S. HRG. 117–151

DEMYSTIFYING CRYPTO: DIGITAL ASSETS AND THE ROLE OF GOVERNMENT

HEARING

BEFORE THE

JOINT ECONOMIC COMMITTEE

OF THE

CONGRESS OF THE UNITED STATES

ONE HUNDRED SEVENTEENTH CONGRESS

FIRST SESSION

NOVEMBER 17, 2021

Printed for the use of the Joint Economic Committee

Available via the World Wide Web: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE
46–819 WASHINGTON : 2022

JOINT ECONOMIC COMMITTEE

[Created pursuant to Sec. 5(a) of Public Law 304, 79th Congress]

HOUSE OF REPRESENTATIVES
DONALD S. BEYER JR., Virginia, *Chairman*
DAVID TRONE, Maryland
JOYCE BEATTY, Ohio
MARK POCAN, Wisconsin
SCOTT PETERS, California
SHARICE L. DAVIDS, Kansas
DAVID SCHWEIKERT, Arizona
JAIME HERRERA BEUTLER, Washington
JODEY C. ARRINGTON, Texas
RON ESTES, Kansas

SENATE
MARTIN HEINRICH, New Mexico, *Vice Chairman*
AMY KLOBUCHAR, Minnesota
MARGARET WOOD HASSAN, New Hampshire
MARK KELLY, Arizona
RAPHAEL G. WARNOCK, Georgia
MIKE LEE, Utah, *Ranking Member*
TOM COTTON, Arkansas
ROB PORTMAN, Ohio
BILL CASSIDY, M.D., Louisiana
TED CRUZ, Texas

TAMARA L. FUCILE, *Executive Director*
VANESSA BROWN CALDER, *Republican Staff Director*
COLLEEN J. HEALY, *Financial Director*

CONTENTS

OPENING STATEMENTS OF MEMBERS

WITNESSES

SUBMISSIONS FOR THE RECORD

DEMYSTIFYING CRYPTO: DIGITAL ASSETS AND THE ROLE OF GOVERNMENT

WEDNESDAY, NOVEMBER 17, 2021

UNITED STATES CONGRESS,
JOINT ECONOMIC COMMITTEE,
Washington, DC.

The hearing was convened, pursuant to notice, at 2:30 p.m., in Room 210, Cannon House Office Building, Hon. Donald S. Beyer Jr., Chairman, presiding.

Representatives present: Beyer, Schweikert, Peters, Estes, Beatty, Arrington, and Pocan.

Senators present: Cruz, Hassan, and Kelly, and Lee.

Staff: Vanessa Brown Calder, Ismael Cid-Martinez, Hugo Dante, Sebi Devlin-Foltz, Carly Eckstrom, Tamara Fucile, Sean Gogolin, Devin Gould, Owen Haaga, Erica Handloff, Colleen Healy, Jeremy Johnson, Adam Michel, Michael Pearson, Elisabeth Raczek, Alexander Schunk, Nita Somasundaram, Sydney Thomas, and Emily Volk.

OPENING STATEMENT OF HON. DONALD BEYER JR., CHAIRMAN, A U.S. REPRESENTATIVE FROM THE COMMONWEALTH OF VIRGINIA

Chairman Beyer. It is exactly 2:30 and I think it is 1930 Greenwich Mean Time. So I want to officially call this hearing to order.

Senator, nice to see you.

I would like to welcome everyone to the Joint Economic Committee's hearing entitled, "Demystifying Crypto: Digital Assets and the Role of Government."

I want to thank all of our truly distinguished witnesses for sharing their expertise today. We will begin with my opening statement and then hear from Senator Lee.

Since the introduction of Bitcoin in 2009, the market for cryptocurrencies and other digital assets has expanded from a niche product to a globally significant asset worth nearly $3 trillion last week. While this rapid rise in value has made some early adopters quite wealthy, it also poses an array of risks, both to everyday investors and the broader financial system.

The purpose of this hearing is to explore emerging trends in the digital asset market and discuss prudent steps that Congress and the Federal Government can take to update our regulatory framework and bring much needed clarity to issuers, ensure transparency for investors, and protect the integrity of our financial system, while also leveraging exciting developments in blockchain

technology. Congress can promote responsible innovation in this market, while also providing basic protections to the investing public.

Interest and involvement in the digital asset market has become increasingly mainstream in recent years. The growth of these products has been especially pronounced since the start of the coronavirus pandemic, as the reported total market value of all digital assets soared from $200 billion, with a "B," in January 2020 to nearly $3 trillion, with a "T," just last week. To put that in perspective, recent price volatility in digital assets has erased $400 billion in value just in the last 7 days, an amount roughly equal to the entire size of the market just a year ago.

As the market has grown, we have seen digital asset investors broaden from a narrow group of true believers in cryptocurrencies to an expanding community that includes everyday investors. A Pew survey conducted this fall found that 16 percent of American adults have personally owned or invested in cryptocurrency at some point, up from just 1 percent that held any Bitcoin in 2015.

While many early Bitcoin transactions occurred on little-known platforms, today investors can buy digital assets through Robinhood or Venmo or on large exchanges run by publicly-traded companies like Coinbase. But this growth in value and interest presents a number of challenges for our economy. The current digital asset market structure and accompanying regulatory framework are ambiguous and risky for both investors and the broader economy. Digital asset holders have been subjected to a market that is, as SEC Chairman Gary Gensler has described, "rife with fraud, scams, and abuse."

The mainstreaming of digital assets is laying the foundation for a huge swath of the economy to invest in this market. Increased crypto market volatility, or digital bank runs, could disrupt more mainstream financial institutions like pension funds and mutual funds. And the underlying assets can create significant consumer protection issues, given existing patterns of financial fraud, hacks, and market manipulation.

Retail investors may be lured in by the hype around a new coin with improbably high rates of return, only to be caught on the wrong end of a speculative bubble and lose their entire investment. A recent example is Squid, a blatant scam token that used the excitement around the popular TV show Squid Game to dupe unwitting investors out $3.3 million.

While all investments involve risk, the lack of disclosure and reporting requirements in many parts of the crypto asset industry tilt the playing field toward the largest investors who can leverage their size to exploit regulatory gaps at the expense of retail investors. It is currently difficult for regulators to prevent market manipulation by large players who can exploit their access to multiple sides of a trade or trade on inside information.

Despite these issues, Congress has not yet weighed in on a comprehensive legal framework around these assets. Updating the U.S. regulatory framework for digital assets would be in line with how officials have responded to past financial innovations, although often after the fact, with stronger rules to protect consumers and market integrity. For example, Dodd-Frank created stronger rules

on complex swaps and derivatives in the wake of, that is, after, the 2008 financial crisis.

