReleases/8369-21.

[31] *See* SEC FinHub, *Framework for "Investment Contract" Analysis of Digital Assets* (Apr. 3, 2019), https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets.

[32] *See* Bill Hinman & Valerie Szczepanik, Statement on "Framework for 'Investment Contract' Analysis of Digital Assets," SEC (Apr. 3, 2019), https://www.sec.gov/news/public-statement/statement-framework-investment-contract-analysis-digital-assets.

coin exclusively derives its value through operations on an already developed platform, there is no capacity to achieve investment returns. As a result, the coin functions as a "utility" within the platform and not a security. Few virtual currencies fall within these exceptions and the SEC regards most initial coin offerings (ICOs) as security issuances.[33]

To date, the SEC has issued over seventy enforcement actions against token issuers. Arguably, none are more significant than its 2020 action against the digital platform Ripple. The SEC claimed that Ripple's issuance of the digital token XRP constituted an unregistered securities offering totaling approximately $600 million.[34] The case, which has not yet gone to trial. could clarify the regulatory landscape for virtual currency offerings. New SEC Chairman Gary Gensler recently urged Congress to clarify the SEC's regulatory authority over digital assets, in particular exchanges, claiming the breadth of the industry is outpacing the SEC's purview.[35]

There is a growing emphasis on banking and depository institutions serving as custodians, issuers, or redemption agents for virtual currencies. A series of interpretive letters by the OCC indicates that commercial and savings banks may implement traditional banking services for virtual currency holdings. The FDIC has requested comments on the potential for digital assets to integrate into the activities of financial institutions.[36] The Federal Reserve Board and the Financial Stability Oversight Council (FSOC) are also looking at potential oversight of stablecoins.

Finally, the IRS treats virtual currencies as property for income tax purposes.[37] The IRS has not provided clear guidance on whether certain virtual currencies and positions are commodities under Internal Revenue Code provisions. In the past, the IRS has deferred to the CFTC's classification, and will likely impose commodity tax treatment on virtual currency transactions designated by the CFTC.[38] Following a 2016 report by the Treasury Inspector General, the agency has worked to build a more cohesive policy for addressing tax compliance and

---

[33] *See Oversight of the Securities and Exchange Commission, Before the S. Comm. on Banking, Housing, and Urban Affairs*, 116th Cong. (2019) (statement of Jay Clayton, Chairman, SEC).

[34] *See* Complaint, *SEC v. Ripple Labs, Inc., Bradley Garlinghouse, and Christian A. Larsen*, No. 20-cv-10832 (S.D.N.Y. 2020), https://www.sec.gov/litigation/complaints/2020/comp-pr2020-338.pdf; *see also* Press Release, SEC, *SEC Charges Ripple and Two Executives with Conducting $1.3 Billion Unregistered Securities Offering* (Dec. 22, 2020), https://www.sec.gov/news/press-release/2020-338.

[35] *See Oversight of the Securities and Exchange Commission, Before the Subcomm. on Fin. Serv. And General Govt. of the H. Appropriations Comm.*, 117th Cong. (2021) (statement of Gary Gensler, Chairman, SEC).

[36] *See* Press Release, FDIC, FDIC Issues Request for Information on Digital Assets (May 17, 2021), https://www.fdic.gov/news/press-releases/2021/pr21046.html.

[37] *See* IRS Notice, *Guidance for Individuals and Businesses on the Tax Treatment of Transactions Using Virtual Currencies* (Apr. 14, 2014), https://www.irs.gov/pub/irs-drop/rr-19-24.pdf; *see also* IRS Notice, *Frequently Asked Questions on Virtual Currency Transactions* (Oct. 9, 2019), https://www.irs.gov/pub/irs-drop/rr-19-24.pdf.

[38] *See* New York State Bar Association Tax Section Report, *Report on the Taxation of Cryptocurrency* (Jan. 26, 2020), https://nysba.org/app/uploads/2020/03/Report-1433.pdf.

underreporting of virtual currency transactions.[39] Similar to a 2016 petition filing directed at Coinbase,[40] the IRS has issued a summons demanding the information of consumers transacting large sums on the Circle, Poloniex, and Kraken platforms.[41]

D. Global Regulatory Environment

Significant differences in regulatory approaches to cryptocurrencies exist worldwide as governments grapple with the fast-paced development of the digital asset sector. While El Salvador has made bitcoin legal tender,[42] China banned trading of cryptocurrencies and declared cryptocurrency mining illegal.[43] Other countries have attempted to craft bespoke legal regimes that attract blockchain-based service developers.

Among the most aggressive jurisdictions are Switzerland and Liechtenstein. While Switzerland has amended its existing legislation,[44] Liechtenstein has introduced an entirely new law. Liechtenstein in fact became the first country to comprehensively pass regulation for the token economy, which entered into force in January 2020.[45] The Liechtenstein Blockchain Act allows any right or asset to be tokenized.[46] In September 2020, the Swiss Parliament passed new

[39] *See* Treasury Inspector General for Tax Administration, *As the Use of Virtual Currencies in Taxable Transactions Becomes More Common, Additional Actions are Needed to Ensure Taxpayer Compliance* (Sept. 21, 2016), https://www.treasury.gov/tigta/auditreports/2016reports/201630083fr.pdf.

[40] *See United States of America v. John Doe*, No. 16-cv-06658-JSC (N.D. CA 2017).

[41] *See* Press Release, U.S. Dep't of Just., *Court Authorizes Service of John Doe Summons Seeking Identities of U.S. Taxpayers Who Have Used Cryptocurrencies* (Apr. 1, 2021), https://www.justice.gov/opa/pr/court-authorizes-service-john-doe-summons-seeking-identities-us-taxpayers-who-have-used-0; *see also* Press Release, U.S. Dep't of Just., *Court Authorizes Service of John Doe Summons Seeking Identities of U.S. Taxpayers Who Have Used Cryptocurrency* (May 5, 2021), https://www.justice.gov/opa/pr/court-authorizes-service-john-doe-summons-seeking-identities-us-taxpayers-who-have-used-1.

[42] *See* Nelson Renteria et al., *In a world first, El Salvador makes bitcoin legal tender,* Reuters (June 9, 2021), https://www.reuters.com/world/americas/el-salvador-approves-first-law-bitcoin-legal-tender-2021-06-09/.

[43] *See* Alun John et al., *China's top regulators ban crypto trading and mining, sending bitcoin tumbling,* Reuters (Sept. 24, 2021), https://www.reuters.com/world/china/china-central-bank-vows-crackdown-cryptocurrency-trading-2021-09-24/. There are some indications that the ban on mining may be subject to reconsideration.