Updated regulation could also reduce the likelihood that these emerging developments would destabilize financial markets in the broader economy. For example, the largest stablecoin, Tether, was recently found not to hold or to not hold sufficient reserves of cash and equivalents to fully pay back their $70 billion value. Applying regulatory scrutiny to assets like Tether and platforms on which they are used could ensure that cracks in one asset don't spread to the larger economy.

Increasing reporting for decentralized finance platforms will shine a light on a fast-growing but lightly regulated segment of the market. Increased information sharing would also improve tax compliance for capital gains from the sale of crypto assets.

The many issues we will discuss today are why I introduced the Digital Asset Market Structure and Investor Protection Act earlier this year, just a start. This legislation would establish much-needed guardrails and provide clarity to regulators and investors without stifling innovation. The present moment gives us an opportunity to take action before a potential crisis hits the broader economy.

So I really look forward to learning from each one of our witnesses today and from my peers' questions.

So, Senator Lee, the floor is yours.

[The prepared statement of Chairman Beyer appears in the Submissions for the Record on page 36.]

OPENING STATEMENT OF HON. MIKE LEE, RANKING MEMBER, A U.S. SENATOR FROM UTAH

Senator Lee. Thanks so much, Mr. Chairman.

Throughout the history of our great Nation, entrepreneurs and creators have served as the heartbeat of the American economy and the engine for America's economic growth. Their advances into unknown frontiers of science and technology have transformed the quality of life for millions upon millions of Americans and also for people around the world.

Today American innovators are advancing into unknown frontiers of cryptocurrencies, using novel technologies to securely, create, and trade digitally scarce assets. Like the internet of the 1990s, cryptocurrencies are still in their infancy. This evolving technology has vast and still very much untapped potential to revolutionize established industries and to create entirely new ones. Cryptocurrencies are already democratizing finance by lowering costs and expanding access to an industry that has historically been hard to reach for millions of Americans, including hundreds of thousands of Utahans.

Beyond the better known applications to finance, blockchain, which is, of course, the technology behind cryptocurrencies, has even broader potential. Blockchain can securely share health records, efficiently track cross-border transactions in global supply chains, and allow online consumers to verify the authenticity of pictures or videos.

I have great optimism that, like the internet before it, the technology behind cryptocurrencies, meaning, again, blockchain, is

something that is going to create a wealth of new opportunities, many of which we can't even really imagine yet.

As new markets like this one emerge and grow, there is always going to be a temptation here in Washington to expand the Federal Government's reach, a temptation to centrally control the innovative process and regulate the products of those individuals who are at the forefront of American advancement. But this is a temptation that must be resisted. Rigid one-size-fits-all regulation is something that is kind of scary, especially when it is targeted at the cryptocurrency. It is certainly unnecessary. And it would all but ensure that this next generation of technology companies would end up moving to other countries, countries other than the United States. Americans would lose access to cryptocurrency markets and miss out on the potential economic and social benefits.

If we want the center of innovation to remain right here in the United States for the benefit of American workers and American families, Congress should focus on creating clarity around how existing rules apply to these new technologies.

In the case that existing law proves outdated or insufficient, then we can assess the need for new rules. However, as it stands today, we just need to appropriately apply the rules that we already have and are already on the books, most of which are applicable here and most of which are very much sufficient.

The proper role of government is to empower innovation through clear rules with a light touch. The best approach is one in which Congress acts in a manner that is tailored to its limited constitutional authority. It is one where the Federal Government acts with restraint and, in so doing, protects the creation and ingenuity that powers our great country because, when we restrain government, we unlock unlimited human potential, potential that among the American people is immense.

In today's hearing, I hope we can focus on policies that protect a flexible regulatory framework for Americans who are building our future. If we can resist centralizing power in Washington, as has long been the impulse of Democrats and Republicans alike in this town, and instead preserve the space for American innovation to flourish, entrepreneurs across the country stand ready to unleash the tremendous opportunity of new digital economies.

Thank you, Mr. Chairman.

[The prepared statement of Senator Lee appears in the Submissions for the Record on page 37.]

Chairman Beyer. Senator Lee, thank you very much.

Now I would like to introduce our four distinguished witnesses.

Ms. Alexis Goldstein is the Financial Policy Director at the Open Markets Institute. She previously worked in financial regulatory policy, climate finance, consumer investor protection, and higher education for Americans for Financial Reform. Prior to working in advocacy, she spent 7 years working on Wall Street as a programmer at Morgan Stanley Electronic Trading, as a business analyst at Merrill Lynch and Deutsche Bank in equity derivatives.

Mr. Timothy Massad is Senior Fellow at the Kennedy School of Government at Harvard University and an adjunct professor of law at Georgetown Law School. From 2014 to 2017, he served as chairman of the U.S. Commodity Futures Trading Commission. Under

his leadership, the agency declared virtual currencies to be commodities, introduced reforms to address automated trading, and strengthened cybersecurity protections. Mr. Massad has a BA from Harvard College and a JD from Harvard Law School.

Mr. Kevin Werbach is a Professor and Department Chairperson of Legal Studies and Business Ethics and director of the Blockchain and Digital Asset Project at the Wharton School of the University of Pennsylvania. His work focuses on telecommunications in internet policy, as well as applying digital game design techniques to business. Before joining the Wharton faculty, he served as Counsel for the New Technology Policy at the Federal Communications Commission during the Clinton administration. He has published four books including "*The Blockchain and the New Architecture of Trust*." Mr. Werbach received a BA from the University of California at Berkeley and a JD from Harvard Law School.

Finally, we have Mr. Peter Van Valkenburgh who is the Director of Research for Coin Center. Formerly he was the Google policy fellow for TechFreedom. He is a graduate of NYU School of Law and a self-taught designer and coder.

So welcome, all of you. We have 5 minutes for each of your testimony, and we will begin with Ms. Goldstein and then continue in the order of introductions.

Ms. Goldstein.

STATEMENT OF ALEXIS GOLDSTEIN, DIRECTOR OF FINANCIAL POLICY, OPEN MARKETS INSTITUTE, WASHINGTON, DC

Ms. Goldstein. Thank you so much.

Chair Beyer, Ranking Member Lee, and distinguished members of the committee, thank you for inviting me to testify today. My name is Alexis Goldstein, and I am the Director of Financial Policy at the Open Markets Institute where my work focuses on financial regulation and consumer protection.

As the chair mentioned, I previously worked on Wall Street as a programmer at Morgan Stanley and then as a business analyst at Merrill Lynch and Deutsche Bank prior and during the 2008 financial crisis.

I am not only a researcher of digit asset markets, I am also a user of them. I have used large exchanges. I have used so-called decentralized finance platforms, or DeFi. I have tried out layer–2 solutions. And I have bridged from one blockchain to another. And my impression as a user and a student of these systems is that, while many claim that this is the future of finance, it looks a lot like the history of finance to me.

The space is full of intermediaries and rent-seeking. For example, if you wanted to swap one crypto asset for another on Ethereum today, you would have to pay over $100 to a miner to execute your transaction on the Ethereum blockchain. If you wanted to do it last week, it might have cost you hundreds of dollars to do so. If you are a large entity, you can also front-run transactions by effectively bribing the miners. You can essentially up the transaction fee that you want to pay to the miner, and they will execute your transaction before others.

Many of these ostensibly decentralized finance platforms also make use of the very same forced arbitration clauses and class action bans that the biggest banks in the United States do in order to deny their customers the right to sue over disputes in a court of law.

We have also seen the CEO of a major crypto lending and borrowing platform called Compound unilaterally threaten to report their users to the IRS if they had benefited from a software bug that Compound itself created, raising more questions about whether this particular platform is truly decentralized.

One of the problems that we see in the existing financial systems is that users with the least amount of money often pay disproportionately high fees. And, unfortunately, I have found this problem is largely replicated in digital asset markets. Coinbase, for example, has two cryptocurrency exchange platforms, Coinbase and Coinbase Pro. Coinbase is aimed at newer users but charges astronomically higher fees than its Coinbase Pro offering.

There are also large concentration concerns in the digital asset space. Facebook is one example who is moving ahead on its digit asset pilot, despite ongoing questions and concerns from lawmakers, concerns that their plans may be incompatible with financial regulatory—the current financial regulatory landscape.

Venture capitalists also play a significant presence in the cryptocurrency markets and appear to hold considerable market power and power over the governance of many of these platforms, and their investment is growing fast. VC firms invested $17 billion in digital asset firms in the first 6 months of 2021, which is more than three times what they invested in all of 2020.

Hedge funds, family offices, and large too-big-to-fail banks are also a growing presence in the crypto markets. There are also questions about conflicts of interest among major market players. To take a single example, the CEO of the exchange FTX, Sam Bankman-Fried, reportedly also owns 90 percent of a proprietary crypto trading firm, Alameda Research.

In traditional financial markets, barring a serious liquidity crisis, you will be able to sell back the product that you purchase. But on DeFi, it is very easy for malicious actors to design tokens that can be bought but never sold. Some crypto investors solve for this by reading the code of new coins to look for pitfalls and ensure they don't fall prey to these kinds of scams, but this is a fairly high bar for non-programmers.

I worked on Wall Street before enduring the 2008 financial crisis before Dodd-Frank, and much what I saw working with the then unregulated over-the-counter derivatives market reminds me of some of the things I see in today's digital asset marketplace.

Systemic risk tends to arise when the scope, size, scale, or interconnectedness of certain activities metastasize and spread contagion to the broader financial system. There are several concerning items including leverage, opacity in market data, and poorly understood interlinkages between market participants that are currently present in digital asset markets and may indicate potential systemic risk.

Congress should continue to examine if there are regulatory gaps that require new legislation in order to ensure consumer and inves-

tor protections and ensure that regulators have the market data they need to evaluate for systemic risks. For their part, regulators should continue to monitor the space and ensure compliance with existing laws and regulations.

Thank you, and I look forward to your questions.

[The prepared statement of Ms. Goldstein appears in the Submissions for the Record on page 38.]

Chairman Beyer. Thank you, Ms. Goldstein, very much.

Next hear from Mr. Massad.

STATEMENT OF TIMOTHY MASSAD, RESEARCH FELLOW, HARVARD KENNEDY SCHOOL, ADJUNCT PROFESSOR OF LAW, GEORGETOWN LAW CENTER, WASHINGTON, DC

Mr. Massad. Chair Beyer, Ranking Member Lee, and members of the committee, thank you for inviting me to testify today. I first testified about crypto in 2014, and it is an honor to be here.

I would like to make eight points. First, there is no question that digital asset innovation is incredibly important and beneficial overall. But there should also be no question that the time to strengthen and clarify regulation of digital asset markets is long overdue. If done responsibly, it will support, not suppress innovation.

Second, stablecoins are one of the most urgent challenges. If properly regulated, they might help modernize our payment system. But today they pose significant risks. The recent report of the President's Working Group on Financial Markets describes this very well. It calls on Congress to adopt legislation that limits stablecoin issuers to ensure depositary institutions.

I prefer a slightly different formulation where we have some bank-like specific regulations of the risks but we limit the issuer's activities so they aren't making loans and they aren't doing all the things that traditional banks do. And in that model deposit insurance may not be necessary. This is a better way, I believe, to foster competition and innovation and address the risks.

Third, I agree with the PWG report on the need to regulate stablecoin arrangements generally, not just the stablecoin issuer. Once issued, stablecoins trade on decentralized blockchains pursuant to smart contracts, as well as on centralized exchanges. This means that no single authority is responsible for the overall operation of the stablecoin. And with regard to decentralization, or what is called DeFi, generally, it can be a good thing. But calling something DeFi should not make it a regulatory free zone, and we should keep in mind that that label can mean lots of different things. We need to apply standards, appropriate standards, to financial market activities, not the technology itself, that occur on such platforms.

Fourth, Bitcoin is neither a widely accepted means of payment or a stable store of value today. It is a highly volatile, speculative investment. It might be tempting to just say let the buyer beware. But the continued growth of a largely unregulated crypto market poses risks to society including risks of illicit activity, tax evasion, ransomware, investor fraud, and potential harm to broader financial markets.

We do not have sufficient information about this market. Neither the SEC nor the CFTC has authority today to regulate the cash or

spot market, if you will, for digital assets, that are not considered securities. That is a point that is actually not understood by many people, and that is where most trading activity occurs today. So we should expand that authority. At the same time we should make sure our regulatory policies are adequately informed by technological expertise. This is very, very important.

Fifth, in regulating crypto generally, we must balance reasonable expectations of privacy and financial transactions with the government's legitimate interests such as preventing illicit activity and tax evasion.

Sixth, the evolution of the digital assets has made it clear that we need to modernize our payment system. It is relatively slow and expensive. A central bank digital currency is one way of doing so. There may be other ways as well. My concern is we are not moving fast enough to either develop a prototype CBDC or to determine what the best strategy is.