[44] *See* Swiss Confederation Federal Act on the Adaptation of Federal Law to Developments in Distributed Ledger Technology of 25 September 2020, https://www.sif.admin.ch/dam/sif/en/dokumente/Blockchain/blockchain_dlt_gesetz.pdf.download.pdf/DLT%20Federal%20Act.pdf.

[45] *See* Press Release, Government Principality of Liechtenstein, *Liechtenstein Parliament approves Blockchain Act unanimously* (Oct. 3, 2019), https://www.regierung.li/en/press-releases/222958/?typ=content&nid=11164. *See* The Token and Trusted Technology Service Provider Act (TVTG), https://www.gesetze.li/konso/2019301000. The English version of the Blockchain Act, including the government consultation report, can be accessed at http://nlaw.li/25.

[46] *Id.*

regulations for blockchain technology, which entered into force in two phases in 2021.[47] The new Swiss DLT Act amends several civil laws, financial market laws, and also securities law to provide a legal basis for trading rights through "electronic registers", as it introduces ledger-based securities that are represented on blockchains.[48] It further introduces special provisions for the treatment of crypto-based assets in case of bankruptcy, and also establishes a new authorization category for DLT trading, a DLT license.

In the European Union (EU), Member States have implemented regulatory requirements relying on guidelines such as the Financial Action Task Force (FATF)'s guidance for virtual asset service providers (VASP)[49] in 2019 and the EU's 5th Anti-Money Laundering Directive (AMLD5),[50] which has been enforced since 2020.[51] AMLD5 requires exchange services between "virtual currencies" and fiat currencies, as well as custodial wallets, to be registered with an EU Member State. Countries such as Gibraltar[52] and Malta have adopted crypto-friendly regimes for VASPs licensing.[53] Gibraltar, for example, in 2017 introduced a tailored license for fintech firms using blockchain technology.[54]

To bring more clarity and provide a harmonious EU-wide approach, the European Commission proposed a new regulatory framework for digital assets as part of the European Union's Digital Finance Strategy. The soon to be ratified proposal for Markets in Crypto Assets (MiCA),[55] aims

---

[47] *See* Press Release, Swiss Confederation Federal Council, *Federal Council brings DLT Act fully into force and issues ordinance* (June 18, 2021), https://www.efd.admin.ch/efd/en/home/the-fdf/nsb-news_list.msg-id-84035.html.

[48] *See* Swiss Confederation Federal Department of Finance, *Digitalisation, Blockchain - Brief Summary*, https://www.efd.admin.ch/efd/en/home/digitalisierung/blockchain.html.

[49] *See* FATF's Guidance for a Risk-Based Approach – Virtual Assets and Virtual Asset Providers, http://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf.

[50] *See* Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L0843&from=EN.

[51] As a directive, it leaves EU countries the freedom to create their own laws to achieve the directive's goals. *See* generally, https://europa.eu/european-union/law/legal-acts_en.

[52] Note that upon UK's withdrawal from the EU, Gibraltar as a British Overseas Territory also ceased to be part of it, but it retains a special status regarding negotiations between the EU and the UK, requiring the involvement of Spain. *See* La Moncloa, Spanish Government on Brexit and resulting consequences regarding Gibraltar, https://www.lamoncloa.gob.es/lang/en/brexit/gibraltar/Paginas/index.aspx.

[53] *See* Sandali Handagama, *Europe's MiCA Crypto Rules Are Coming Soon. Here's Why They Matter,* Coindesk (Nov 2, 2021), https://www.coindesk.com/policy/2021/11/02/unpacking-europes-looming-mica-crypto-regulation/.

[54] *See* Huw Jones, *Gibraltar launches financial services license for blockchain*, Reuters (Dec. 14, 2017), https://www.reuters.com/article/us-gibraltar-regulator-blockchain-idUSKBN1E81JO.

[55] *See* European Commission COM(2020) 593 final, Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593.

to establish a common approach to digital assets beyond the existing rules for securities. Under MiCA, businesses issuing digital assets or serving as VASPs need to acquire a license in one EU Member State, which then becomes valid in all the EU. The proposal includes safeguards to address potential systemic risks, especially in relation to categories of digital assets, such as stablecoins.

In Asia, regulatory approaches vary widely. Japan, which once was home to Mt Gox, the biggest crypto exchange which handled 80% of global bitcoin trading before it went bankrupt due to a major hack, was the first country in the world to define a crypto exchange business in 2017 and legally define "virtual currency".[56] Singapore, considered one of the crypto-friendliest nations and home to many startups, continues to attract crypto related business and already regulates crypto currency exchanges under the Payment Services Act.[57] Whereas in other parts of Asia, such as South Korea and Hong Kong, the cryptocurrency industry is facing new restrictions.[58]

This is not a comprehensive global survey. And there are many details necessary to effectively compare policies across jurisdictions. I describe these global activities in part to illustrate that many other nations, including significant American competitors, are taking the digital asset phenomenon seriously. They are adopting distinctive approaches based on their own policy objectives and existing legal or regulatory structures. The U.S. should do the same.

III. DeFi Regulation

One of the most significant and rapidly growing parts of the blockchain sector is Decentralized Finance (DeFi). DeFi refers to financial services, and associated activity such as price feeds, with three distinctive characteristics: (i) trust-minimized execution and settlement on a permissionless blockchain; (ii) non-custodial treatment of assets; and (iii) software-based implementation that is open, programmable, and composable.[59] DeFi poses particularly acute challenges for regulators and policy-makers. Some of these relate to questions about securities rules or tax treatment for digital assets that have been under discussion and subject to regulatory pronouncements for years. Others are entirely new.

[56] *See* Sygna Blog, *Guide: Japan Crypto Asset Regulation*, https://www.sygna.io/blog/japan-crypto-asset-regulation-guide/.

[57] *See* Monetary Authority of Singapore (MAS) Payment Services Act, https://www.mas.gov.sg/regulation/acts/payment-services-act.

[58] *See* Mercedes Ruehl and Leo Lewis, *Stakes Rise for Singapore's Big Crypto Bet*, Financial Times (Sept. 30, 2021), https://www.ft.com/content/1f948b38-2061-416d-951d-69415b879c17.

[59] *See* DeFi Policy-Maker Toolkit, *supra* note 3 at 21 *et seq*.

A. DeFi Benefits and Risks

Total value locked (TVL) in DeFi, representing the value of digital assets which are committed as liquidity or collateral for DeFi services, went from roughly $1 billion in late 2019, to more than $10 billion in mid 2020, to $110 billion in November 2021,[60] with further growth projected.[61] Centralized cryptocurrency exchanges, such as Bitfinex, have started offering bridges between their custodial trading platforms and DeFi offerings.[62] DeFi developers and others are also looking at ways to connect DeFi with traditional finance (TradFi) institutions and markets. For example, payment processors are partnering with DeFi applications to enable direct purchases of stablecoins,[63] and brokerages are starting to offer clients crypto wallets to access the DeFi ecosystem.[64]

DeFi taps into the desire for an open, inclusive financial system that operates globally. A fully transparent system with no central authority, where users have ultimate control over their assets and can borrow, lend, trade, save and invest freely. The fact that the DeFi ecosystem is fully digital and typically operates on the shared trust infrastructure and standards of a particular blockchain ledger means that services can be modified and combined far more easily than in traditional finance. Increasing the velocity of assets and unlocking potential opportunities to earn yields or obtain capital efficiently has the potential to increase the risk-adjusted returns available to market participants.

As with other digital asset-based markets, DeFi also poses significant risks. In *The DeFi Policy Maker Toolkit*, a collaboration of the Wharton Blockchain and Digital Asset Project and the World Economic Forum, we identified five major categories of DeFi risks:[65]

> Financial: Depletion of funds due to market activity of other users, including rapid price declines, failure of liquidity, or strategic behavior.
>
> Technical: Failures of the software systems supporting transaction execution, pricing, and integrity. These include issues such as smart contract vulnerabilities, poorly written smart

[60] *See* Total Value Locked (USD) in DeFi, https://defipulse.com/.

[61] *See*, e.g., Ethan Wu, *Why DeFi could be an $800 billion industry next year, according to a crypto expert*, Businessinsider (Aug. 19, 2021), https://markets.businessinsider.com/news/currencies/defi-crypto-800-billion-industry-billionaire-decentralized-finance-vesper-2021-08.

[62] *See* Tom Farren, *Bitfinex launches the first L2 bridge from CeFi to DeFi*, Cointelegraph (Sep. 23, 2021), https://cointelegraph.com/news/bitfinex-launches-the-first-l2-bridge-from-cefi-to-defi.

[63] *See* Adrian Zmudzinski, *DeFi Leader MakerDAO Partners With Simplex to Create a Dai Fiat On-Ramp*, Cointelegraph (Mar. 3, 2020), https://cointelegraph.com/news/defi-leader-markerdao-partners-with-simplex-to-create-a-dai-fiat-on-ramp.

[64] *See* Robert Stevens, *Robinhood Crypto COO, CTO Hint That DeFi Features Are Coming*, Decrypt (Sep. 26, 2021), https://decrypt.co/81946/robinhood-crypto-coo-cto-defi-tools.

[65] *See* DeFi Policy-Maker Toolkit, *supra* note 3 at 13 *et seq*.

contracts, failures of price oracles, or failures of the underlying blockchain settlement process.

Operational: Failures of the human systems for key management, protocol development, or governance. These include problems with updates or forks, key management for users and governance participants, and how to resolve disputes.

Legal Compliance: Use of DeFi to engage in illicit activity or to evade regulatory obligations.

Emergent: Macro-scale crashes due to the interaction, scaling, and integration of DeFi components. These risks become particularly worrisome as DeFi services plug into each other, and into traditional financial services markets, with limited visibility into the full set of interconnections.

In some cases, DeFi mitigates risks that are a serious problem calling for regulatory involvement in traditional finance. For example, with fully collateralized or over-collateralized DeFi transactions, there is not the counterparty risk that parties will not actually have the capital they claim to have. Positions are visible on the blockchain, and cryptographically secured. In other cases, DeFi generates risks that have no analogue in the established environment. A software error in a traditional derivatives trade, if identified, can be the basis for legal redress or rolling back a transaction. DeFi is based on immutable execution of smart contracts, which can make even obvious mistakes nearly impossible to fix, unless some anticipatory mechanism is put into place.

DeFi market participants, services such as smart contract auditors and DeFi insurance providers, and regulators are actively working to evaluate and address many of these risk categories. A full discussion of the state of play is beyond the scope of this testimony. More to the point, many of these risks involve the kinds of technical issues best addressed by expert agencies or departments within the scope of their mandate. The question for the Congress is whether, and if so how, to alter the statutory framework.

B. DeFi and Regulating Decentralized Systems

DeFi squarely poses the challenge of how it may be possible regulate decentralized systems. A custodial cryptocurrency exchange has a corporate structure, headquarters, management team, and typically licenses or registrations. A decentralized exchange functioning as an automated market maker (AMM), or other on-chain DeFi protocol, need only be software code in the form of smart contracts running on a distributed blockchain network. If the code allows transactions that violate U.S. law, such as sending funds to sanctioned entities or transacting in unregistered securities, the question arises as to how those regulations could be enforced. No natural person or firm needs to be involved for the code to execute and process a trade. Furthermore, if a regulator wished to take enforcement action, there would appear to be no person or firm to take action against.

While this may sound like an insoluble problem, it is likely to be manageable in practice, if regulators adapt their approaches and focus on the objectives of legal requirements. There are three points of contact that deserve consideration as means of addressing potential regulatory concerns about DeFi: stablecoins, app platforms, and token issuance.

Stablecoins

DeFi services are heavily dependent on stablecoins. This is partly because DeFi, being constructed of smart contracts running on blockchains, cannot directly interface with off-chain payment mechanisms. There is no way to take out a DeFi loan involving traditional U.S. dollars, or interfacing directly with traditional payment rails. Instead, DeFi uses digital assets that are functionally equivalent to those dollars.

The vast majority of stablecoin activity today is associated with centralized stablecoins, most notably Tether (USDT), USD Coin (USDC), and Binance Dollar (BUSD).[66] Facebook's proposed Diem platform, formerly Libra, would also operate in a centralized fashion. Such operators maintain reserves of high-quality liquid assets as backing for the stablecoin. The stablecoin may be manifested as a token on multiple blockchains. However, those tokens are always associated with an identifiable entity that is subject to licensure and regulatory oversight. The exception is Tether, which has an obscure management structure. Tether claims to do no business in the United States, even though it is widely available through U.S.-based exchanges.

Today, centralized stablecoins are not subject to a consistent regulatory framework in the U.S. Some have obtained state money transmission licenses.[67] Others have state trust licenses.[68] Circle has announced plans to become a regulated full-reserve bank.[69] Avanti Bank and Trust plans to launch a stablecoin connected to a Wyoming-chartered Special Purpose Depository Institution.[70] And as noted, Tether, the largest stablecoin by assets, is not currently regulated in the U.S. at

[66] *See* Top Stablecoin Tokens by Market Capitalization, CoinMarketCap, https://coinmarketcap.com/view/stablecoin/.

[67] The USDC Stablecoin's issuer Circle, for example, is regulated by FinCEN as a Money Services Business and holds money transmitter licenses in several states. *See* Circle US Licenses, https://www.circle.com/en/legal/us-licenses.