Seventh, CBDC, stablecoins, and digital assets generally are often cited as a means to achieve greater financial inclusion, and we should consider their potential for doing so. But we should act now to prevent—to improve access to financial services through other means as well. The need is too great, and this should not be deferred.

Finally, the challenge we face is not unusual, because the financial sector constantly innovates and our regulatory system has to catch up. I helped draft the original agreements for swaps 30 years ago, and swaps created a lot of beneficial hedging. But the industry resisted regulation and eventually generated excessive risks that almost brought down our financial system. It was only then that we created a regulatory framework under which the industry is thriving today.

To conclude, we should take some actions now to strengthen the regulatory framework. And some key things that Congress should do are, first, require that stablecoin issuers and related arrangements be supervised by the Fed or the OCC along the lines I have suggested.

Two, give the SEC or the CFTC clear authority to regulate the cash market for cryptocurrencies.

Three, make sure FinCEN has the tools and resources it needs to implement KYC, AML, and CFT standards thoroughly.

And, four, urge the Fed and the Biden administration to accelerate work on modernizing our payment system, including by developing a hypothetical CBDC.

Thank you, and I look forward to your questions.

[The prepared statement of Mr. Massad appears in the Submissions for the Record on page 59.]

Chairman Beyer. Thank you very much, Mr. Massad.

We will next hear from Professor Werbach.

STATEMENT OF KEVIN WERBACH, PROFESSOR OF LEGAL STUDIES AND BUSINESS ETHICS, DIRECTOR OF THE BLOCKCHAIN AND DIGITAL ASSET PROJECT, THE WHARTON SCHOOL, THE UNIVERSITY OF PENNSYLVANIA, PHILADELPHIA, PA

Mr. Werbach. Chairman Beyer, Ranking Member Lee, members of the committee, thank you for the opportunity to speak before you today.

Blockchain technology and the digital asset ecosystems it enables could well represent the most important developments in information technology since the internet. The potential exists to not only improve the efficiency of many kinds of transactions but to make markets more fair, inclusive, open, dynamic, 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 major risks involved in digital asset-based markets, and it is important to distinguish potential from reality.

These are still in many ways immature technologies. There are important questions about energy usage of proof of work networks. Holdings of most digital assets are highly concentrated, and there are serious concerns about market manipulation. It is essential for both market participants and policymakers to 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 is an important or even necessary condition for long-lasting and transformative innovation.

A quarter century ago I served on the White House working group that drafted the Framework for Global Electronic Commerce, the U.S. Government's approach to the internet. The policy adopted then was not that the internet should be a totally unregulated space or that the harms it brought should be ignored in light of its benefits. While the framework opposed, quote, "undue restrictions," it also identified the need for a predictable, minimalist, consistent, and simple legal environment. That is what we should be seeking today for cryptocurrencies and digital assets.

Take, for example, decentralized finance, or DeFi. DeFi could create a more open, inclusive financial services environment by removing intermediaries and improving access to capital. Increasing the velocity of assets, facilitating service composability, unlocking yield opportunities, all have the potential to increase risk-adjusted returns available to market participants.

However, DeFi also poses significant dangers which were detailed in the DeFi policymaker toolkit, a collaboration of the Wharton Blockchain and Digital Asset Project and the World Economic Forum.

The challenge DeFi poses is how to address these challenges and risks through regulation. A centralized cryptocurrency exchange has a corporate parent, offices, management team, custodial assets, and typically licenses or registrations. An automated market maker, AMM, or other OnChain DeFi protocol, though, need only be software code running on a decentralized global blockchain network.

While this may sound like an insoluble problem, it is likely to be manageable in practice. First, DeFi services are heavily dependent on stablecoins as on-ramps and off-ramps. Clarifying the regulatory context around stablecoins and ensuring they are subject to appropriate obligations could help address the DeFi regulatory conundrum.

Second, users often access DeFi functionality through websites and services maintained by protocol developers. Some developers have already taken steps such as blacklisting tokens whose trading would clearly violate securities laws.

Finally, DeFi protocol and governance tokens do not appear from nowhere. The moment of token issuance is an important regulatory opportunity. This is, for example, an area of focus of MiCA, the European regime under development now for non-securities digital assets.

The history of peer-to-peer, or P2P, file sharing applications such as Napster 20 years ago also provides a helpful roadmap for how seemingly unregulable services can be addressed. These applications were held liable for copyright infringement when they maintained essential components of central control or when they knowingly induced illegal activity.

Going forward, Congress should take a three-pronged approach to the regulatory questions that cryptocurrencies raise.

First, where possible, provide breathing space and help policymakers gain greater understanding of market dynamics.

Second, quickly address the low-hanging fruit. There are laws and regulations with language that inadvertently fails to accommodate digital assets, and fixes are relatively uncontroversial. There are also too many obvious bad actors who have not faced legal consequences and large players in the blockchain ecosystem credibly accused of systemic market manipulation.

Third, at some point outdated legal frameworks are no longer technology neutral or effective. Over time, we will need to reconsider the basic foundations of financial regulation put into place nearly 90 years ago after the Great Depression. Such an effort will position the U.S. to maintain its leadership in the global financial system as it moves into its next technological transition and leadership in the emergent sphere of blockchain based activity.

I look forward to your questions.

[The prepared statement of Mr. Werbach appears in the Submissions for the Record on page 72.]

Chairman Beyer. Thank you, Professor, very much.

And, last, we will hear from Mr. Van Valkenburgh.

STATEMENT OF PETER VAN VALKENBURGH, DIRECTOR OF RESEARCH, COIN CENTER, WASHINGTON, DC

Mr. Van Valkenburgh. Chair Beyer, Ranking Member Lee, members of the committee, thank you for this opportunity to speak with you today.

On Halloween 13 years ago, an email to a public mailing list shared a link to a PDF. It was the Bitcoin white paper, 3,192 words, a handful of simple illustrations, and some C++ computer code. The following January, a 2-megabyte computer program was made freely available for download to the same public mailing list.

Less than 5 years later, the person or persons sending these emails under the pseudonym Satoshi Nakamoto sent their last message and has not been heard from since.

Today, a few thousands words, a computer file smaller than a cat video, and a missing author have brought about an economic revolution, over $3 trillion worth of economic activity recorded and secured on blockchains, shared ledgers that no single person, corporation, or government permissions or controls.

Who can we thank for that remarkable, utterly unpredictable outcome? Not just the person or persons who went by Satoshi. They stood on the shoulders of brilliant cryptographers and computer scientists. Perhaps above all, they were inspired by another shared and open computer network that no single person controls, the internet, a place where a good idea shared anonymously and publicly can stand on its merits, spread to a community of like-minded innovators, and flourish.

America grew rich because of that openness, The ingenuity of immigrants, entrepreneurs, explorers, and technological pioneers. We don't like permissioned systems in this country because we know that you can't prejudge genius. We want open systems that afford dignity and access even to people we don't yet know or understand. As Steve Jobs would have put it, the crazy ones, the misfits, the rebels.

So I am not going to tell you who is going to show up on the bitcoin blockchain or the coming decentralized web or what exactly they are going to build. I couldn't tell you that today anymore than I could have told you in 1990 that Satoshi would show up on the internet alongside Sergey and Larry with Google and Jimmy Wales with Wikipedia.

All I am going to tell you is that we finally built a tool that can make money work without banks, make organizations work without corporations and courts, make sharing and transacting online work without big tech, and that, because of all that, there is a better chance that tomorrow's misfits will be able to speak, share, and innovate.

This uniquely American ideal, however, isn't about anarchy. It is about opportunity under the law. Bitcoin and follow-on cryptocurrencies are not unregulated. Sensible, technology-neutral regulations have protected consumers and investors and prevented money laundering and illicit finance. The American approach is to flexibly regulate activities, not to ban or blacklist the publishing of new ideas and tools.

Anyone can freely write and share the open source software that makes these technologies works. Any prior restraint on sharing that expressive content violates our First Amendment rights. But if you promise an investor you will invent and build them a new future cryptocurrency, we expect you to register as the issuer of the security.

No one is made to open their homes and private bitcoin wallets to a search by the police without a warrant. But if you provide a service to help people buy and sell bitcoin as a third party, you are expected to know your customers and apply anti-money laundering controls.

There are some gaps in America's crypto public policy. The gaps are not, contrary to popular belief, a central bank digital currency gap with China. The CCP is more interested in banning permissionless tools like bitcoin and substituting a surveillance tool that will give them even more control over the misfits within their borders. We should not emulate that policy.

The gaps are much more mundane. On the margin, securities and commodities futures laws can be improved. And there are well-drafted bills in the House that address those issues. Other gaps concern taxes. The recently passed infrastructure bill included rushed language that could unintentionally stifle innovation and invade personal privacy. There was a bipartisan solution with widespread support, but procedurally it was impossible to implement before the bill's passage.

Existing IRS policy leaves taxpayers uncertain of their obligations with regard to cryptocurrency transactions. Tax issues are complex. So I have left specifics to my written testimony.

Suffice it to say, there is no reason why America can't continue to be a home for permissionless innovation, while also enriching its treasury. We did it with the early internet, and we will do it again with cryptocurrency networks.

Thank you.

[The prepared statement of Mr. Van Valkenburgh appears in the Submissions for the Record on page 100.]

Chairman Beyer. Thank you, Mr. Van Valkenburgh.

Thank you all very much. Fascinating testimonies. I encourage all of us to read the larger versions, too, because there is so much more content in them.

Let me begin my five minutes of questions.

Mr. Massad, you talk some about stablecoins. And we just heard Mr. Van Valkenburgh say that, you know, already we are sufficiently protected against too much illicit use of stablecoins or cryptocurrencies, tax evasion, terrorism. And we have read a number of times in the last week about Tether having the $64 billion, $70 billion but not enough actual assets if converted.

How do we protect investors from a run on a stablecoin like Tether?

Mr. Massad. Sure. Thank you, Mr. Chairman, for the question.

We have to have policies that require that the reserves that they receive, in other words, the money they receive for the tokens, are invested in highly safe liquid assets, ideally just cash so that it is always there.

What we have today is a situation where there are no requirements, and a firm like Tether has investments in commercial paper. We don't even know what kind of commercial paper. There is a lot of speculation that it is commercial paper in China. They have loans. They were found to have loans to affiliates. They may even have investments in cryptocurrencies.

So that risk is that if there is a sudden spike in demand for redemptions, they will not be able to meet it. Or if they have to liquidate assets, that could cause downward pressure on assets prices. If they, in fact, have $30 billion of commercial paper, that is a huge amount that would affect the market. So that is the main thing.

And then we also have to address the ancillary arrangements, the fact that these things are traded on decentralized blockchains.

Chairman Beyer. We often wonder how many of these investors realize that these are not insured deposits, you know, with the FDIC.

Mr. Massad. Well, that is a good question. There is a lot of stickiness, though, to people's use of Tether because Tether plays a very important role. It allows people to move value around between exchanges and between cryptocurrencies. And, frankly, Tether illustrates that our payment system needs to be modernized, needs to be improved. That is why it has grown so much. It has also probably grown because it is a vehicle for tax evasion and potentially for illicit activity.

Chairman Beyer. Thank you.

Ms. Goldstein, in your written testimony you highlighted the Squid incident where developers pulled all the liquidity out of the coin. Can you explain how a rug pull works and what we can do to prevent rug pulls?

Ms. Goldstein. So a rug pull typically happens when a developer creates a token, puts it on a blockchain, whether it be the Ethereum blockchain or another blockchain. There is lots to choose from: Avalanche, Harmony ONE—take your pick—Binance Smart Chain. And you create what is called a liquidity pull for it.

And what that involves is going to a decentralized exchange like Uniswap or one of their competitors and basically putting two tokens together, your new token, your Squid Game token, and usually a stablecoin. And you put enough volume of those two tokens on there so that people who want to buy your Squid token can go in, use the stablecoin that they have put into the liquidity pull, and buy their Squid Game token.

But because they are the ones who have sort of initially provided the liquidity for that pull, once people come in and they buy the Squid Game token, they can also pull that liquidity out at any time and essentially cause the price of the token to crash.

So they basically tend to wait until enough people buy it up that the price begins to run up. And it runs up sufficiently enough that this new token that they have minted out of thin air, right, they have created it out of nothing, is worth something. And they pull all the liquidity out and run off with the money and that is what happened with the Squid Game token.

Chairman Beyer. Thank you very much, I think.

Professor Werbach, Senator Lee talked about a light touch and not centralizing everything in Washington, DC, you know, with the fear that too much regulation stifles innovation. How do you see that tradeoff or even that that supported network between regulation on the one hand and innovation on the other?

Mr. Werbach. Innovation is not just one thing. There are many different kinds of regulation, and I think the concern is a valid one. There are ill-fitting regulations. There are situations where regulation is not necessary. But it is not inherently the case that having a regulated market is inconsistent with having innovated market. If that were the case, then the U.S. would be the least regulated financial market in the world instead of one of the most regulated.