[68] *E.g.,* Paxos Standard (PAX) and the Gemini Dollar (GUSD) are Trust companies regulated by the New York State Department of Financial Services (NYDFS). *See* Press Release, NYDFS, *DFS continues to foster responsible growth in New York's FinTech industry with new virtual currency product approvals* (Sept. 10, 2018), https://www.dfs.ny.gov/reports_and_publications/press_releases/pr1809101.

[69] *See* Jeremy Allaire, *Our Journey to Become a National Digital Currency Bank*, Circle Blog (Aug. 9, 2021), https://www.circle.com/blog/our-journey-to-become-a-national-digital-currency-bank.

[70] *See* Nate DiCamillo, *Unpacking the Avit, Avanti Bank's New Digital Asset Being Built With Blockstream*, Coindesk (Aug. 12, 2020), https://www.coindesk.com/business/2020/08/12/unpacking-the-avit-avanti-banks-new-digital-asset-being-built-with-blockstream/.

all.[71] The proposed STABLE Act would require all stablecoins to be regulated as banks,[72] while Cornell law professor Dan Awrey proposes that they be treated as money market funds.[73]

Clarifying the regulatory context around stablecoins, and ensuring that they are subject to appropriate obligations, is a critically important step for policy-makers and regulators.[74] A run on a major stablecoin could be devastating for digital asset holders, and could have spillover effects into the larger financial system. Similarly, if the allegations of insufficient backing, fraudulent statements, and market manipulation against Tether turn out to be accurate, it could undermine trust in the entire digital asset trading market, given how deeply embedded Tether is in that market. There are important issues in deciding the proper structure of stablecoin regulation to address these public policy considerations, while not overly restricting innovative activity or excessively compromising Americans' financial privacy. Therefore, I will not advocate for a specific solution here.

Any stablecoin regulatory framework must consider not only investor protection, market integrity, and financial stability, but also the potential role of stablecoins as DeFi onramps and offramps. If stablecoin operators are all treated as a virtual asset service providers subject to anti-money laundering obligations such as Know Your Customer (KYC) rules, that would provide a check that funds entering or leaving the DeFi ecosystem will associated with known, non-sanctioned individuals or entities. It would also provide an aggregation point for law enforcement agencies to monitor activity, with the assistance of sophisticated blockchain analytics tools. While this alone would not eliminate concerns about DeFi being used for criminal activity, it might ameliorate them to a material extent.[75]

---

[71] Tether and Bitfinex were sued by the New York Attorney General and agreed to pay a $18.5 million fee for fraudulent activity. The settlement included a commitment that the entities would cease operations in New York. *See* Press Release, Letitia James NY Attorney General (Feb. 23, 2021), https://ag.ny.gov/press-release/2021/attorney-general-james-ends-virtual-currency-trading-platform-bitfinexs-illegal.

[72] *See,* Stablecoin Classification and Regulation Act of 2020 (US Congress H.R.8827), *https://www.congress.gov/bill/116th-congress/house-bill/8827/text?r=1&s=1. See also* Press Release, Congresswoman Rashida Tlaib (MI-13), Tlaib, García and Lynch Introduce Legislation Protecting Consumers from Cryptocurrency-Related Financial Threats (Dec. 2, 2020), https://tlaib.house.gov/media/press-releases/tlaib-garcia-and-lynch-stableact.

[73] *See* Dan Awrey, Bad Money, 106:1 Cornell Law Review 1 (2020); Cornell Legal Studies Research Paper No. 20-38, https://ssrn.com/abstract=3532681.

[74] *See* Kevin Werbach, *Comments regarding Docket No. OP-1747, Proposed Guidelines to Evaluate Requests for Accounts and Services at Federal Reserve Bank* (Letter, July 9, 2021), https://www.federalreserve.gov/SECRS/2021/July/20210721/OP-1747/OP-1747_070921_138743_356123729916_1.pdf.

[75] There are also stablecoins which operate as entirely smart contracts, rather than through fiat backing. The most prominent of these is MakerDAO, which has $19 billion in assets. There are many others, which either use collateral in the form of digital assets to back the stablecoin or dynamically increase and decrease supply to keep the price stable. Several algorithmic stablecoins have failed to maintain their peg during periods of market volatility or due to deliberate attack, although others have so far managed to avoid that outcome. These on-chain stablecoins raise similar regulatory challenges as DeFi services such as AMMs and lending engines. Although, perhaps ironically,

An open question is whether stablecoin regulations would go beyond sanctions enforcement and standard anti-money laundering checks to, for example, incorporate blacklists of transactions with non-compliant DeFi protocols. Such a move could significantly increase regulators leverage against decentralized DeFi protocols. However, it would also raise concerns about pushing activity to unregulated or offshore alternatives, as well as privacy concerns. The technical and policy aspects of such a step should be carefully considered.

App Interfaces

The second point of potential regulatory oversight for DeFi is the centralized component of major services. While the smart contracts themselves run on decentralized blockchains such as Ethereum, users often access their functionality through traditional websites. For example, Uniswap allows users to trade tokens on its Uniswap.org website, by connecting a wallet such as Metamask. This website is operated by the company Uniswap Labs which employs developers and can make changes to the code. For example, Uniswap delisted approximately 100 tokens in July 2021, including synthetic stock tokens, which would represent unauthorized unregistered securities transactions.[76] Users cannot now trade those tokens through the Uniswap app. They can, however, still send them programmatically to the Uniswap smart contract.

Because Uniswap Labs, the company clearly controls the website and develops the end-user app, it has significant legal exposure to illicit or non-compliant activity they facilitate. Explicit declarations by regulators of their intent to take action against DeFi app providers if they fail to meet certain obligations could therefore have a significant impact, even when the protocols themselves are nominally decentralized. Due consideration should be given to the burdens such obligations would impose, and the possibility that DeFi app providers will either move to another jurisdiction or shift away from a corporate form to a decentralized autonomous organization (DAO) structure. Such steps, however, are not costless, nor do they necessarily eliminate regulators' ability to act.

The significance of platform-targeted enforcement depends on how much activity flows through the website or consumer-facing app, and how much is directly sent through the smart contract.[77] The app interfaces are more user-friendly, and therefore tend to be used by less-sophisticated and smaller-scale DeFi market participants. Most retail investors, even those who express a commitment to the ideals of decentralization, tend to care more about user experience. After all,

---

MakerDAO's collateral has become increasingly dominated by USDC, a fiat-backed stablecoin, which may make it less difficult to address from a regulatory perspective. *See* Dai Stats, https://daistats.com/#/overview.

[76] *See* Martin Young, *Uniswap delists 100 tokens from interface, including options and indexes*, Cointelegraph (July 26, 2021), https://cointelegraph.com/news/uniswap-delists-100-tokens-from-interface-including-options-and-indexes.

[77] Uniswap reportedly has more volume directly through the smart contract than through the consumer-facing app, users can also execute transactions by the interface of other DeFi applications, such as the DEX aggregator 1inch. It is early, however, to make definitive judgements, given how fast the DeFi market is growing and changing.

centralized platforms dominate social media and investment services. A more decentralized system, all things being equal, is usually harder to use, or worse on some other dimension. The slow processing speed and limited capacity of Bitcoin compared to traditional payment networks is an example. There are technical tradeoffs involved in building effective decentralized systems, and mechanisms to hide the resulting complexity from end uses often wind up recreating new points of gateway control. All this suggests that regulation of application platforms—in other words, the more centralized component of DeFi services—could have significant effects, especially for the more vulnerable investors who are a source of particular concern.

The other side of the coin is how sophisticated an institutional actors will respond. There is some evidence that, although there is a significant and active retail DeFi community, including aggressive risk-taking "degens," it is actually dwarfed by institutional-scale activity. The gas costs of every transaction on Ethereum, which is still the dominant platform for DeFi activity, can easily exceed $100, which limits the scope of small-scale trades.[78] Independent of that fact, the kinds of complex capital allocation and yield generation activities that DeFi offers, as well as the opportunity to trade large amounts of assets with limited "slippage" (corresponding price movement), appeal particularly to sophisticated traders. A recent Chainalysis report found that over 60% of DeFi volume was in transactions exceeding $10 million.[79]

On the one hand, sophisticated traders may be better able to, or more interested in, finding ways to transaction without going through central gatekeepers or subjecting themselves to regulatory controls. On the other hand, many of these are regulated actors, or affiliated with regulated institutions. Regulators know who *they* are, and they will not engage in DeFi activities that expose them to major compliance risk. Recognizing how much capital that might flow into DeFi is controlled by institutional actors subject to regulatory obligations, DeFi service have begun to provide tailored offerings that meet their compliance obligations. For example, Aave, one of the largest DeFi lending platforms, has created a separate set of collateral pools, called Aave Arc, which are only accessible to verified liquidity providers that are identified through KYC.[80] Again, the fact that DeFi services are moving in this direction on their own suggests that, as regulators more clearly identify concerns and paths to compliance, major segments of the DeFi market may adapt in ways that make enforcement more feasible.

There will always be some actors in DeFi, and in the blockchain world more generally, who are committed to evading legal obligations. They may do so for strong ideological reasons, because they see significant profit opportunities, or because they provide services to criminals and other

[78] There are ways to keep some transactions off-chain. Scaling solutions for Ethereum, such as sidechains and layer-2 "rollups," as well as alternative blockchains such as Solana and Avalanche with lower transaction costs, may remove this impediment to small-scale DeFi activity. Exactly how and how quickly, though, remains to be seen.

[79] *See* Osato Avan-Nomayo*, Institutional investors dominated the DeFi scene in Q2: Chainalysis report*, Cointelegraph (Sept. 8, 2021), https://cointelegraph.com/news/institutional-investors-dominated-the-defi-scene-in-q2-chainalysis-report.

[80] Tim Copeland, *DeFi Permissioned DeFi platform Aave Arc gears up for launch*, The Block (September 27, 2021), https://www.theblockcrypto.com/linked/118822/permissioned-defi-platform-aave-arc-gears-up-for-launch.

illicit actors (or themselves fit into that category). However, enforcement need not be perfect to be effective. There are non-compliant actors in the traditional financial system as well. Most market participants, especially those seeking to become large and successful, do not aspire to target the market of criminals, terrorists, and sanctioned nations. They want to attract large numbers of users. Those users, in turn, want platforms they can trust. They are used to relying on the protections of legal enforcement and consumer protection measures, rather than hoping for honor among thieves. If the burdens of regulatory compliance are not excessive, therefore, the larger DeFi market participants in particular are likely to accommodate them.

This is true even though blockchains are global. There is increasing coordination among major nations around regulatory approaches to blockchain-based systems, starting with financial crime guidelines under the Financial Action Task Force (FATF). Large financial markets are moving to harmonize their rules—with the exception of China, which is imposing considerably more stringent restrictions on its local digital asset economy. Small countries that seek to attract capital with loose regimes run the risk of being sanctioned or cut off from the global financial system. Again, this process is messy, but fundamentally resembles broader efforts to harmonize requirements for increasingly global financial services activity that have been ongoing for decades.

Token Issuers

A final opportunity for regulatory engagement with DeFi is in the tokens that power these services. Tokens do not appear from nowhere. Once they are issued and accessible through blockchain networks, it may be impossible to point to any entity managing them or controlling their distribution. However, there is always a point in time at which tokens are issued. And there is an entity that structured the token issuance, initiates it, and often promotes it or connects it to other deliberate activities.

The moment of token issuance, therefore, is an important regulatory opportunity. It is the point at which there is likely to be some identifiable actor who must engage with the blockchain and the outside world. The first major wave of enforcement actions against blockchain-based services followed the 2017 boom in Initial Coin Offerings (ICOs), in which developers pre-mined tokens and issued them to raise funds for new applications or networks. Even when a token is not a security subject to registration requirements, however, the point of issuance is still the moment at which it is easiest to assess and implement regulatory obligations.

It is not surprising, therefore, that the MiCA framework under development by the European Union focuses heavily on requirements for token issuers.[81] I am not advocating that the U.S. take exactly the same steps as Europe; there are issues with the MiCA rules and the overall legal framework is somewhat different. However, it is a model that bears studying on this side of the Atlantic.

[81] The other major category in MiCA are virtual asset service providers, primarily for financial crime prevention.

C. The File-Sharing Analogy: Intent Matters

In considering novel developments such as the rise of blockchain and digital asset markets, it is often helpful to look back to historical analogies. In the case of DeFi, important precursors are the rapid rise—and equally rapid fall—of peer to peer (P2P) file sharing applications. While the story is a familiar one in technology circles, the legal resolution of the P2P file-sharing challenges is not as well remembered. And it turns out to be directly relevant to DeFi.

P2P file-sharing threatened to undermine the economic foundations of the music industry, and other media industries as well…or perhaps merely to transform them. It all started with Napster, written by college student Shawn Fanning, and launched in 1999. Within a few months, Napster had more than 20 million downloads and 4 million songs in circulation.[82] These are astronomical numbers considering how much smaller the internet was at that point. App store ecosystems, or even smartphones, did not exist, and most internet users were still on dial-up connections over the telephone network. Napster and other P2P file-sharing applications took off primarily because they allowed people to access commercially-released music for free. At the time, the only way to purchase recorded music was on physical media such as CDs. Streaming was negligible and record labels refused to license online distribution of songs. With Napster, a user could freely download any songs shared by other users of the peer-to-peer network. The music industry saw it as an existential threat.