Regulation can promote trust. There is a reason why our capital markets are so successful. People come here because they trust that it is a fair and open market and one that will allow their sophisticated activities in an appropriate way.

So the question is really what kinds of regulations we have, and I agree with Mr. Van Valkenburgh. It is not that there is no regulation in this digital asset space. We have existing rules which in some cases are not being enforced. In some cases there are questions about how they can be enforced for new kinds of assets. In some cases there are gaps.

So what we need to do is something like what we did 25 years ago with the internet. Do an inventory. Identify what the issues are. Identify what the existing regulatory structures are and identify where there are gaps, where there are problems, where the danger is that either the absence of regulation or the lack of clarity about regulation that exists will lead to these kinds of abuses and will lead to a situation where the market potentially collapses.

Chairman Beyer. Thank you very much.

Let me now yield to Senator Lee from Utah for five minutes.

Senator Lee. Thanks so much, Mr. Chairman.

Mr. Van Valkenburgh, I would like to start with you, if that is all right.

Sometimes when Congress discusses cryptocurrency, you see concerned faces. You see sometimes people reflecting a certain degree of fear or anxiety. But the conversation is almost always alarmist in nature when it comes up in these hallways and those on the other side of the Capitol. We hear claims to the effect that this is a space that is sort of analogous to the Wild Wild West and could likely lead to chaos, pandemonium, more criminal activity and financial ruin on a widespread basis including victimization by those who are least able to absorb risk.

But as you have pointed out, the industry is, in fact, already regulated. I mean, crypto markets do, in fact, face consumer protections when enforced by a whole host of alphabet soup Federal regulatory agencies—CFPB, FTC, FT—CFTC, SEC, and FinCEN, just to name a few. State attorneys general also have authority. Is that accurate?

Mr. Van Valkenburgh. It is quite accurate, Senator.

Senator Lee. And cryptocurrency and the blockchain technology that it is built on itself contains its own sort of mechanism for self-regulation and protections against fraud and abuse, does it not?

Mr. Van Valkenburgh. That is the foundational principle behind bitcoin is the double spending which is the most obvious type of fraud. Counterfeiting of digital money is policed for by a public transparent ledger that anyone can audit and check themselves.

Senator Lee. In fact, for these very reasons aren't there ways in which crypto markets are always improving consumer safety and reducing financial risk?

Mr. Van Valkenburgh. Always improving is a strong statement. I think, by virtue of these networks being inherently public, we have great advantages. However, by these technologies being very new, there is a steep learning curve. I am very optimistic for the long-term future of the technology, however.

Senator Lee. Because they are based on a new technology, they could offer some real advantages, it seems to me, to lower-income customers who are looking either at them from the standpoint of something to invest in or something to use as a means of transferring money from one place to another. In some ways there could be economic benefits to poor and middle-class consumers everywhere from them, wouldn't there?

Mr. Van Valkenburgh. I think its greatest benefits, quite frankly, are not even here in the U.S. They are in countries that have literally no access to financial services because they don't have the rule of law, and the technology even in its current state can easily fill a gap in those places that have been left behind.

Senator Lee. Like the underbanked, the underbanked could benefit significantly from it.

So if we ban some of these privacy features in cryptocurrencies or if we regulate them to death, how might we be precluding or missing out on some of the beneficial innovations that require privacy protections?

Mr. Van Valkenburgh. I think innovation and creativity require some sphere of privacy so that you are not immediately judged for the things that you are going do that are nontraditional, and that was the big story of the internet was a bunch of misfits who felt like they could come up with a new idea for a social network or something like that and be able to experiment freely. I think the same will be true of open block networks which also afford people that free and open platform for experimentation.

Senator Lee. Are you familiar with the phrase "born in regulatory captivity" versus "born in regulatory freedom"?

Mr. Van Valkenburgh. Yes.

Senator Lee. It seems like it might be apropos here.

Now for Americans who own a little Bitcoin and use it to buy something or to send some money back home, how could Congress help make it easier for them to comply with the Byzantine labyrinth of legal implications that could accompany that?

Mr. Van Valkenburgh. I think the thing Congress can do to help those folks most would be to regularize and make clear our tax policies, especially by providing a *de minimis* exemption from capital gains taxation for small cryptocurrency transactions which otherwise trigger a capital gain and a need to report and simply make using the technology very difficult. We have that kind of exemption for foreign currency transactions. It makes sense to have the same for cryptocurrency transactions.

Senator Lee. Where would you be inclined to set the limit, if you were king for a day and you had the ability to set the *de minimis* safe harbor? Where would you put it?

Mr. Van Valkenburgh. Being a humble person, I would set it where the foreign currency exemption is. And that is where it is set in legislation we have seen in the House from DelBene and Mr. Schweikert.

Senator Lee. You know, as you have noted, a lot of the barriers to innovation for cryptocurrencies come from existing laws and uncertainty about how those laws might be enforced, some variation in whether it is in enforcers or in interpretation of existing authorities.

In many cases that uncertainty and overly broad interpretations of these existing financial regulations have begun to push some of this technology overseas or at least some of the pioneering U.S. technology companies overseas.

What do you think is the best way to protect consumers and to ensure America remains, you know, at the cutting edge of this type of innovation?

Mr. Van Valkenburgh. I would agree with my fellow panelists that stablecoins are an interesting area, and the regulatory field there is somewhat convoluted. There are certainly stablecoin issuers who are violating the law, who have not registered as State money transmitters, or who have not chartered themselves as State banks or trust charters. There are also regulated stablecoin issuer, and there is also the possibility of creating more of a Federal home for regulation of stablecoins. We don't have a legal gap there, I think. We just have an enforcement gap, and that is a real problem.

Senator Lee. My time has expired. I appreciate year testimony. This really could be a boon for America's poor and middle class. Let's not get in the way of it.

Chairman Beyer. Thank you, Senator, very much.

I now recognize the Senator from New Hampshire, Senator Hassan.

Senator Hassan. Well, thank you very much, Mr. Chair and Ranking Member Lee. And thanks to all the witnesses today for your work.

Ms. Goldstein, I want to start with a question to you. I recently wrote to several agencies including the Department of Justice and the Treasury, highlighting a cyberattack on the town of Peterborough, New Hampshire. The perpetrators quickly converted most of the $2.3 million, which in a small town in New Hampshire I can assure you is a lot of money, in taxpayer dollars that they stole. And they converted it into cryptocurrency, making it unrecoverable.

What actions can agencies take to prevent this kind of criminal activity such as the rapid conversion of illicit funds into cryptocurrency?