Napster posed an issue similar to the one we now face with DeFi: how to regulate decentralized activity? The legal issue in the earlier case was copyright infringement rather than financial regulation, but the structure of the problem was the same. Napster itself did not distribute any music. It did not store any music on its servers. It did not create or control the network through which users traded music. It merely distributed software, which connected itself to a dynamic decentralized network by finding other users of the software online at the same time. Napster and its defenders argued that Napster was not, in fact, contributing to infringement; it only provided a neutral tool that could be used to exchange any files of the user's choosing.

The record industry sued Napster, and the case went to the United States Court of Appeals for the Ninth Circuit.[83] Napster lost. The court found that even though Napster did not itself store or transfer music files, Napster maintained a central database of all content accessible on the network at any time. Napster users contributed their own list of files automatically to this database, which other users referenced to identify what was available where. As a result, Napster knew exactly what was being traded on its network. It could clearly see that the vast majority of the activity involved illicit sharing of licensed content. Furthermore, Napster was essential to this activity. Without the dynamic database that Napster maintained, the file sharing network could

[82] *See Napster: 20 million users*, CNN Money July 19, 2000), https://money.cnn.com/2000/07/19/technology/napster/index.htm.

[83] *See* A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001).

not operate. In other words, Napster was essentially a DINO—decentralized in name only. It effectively maintained control of essential elements of the network, and therefore could be held legally responsible for the network's activity/ Napster was quickly shut down.[84]

There are today similar DeFi services that are decentralized in name only. Some of these simply associate with the name DeFi for marketing reasons, without having any real decentralization compared to more established services. DeFi Money Market (DMM), for example, was styled as a centralized lending pool that would aggregate participants' capital and pay them interest.[85] It was in fact a fraud. Even as described, however, DMM was centralized: the operator of the pool controlled all the assets. The SEC had little difficulty taking action against DMM.[86]

There are likely to be many more DeFi services that are similarly centralized in practice, or that maintain a significant amount of central control. The SEC in 2018 took action against EtherDelta, an early decentralized exchange (DEX).[87] EtherDelta, like today's DeFi AMMs, did not take custody over users' assets. However, it was controlled by a single developer who controlled the order book, listings, and access to the system. The SEC had little difficulty going after EtherDelta for impermissibly trading unregistered securities.

The more interesting parts of the P2P file-sharing story are what happened after Napster. Newer file-sharing applications architected themselves to remove the central control point that doomed Napster. These apps, most famously Kazaa but also including Grokster, LimeWire, and others, built up the database of available songs in a decentralized way, through direct communications between users' software. There was no central database, and therefore the application developer could not directly see what users were transferring. Nor could the app distributor blacklist certain files. It had no direct control.

Nonetheless, the distributed P2P file-sharing services also lost in court. In *MGM v. Grokster*, the Supreme Court concluded that they were, like Napster, legally responsible for the activity on their network.[88] The legal theory in this case was that, even though these services did not see or allow each individual infringing transfer, they knew and encouraged the creation of a marketplace that was dominated by infringement. In other words, Grokster and Kazaa "induced" the illegal activity. Their marketing materials, business models, internal communications, and the

[84] The service had a second life as a tool for licensed music distribution, but never regained its prior success.

[85] See Gregory Keough et al., *DeFi Money Market Ecosystem – Earn Interest on Digital Assets Backed By Real-World Assets Represented On-Chain*, Whitepaper (Feb, 2020), https://defimoneymarket.com/files/DMM-Ecosystem.pdf.

[86] See Press Release, SEC, *SEC Charges Decentralized Finance Lender and Top Executive for Raising $30 Million Through Fraudulent Offerings* (Aug. 6, 2021), https://www.sec.gov/news/press-release/2021-145.

[87] *See* Press Release, SEC, *SEC Charges EtherDelta Founder With Operating an Unregistered Exchange* (Nov. 8, 2018), https://www.sec.gov/news/press-release/2018-258.

[88] *See* MGM Studios, Inc. v. Grokster, Ltd., 545 U.S. 913 (2005).

obvious evidence of the market dynamics made clear that the file-sharing applications developers were not just innocent bystanders.

Further reinforcing this test, there was no legal action taken against BitTorrent, a P2P file-sharing protocol optimized for distribution of video. Even though at one point upwards of one third of all internet traffic globally involved BitTorrent transfers,[89] and most of them were not licensed by the content owners, BitTorrent the company did nothing to induce such activity. It merely disseminated open-source software. Its own business was built around offering content owners the ability to distribute licensed video with protections against infringement.[90]

The important point here is that the "why" of activity matters. Even when not explicitly spelled out in the laws or regulation, intent is a significant factor that regulators and enforcement agents consider in deciding whether to take action, and that courts consider in resolving cases. This is relevant in the blockchain context as well. For example, an alarmist study found that the code for child pornographic images, in text form, had been embedded in the Bitcoin blockchain, and suggested that miners might be subject to criminal prosecution for possessing such material.[91] No such prosecutions have occurred. Law enforcement officials understand the distinction between actors who contribute to the scourge of child sexual abuse and those, who through no fault of their own and with no ability to remove it, happen to store data that could theoretically be reconstructed into an illicit image.[92]

One of the important questions for DeFi services will be why they decentralize. There are many legitimate reasons to do so. Decentralization removed power from intermediaries who extract rents, making services cheaper and more broadly accessible. It can make services more efficient while also making them more inclusive and equal. It can make systems more robust and secure, while drawing powerfully on the contributions of more participants. In these cases, the regulatory challenges DeFi poses are unintended side effects. In other cases, however, such as the Kazaa/Grokster architecture, decentralization is a deliberate means of avoiding legal obligations. If breaking the law is the primary benefit of decentralization, which otherwise creates difficulties for the service, it is fair to ask whether regulators should defer action in the name of "innovation." Certainly, there will be many cases where intent is not obvious. That should not prevent use from identifying those where it is.

---

[89] *See CacheLogic says 35% of all Internet traffic is now BitTorrent*, ZDNet (November 4, 2004), https://www.zdnet.com/article/cachelogic-says-35-of-all-internet-traffic-is-now-bittorrent/.

[90] Ironically, the BitTorrent company was eventually purchased by Tron, a blockchain network. *See* Ingrid Lunden, *BitTorrent is selling for $140M to Justin Sun and his blockchain startup Tron,* TechCrunch (Jun. 18, 2018), https://techcrunch.com/2018/06/18/bittorrent-tron/.

[91] *See* Hamza Shaban, *People are using bitcoin's system to share child pornography, researchers say*, The Washington Post (Mar. 22, 2018), https://www.washingtonpost.com/news/the-switch/wp/2018/03/22/people-are-using-bitcoins-system-to-share-child-pornography/.

[92] *See* Kevin Werbach, Arvind Narayanan and James Grimmelmann, *Why Porn on the Blockchain Won't Doom Bitcoin* (Wired Online, March 29, 2018), https://www.wired.com/story/why-porn-on-the-blockchain-wont-doom-bitcoin/.

IV. Recommendations

The rise of digital assets, and the overlapping trends increasingly described as Web 3, is not a fad. These are volatile markets that have crashed before and will crash again. There is a good deal of irrational exuberance in the current crypto market, or rational exuberance about short-term speculative profits that are nonetheless not sustainable or generalizable. And as detailed earlier, there are serious risks and abuses associated with cryptocurrencies which policy-makers must address. None of this, however, calls into question the basic value proposition for blockchain as a foundational technology and digital assets a means of powering financial and other services.

Congress should take a three-pronged approach to the regulatory questions that cryptocurrencies raise. This is in addition to the normal oversight process for the various agencies addressing issues under their jurisdiction, and coordination with the Executive Branch. The three components of an effective approach are capacity building, addressing "low hanging fruit" aggressively, and engaging in a long-term examination the existing financial regulatory legal regime.

A. Capacity Building

The first step is to recognize that cryptocurrencies and blockchain pose thorny new challenges which regulators may be ill-prepared to address. There are also important questions relevant to the future of DeFi and other digital asset-based markets where even experts in the industry do not have good answers. Steps should be taken to improve the state of knowledge, and where possible to provide breathing space and help policy-makers gain a greater understanding of market dynamics.

One part of this step is to ramp up public research and development efforts, as well as experimentation by government agencies with blockchain-based solutions. There are many important research questions related to blockchain and cryptocurrencies that have not been subject to sufficient academic attention, especially regarding the business and financial dynamics rather than purely the computer science foundations. Public funding of research and government operating as a convenor of public sector, private sector, and academic experts should both receive higher priority, given the potential importance of digital assets and blockchain.

Other countries provide significant support for research and development in this area. For example, the European Union has funded blockchain research for several years through its Horizon 2020 initiative, as well as other mechanisms.[93] The EU Blockchain Observatory and

[93] *See* European Commission on Shaping Europe's digital future, Blockchain funding and investment, https://digital-strategy.ec.europa.eu/en/policies/blockchain-funding.

Forum[94] and European Blockchain Service Infrastructure[95] are convening experts, developing standards, and coordinating responses to important issues. Chinese officials often describe blockchain as part of the country's "New Infrastructure" strategy, along with other strategic technologies such as 5G wireless and artificial intelligence.[96]

At the same time as government supports external research, agencies need to build the internal capacity to address tricky cryptocurrency-related questions effectively. Some mechanisms that have proven effective in similar contexts include:[97]

Specialized regulatory units. A targeted group with qualified staffing, such as the SEC's FinHub, can serve as an initial gateway to gain experience in new technology, interact with the industry and provide guidance. This knowledge can be shared with policy-makers and actions may include issuing non-action letters under existing regulatory regimes.

Incentivizing information flow. Disclosure is one of the most common tools of financial regulation. Even when the applicability of existing disclosure requirements on DeFi platforms is uncertain, efforts to encourage broad and consistent information disclosure may prove fruitful for regulatory analysis.

Regulatory sandboxes. Policy-makers may decide to establish regulatory forbearance programs such as sandboxes, where companies may test and operate their technology in a limited scope and therefore with limited regulatory risks. The sandbox gives start-ups a chance to address regulatory compliance concerns and gives regulators a better understanding of the risks and benefits of a new space.

Coordinating government action. In some cases, it may be useful to bring together different government entities for a harmonized response. Such efforts are already underway, through vehicles such as the President's Working Group on Financial Markets, the Financial Stability Oversight Counsel, and the digital asset policy "sprint" between the OCC, FDIC, and Fed. More coordination will likely be valuable, however, including coordination with state authorities and regulators outside the U.S.

This list is not intended to be comprehensive. Nor does it presuppose any policy outcomes. The point of all the ideas listed in this section is to improve both the process and the substance of regulatory engagement with blockchain and digital asset firms, whatever direction that engagement takes.

---

[94] European Commission initiative EU Blockchain Observatory and Forum, https://www.eublockchainforum.eu/.

[95] European Commission on Shaping Europe's digital future, European Blockchain Services Infrastructure, https://digital-strategy.ec.europa.eu/en/policies/european-blockchain-services-infrastructure.

[96] See Jane Wu, *Blockchain as an Infrastructure: A Deep Dive Into China's DLT Strategy,* Cointelegraph (Jun. 23, 2020), https://cointelegraph.com/news/blockchain-as-an-infrastructure-a-deep-dive-into-chinas-dlt-strategy.

[97] This list is derived from a section of the DeFi Policy-Maker Toolkit, *see supra* note 3.

B. Short-Term: Low-Hanging Fruit

The blockchain sector is developing and growing fast. Some needed policy actions do not require significant gestation and debate; they should be adopted as quickly as possible.

First, there are a number of situations where laws and regulations were written with language that fails to effectively accommodate digital assets and the distinctive features of blockchain-based systems. These are generally situations of un-intended consequences. Unclear or ill-fitting statutory language creates impediments for market participants that do not service any public policy objective.

In preparation for this testimony, I surveyed several legal experts from different areas of the digital asset space, and asked them what "low-hanging fruit" Congress could address in the near term. The following is a non-exhaustive list:

- The Infrastructure Investment and Jobs Act includes language classifying digital asset service providers as "brokers" subject to IRS reporting requirements. As drafted, it could cover actors, such as cryptocurrency miners, who have no means of complying and do not function as intermediaries targeted by the language. A bipartisan amendment was offered to address this oversight. Despite no direct opposition, it was not included in the final bill.

- The Infrastructure bill also included language incorporating digital assets into Section 6050I of the Internal Revenue Code, which requires those making transactions over $10,000 in their "trade or business" to report the counterparties' social security number and other personal information. Without clarification or narrowing, this could sweep in a great deal of transactional activity that does not require reporting in the analogous situation involving traditional assets.

- Under current IRS guidance, any cryptocurrency transaction, even for payments, can constitute a taxable event. A *de minimis* exemption has been proposed in multiple sessions of Congress, but has not been adopted.

- Section 409A of the Internal Revenue Code provides exemptions for compensation involving "service recipient common stock" and "incentive stock option" plans, but does not appear to address the equivalent scenario in which compensation is provided on a deferred and scheduled based in the form of tokens.

There are other areas which, though somewhat more complicated, call for rapid action to resolve significant market uncertainty or address under-regulated activity. I have already mentioned one: implementing a consistent regulatory structure for stablecoins. Others include:

- Allocation of authority over digital assets between the SEC and CFTC, given the ambiguity of when these assets function as securities, commodities, or something else, and the confluence of spot and derivatives markets.