Ms. Goldstein. Senator, thank you for your question.

There are four suggestions that I have. The first is that a large portion of this marketplace likely falls under existing securities laws. And applying those rules, including rules that apply to broker dealers, I think would help stop illicit actors' ability to move money anonymously and help prevent that sort of ransomware conversion.

My second suggestion is that the Treasury Department can enforce some guidance that they just put out in October. OFAC put out this clarification that if you do digital assets, you need to comply with sanctions. You need to check whoever is using your platform against the sanctions list. And I think the Treasury Department enforcing that guidance would be a good step forward.

The third is anything the agencies can do with your help, if needed, to promote more information sharing can always help. FinCEN analysts can put out reports as a result of that.

And the last think I would suggest is that FinCEN has a very specific set of financial regulations regarding financial crimes spe-

cifically. And I know you are already talking to them about this, but I think strong enforcement of those would also be helpful.

Senator Hassan. Okay. Thank you so much.

Mr. Massad, in the letters that I wrote, I emphasized how stronger know your customer requirements for cryptocurrency exchanges can curtail the criminal use of cryptocurrency. It becomes much harder to evade law enforcement when your name is attached to the cryptocurrency wallet you are using to commit crimes like ransomware attacks, drug trafficking, and money laundering.

How could stronger know your customer requirements for cryptocurrency exchanges help authorities prevent and prosecute criminal uses of cryptocurrency?

Mr. Massad. Thank you for the question, Senator.

It is extremely important, and one big example of this is what is happening with ransomware. There was a recent FinCEN report just issued a couple of weeks ago that documented how ransomware is increasing rapidly. I think the Colonial Pipeline incident was a real wake-up call, too, because that is a company that didn't have a lot of personal identifying information. It was an infrastructure company, and yet it was hit. I think we are going to see more of that.

The FinCEN report talks about how these illicit actors often act through the crypto exchanges. They reuse addresses. They make multiple transfers of the illicit profits so they can't be traced. And, you know, KYC is critical here. And we need to bolster, you know, FinCEN in this. But it is more than that. We also have to have a structure of regulation around these exchanges.

Coinbase, Kraken, these other exchanges, they are not subject to the same standards that we have for securities and derivatives exchanges. They are registered as money transmitters. That is a pretty light touch of regulation. They don't have standards to prevent fraud, to prevent conflicts of interest, to prevent things like wash trading. Wash trading is where you essentially trade with yourself or with an affiliate. That is very, very common.

And there is a very interesting CFTC action here. The CFTC only regulates derivatives contracts. So to say that, you know, the SEC or the CFTC has power over these exchanges is wrong because the CFTC can't regulate that cash market for Bitcoin anymore than it can regulate the sale of cows just because it regulates cattle futures.

And yet it does have very limited power to bring fraud actions, but that takes a lot of resources to do. They did bring one against Coinbase. But even one of the Republican commissioners said, "you know, this is going to mislead the public into thinking that we regulate these exchanges. And we don't." So that is—it is a broader problem than just KYC standards but that is critical.

Senator Hassan. That is very helpful. Thank you.

One more question again for you, Ms. Goldstein. I recently introduced a bipartisan bill with Senator Ernst that would require Treasury to report to Congress on how cryptocurrency is used globally and its effects on global supply chains. How has cryptocurrency mining affected global supply chains in recent years including for critical technologies such as semiconductors?

Ms. Goldstein. Well, Senator, I commend you and your fellow senator for the bill and the report that you request.

Essentially cryptomining has an arms race. Their technology needs to improve all the time so they can keep up and make money. And that means often they have to replace the equipment very fast, and that means more demand for semiconductors. And that means less, you know, electronics makers who use semiconductors for other things are able to access them.

So I do think that there a lot of research, in particular, showing, for example, graphics card needs secondhand goes in conjunction with the price of ether, for example.

Senator Hassan. Okay. Thank you very much.

And thank you Mr. Chair.

Chairman Beyer. Thank you, Senator, very much.

I now recognize the gentleman from Arizona, Mr. Schweikert.

Representative Schweikert. Thank you, Mr. Chairman.

I may take this a slightly different way just because you and I have worked on discussions around this for a long time. I have a fascination with distributive ledger technologies. I think I hold the record of being the first one to actually mention bitcoin in a Ron Paul hearing, believe it or not, many years ago.

Could we spend a couple of seconds, because three of you have sort of touched on it, let's do some societal good. Transaction costs, using of my credit card, the wire transfer, what do we as policymakers need to do to in many ways use the technology that should crash the price of someone walking into, whether it be Walmart and using a credit card or sending money back to the family in Guatemala? This technology should be crashing that price.

First, what do we as regulators need to do on that? And then we are going to go down the rabbit hole on a couple of other things like identity and other things that could actually help. We were trying to do an experiment in Arizona of using a blockchain to identify homeless activities and the benefits attached to them and have it in a universal spot.

Mr. Massad. Thank you, Congressman. It is an excellent question. Stablecoins are one possible way to do that if they are properly regulated. A stablecoin is simply a token.

Representative Schweikert. Well, I am sorry. I am going to geek out with you just——

Mr. Massad. Yes.

Representative Schweikert. I am very familiar with the underlying mechanism. Matter of fact, years ago I worked on an escrowing for a blockchain code——

Mr. Massad. Uh-huh. Uh-huh.

Representative Schweikert [continuing]. to show you how far down the rabbit hole I went.

But you think a stablecoin would be your methodology for creating a——

Mr. Massad. A faster——

Representative Schweikert [continuing]. rail.

Mr. Massad [continuing]. pace. It certainly could be because, again, it is a token that is then backed by the dollar and there is a lot of proposals——

Representative Schweikert. Would you use a stable token?

Mr. Massad. A stable token?

Representative Schweikert. Yes, where there is a——

Mr. Massad. An algorithmic kind of——

Representative Schweikert. Yes.

Mr. Massad [continuing]. formula?

Representative Schweikert. You know, here is my piece of plastic. I swipe it over here. We have an agreement that it represents this many units.

Mr. Massad. Well, that is the hardware——

Representative Schweikert. Yes.

Mr. Massad [continuing]. the plastic part.

What I am talking about is, you know, currently, as you point out, our system, our payment system is it is essentially bank deposit dominated. Credit cards still go through banks.

Representative Schweikert. Uh-huh.

Mr. Massad. You know, wire transfers go through banks. And banks, frankly, haven't innovated enough. With a stablecoin, if properly regulated, you could potentially have new entrants into payments that then are creating new payment rails using that digital technology.