- Clarity on the definition of a qualified custodian for digital assets. Custody of digital assets is very different at a technical and operational level from custody of traditional financial assets. However, the market has become far more sophisticated in custody solutions than a few years ago.

- A pathway for a digital asset firm to gain broad access to the banking system, FDIC insurance, and payments networks, including Federal Reserve master account. There are many appropriate reasons for banks and bank regulators to be concerned about risks of digital assets. That does not mean that mechanisms for addressing those risks can never be identified.

At the same time such efforts are underway to facilitate legitimate digital asset activity, significantly stronger action must be taken against the bad actors. There is no reason for firms to make efforts to comply with the rules if they see that others who demonstrably do not suffer no ill consequences. Put simply, there is a great deal of obvious fraud and regulatory avoidance in the blockchain world. There has been for some time.

While a few fraudulent actors have been subject to enforcement actions, many have not. Limits on enforcement resources and the difficulty of successfully bringing cases are certainly part of the explanation. It is infeasible to pursue every case that appears to involve illicit activity. However, regulators and law enforcement should prioritize large and visible cases of fraud and theft, and seek to set examples. If funding is the limiting factor, the Congress should consider additional appropriations.

At the same time as action is taken against the obvious bad actors, investigative resources should be devoted to the large players in the blockchain ecosystem who have been credibly accused of market manipulation, such as Tether and Binance.[98] Most of these purport not to operate in the U.S.; some claim to have no headquarters at all; others shift between jurisdictions whenever questions are raised about their activities. Any enforcement action will therefore require significant cooperation with foreign law enforcement authorities. The effort is worth it. In the current environment, regulated U.S.-based actors transact with, and apparently derive significant benefits from, these offshore entities. In other situations, individual and firms take steps to nominally remove themselves from the U.S., while still enjoying the benefits of citizenship and easy access to U.S. capital markets.

[98] It is for regulators and law enforcement to decide whether these allegations are accurate. I raise them to note that they are long-standing and not unsupported by available evidence. *See supra* notes 8, 71. Furthermore, even if cryptocurrency markets do not constituted trading in securities, that does not mean that market integrity concerns should be ignored.

Such conduct blurs the distinction between compliant and non-compliant service providers, and calls into question the integrity of the entire market. It may turn out that, after investigations, there is smoke but not fire. If that is the case, termination of investigations should help bring confidence to the market. If, on the other hand, even a portion of the allegations of systemic manipulation are true, many investors and other market participants are being taken advantage of, at massive scale. And it is only a matter of time before the shell game ends, with potentially disastrous consequences.

C. Re-Thinking Financial Regulation

Long-term, I do not think we can escape from the conclusion that blockchain and digital assets, along with other fintech developments, will contribute to a fundamental reshaping of our financial markets, and have major impacts in many other domains.

The fact that the relevant laws and, in many cases, judicial decisions establishing common-law doctrines, are decades old, is not itself a problem. We venerate the Constitution because its broad language can be interpreted to address issues the Framers themselves would never experience. It makes no sense to adopt new laws, and narrowly tailored laws, for every significant technological change. Laws and rules that are technology-specific tend to advantage or disadvantage one technological approach, which should not be the role of government, and quickly become outdated as newer technologies emerge.

However, there are situations where laws or regulatory structures do need to be re-evaluated. There is broad consensus, for example, that the accredited investor regime is an increasingly poor fit for the current investing environment, a problem that digital assets magnify. More generally, information disclosure, the centerpiece of the securities regulatory structure, means something different in a blockchain context where all transactions are transparent and cryptographically guaranteed although interpreting the transaction data and associating it with market participants may be more challenging than in traditional finance. And the highly fragmented financial regulatory structure that is almost entirely unique to the U.S. deserves a closer look in an era of digital convergence. A structure of multiple specialized agencies has benefits, but it also creates opportunities for regulatory arbitrage and confusion.

In 1996, after several years of effort, Congress passed the Telecommunications Act, which rewrote the outmoded Communications Act of 1934. There are many problems with the 1996 Act, not the least that it failed to anticipate how important the internet would become in the communications, media, and technology sectors. However, we would be worse off trying to regulate today under the old law, which could barely be stretched to cover cable television. At some point, frameworks that poorly fit new technologies are, in effect, no longer technology neutral.

The re-think I am describing will take time. It will address many issues beyond blockchain. Some of the necessary changes are along the lines of the previous section, going more to clarifying language for a new context than changing the basic regulatory structure. Others,

however, are deeper. The exercise of identifying high-level public policy goals, studying best practices for addressing them, balancing competing interests, and setting forth a modern framework will produce benefits in itself. And if successful, it could position the U.S. to maintain its leadership in the global financial system as it moves through its next technological transition.

V. Conclusion

I have attempted to set out a series of actions that Congress, agencies, Executive Branch Departments, and the Federal Reserve could take to address the dangers of cryptocurrencies and digital assets while both recognizing and facilitating their benefits. This list is not comprehensive; nor does it entirely represent a divergence from current approaches. There is significant activity underway in individual agencies and through coordination efforts such as the President's Working Group on Financial Markets. Legislation has been introduced in many of these areas, and other legislative proposals are no doubt under development.

Perhaps the most important point to make is that, for all the rhetoric about how the U.S. is losing out to more tolerant jurisdictions, or to China's aggressive state-led central bank digital currency, the reality is that America is one of the largest and most important markets for development of blockchain technology and activity in the digital asset economy. Many of the key development teams and companies are based in the U.S. or have significant presence here. That is true of an even larger percentage of the investment and market activity. The U.S. is the most sophisticated and most advanced capital market in the world, and also the home of a large percentage of the world's most important technology firms. The factors that have put the U.S. in such a prominent position do not disappear in the blockchain world. While it is true that the global nature of blockchains and their ability to remove barriers to participants allows individuals from anywhere in the world to contribute, that is a dynamic leading U.S.-based firms have taken advantage of for a long time.

Of course, we cannot assume that the U.S. will always and automatically be a leader on the blockchain sector, or any other sector. China's multi-pronged efforts to develop blockchain as a strategic technology and to bend digital assets into a state-superintended environment should not be dismissed. Nor should initiatives in Europe and in jurisdictions such as Singapore, Japan, Russia, and elsewhere be ignored. We need to do what worked so successfully in the early days of the commercial internet: articulate policy goals; clarify where uncertainty is an unnecessary check on innovation; take action where it is warranted; and adapt both our policy tools and our legal structures to take into account the deep changes underway.

There are many hard questions still to resolve, and many pieces to the blockchain regulatory puzzle. That should not stop us from moving forward to realize the incredible potential that digital assets and blockchain present.