Representative Schweikert. Okay. So, instead of you and I going over thin line technology because we have white-boarded a fixed—a stable token actually——

Mr. Massad. Uh-huh.

Representative Schweikert [continuing]. which is pretty much the same thing, what do we have to do policywise to make that available? Because overnight that would actually change costs in our society of using——

Mr. Massad. Right.

Representative Schweikert [continuing]. three percent, five percent?

Mr. Massad. Yes, it could. I think we need to create a regulatory framework to regulate those issuers so that—and the PWG report I think lays out a lot of issues. My only concern with it is it recommends that Congress adopt legislation that says only insured depository institutions can do this.

Representative Schweikert. But that would——

Mr. Massad. And——

Representative Schweikert [continuing]. screw up the cost structure again.

Mr. Massad. I think that limits competition.

Representative Schweikert. Okay.

Mr. Massad. Right.

Representative Schweikert. Okay. The same sort of question. How do I make—how do I use distributive ledger, blockchain technology, whatever title you want to give it—I know this is more crypto—but also using the knowledge that we are developing here to benefit society and those transactions?

Mr. Van Valkenburgh. So, I think my fellow witness, Mr. Werbach, with his insights about the Clinton administration's Framework for Global Electronic Commerce is on the money.

Technologies back then in the 1996 hearings about the internet could not have allowed people to share high-speed video, could not have allowed people to have Zoom conferences instead of hearings,

could not have allowed people to do online banking. You could send a very small amount of data through the internet at that point. I didn't have——

Representative Schweikert. I was involved in the old Check 21, to give you an idea how far back.

Mr. Van Valkenburgh. Yes. And in a very real sense today, we still are at that point with respect to cryptocurrencies. As my fellow witness said, sometimes the fees are actually quite high. And it seems as though there is no hope of moving more economic activity, let alone social networking transactions, identity transactions onto these networks.

The layered architecture of these technologies, however, means we have lots of avenues to build more scaleable, more efficient solutions. And it is a story of free and open platforms that allow anyone to build that innovation.

We gave a briefing in the House, I think in this very building, where we used the Lightning Network, an open payment network built on top of bitcoin's open protocol, to buy candy from a candy machine. A transaction of half a penny got you M&Ms from the machine, and the fee for that transaction was 1/250 of a penny. That was actually a settled transaction that ultimately ended up batch settled without just on the blockchain by the Lightning Network far better than the corresponding banking system that we have today, ACH, credit card authorizations.

Representative Schweikert. I am actually up against the time. But that is actually part of the discussion of ID, licensing, benefits, my ability to send some resources to grandma. I know we—I know the money is in the cryptocurrency. That is where the enthusiasm is. But sometimes I think we failed to understand. If we do this smartly, the benefits of distributive ledger and stable code—and code is ultimately insurable, if we can ever get that far—could we actually also do some really good thing to society, not only in our country but around the world?

And with that, I yield back.

Chairman Beyer. Thank you, David, very much.

Now I recognize the Senator from southern California, Mr. Peters.

Representative Peters. I wish I was a Senator. That would be a nice six year term, but I am just a lowly Representative.

Thank you very much, Mr. Chairman. Thanks for having this hearing. This has actually been fascinating and a really good presentation.

It sounds like we are struggling at the beginning of this phenomenon with using government to come up with fair rules like the markets have that people can trust without getting in the way of innovation that can happen. I think that is a pretty common story, and we are just at the beginning of it.

One issue I had for you, though, Ms. Goldstein, is to be fair, we want to make sure that there is—this currency is not used for tax evasion. And I just want to refer to the bipartisan infrastructure framework. There was a provision that attempts to prevent tax evasion in the crypto space by requiring starting in 2024 brokers to report cryptocurrency gains in a 1099-B form.

I wonder what you thought of that as a measure to curb tax evasion. Is that sufficient, or do you think there are other particular measures that we should pursue?

Ms. Goldstein. I am a supporter of that language. I think it is important. I think, you know, we talk a lot about innovation in this space, but, you know, there are a lot of companies we think of as so innovative like Charles Schwab or TD Ameritrade and they are supplying those sorts of tax reporting every day.

And I think—I had to do my cryptocurrency taxes last year because I did not get a 1099-B form from a lot of the different platforms that I used. I had to pay a third-party vendor over $100 or $200, I don't exactly remember, in order to generate my tax form for me so that I could submit it to the IRS and make sure that my crypto taxes were paid appropriately.

And so, I think not only is there a benefit of sort of going after some of the tax evasion that the administration has reported is happening, but there also is a benefit to the end user. It would make it a little bit easier for them to do their own taxes. The burden would no longer be on the own individual investors, it would be on the platform.

Representative Peters. Right. And I assume in this industry we won't hear any back talk about how difficult it is to calculate this, because appreciables and standard operations it seems like.

I had a question for Mr. Massad. In a recent Brookings Report you suggest that the Financial Stability Oversight Council should commence a review of stablecoins. Can you tell us a little more about what you think in general we are going to get out of this, not at the level Mr. Schweikert would understand but maybe the public could. Not to ding Mr. Schweikert, but it is no surprise that he understands this at the same level as the witnesses.

Mr. Massad. The Financial Stability Oversight Council has the power under the Dodd-Frank Act to designate a payment activity as systemically important or likely to become systemically important. And I think the growth of stablecoins from very low numbers to over $130 billion today, plus the potential future growth if we did allow them to do broader application might very well meet that test.

If they do that, then the Federal Reserve is charged with developing risk management standards. So I think that is a way to create a regulatory framework, certainly Congress could pass legislation too, but I think the FSOC could take that action and that could address a lot of the issues that we have mentioned, making sure the reserves are invested in cash, making sure there is liquidity, making sure there is operational resilience, and making sure things like KYC are adequately dealt with.

Representative Peters. That would certainly be an important thing in lieu of there is no deposit guarantee——

Mr. Massad. Correct.

Representative Peters [continuing]. There is cash behind it.

Mr. Massad. That is right. And today some of the stablecoin issuers are registered as trust companies, but that State registration doesn't mandate all the standards that I am talking about. It is still a light touch.

Representative Peters. Mr. Werbach, tell me what the key differences are you would identify between decentralized finance in traditional banking and whether you think there is a potential that affects the integrity of the dollar, this whole phenomenon.

Mr. Werbach. Well, decentralized finance is essentially transforming finance and financial services entirely to software. So it is about financial services that settle on a blockchain, a decentralized ledger that are noncustodial so you don't give up control of your assets to the third party and that are open, programmable, and composeable.

So this is basically open so software and these pieces can be plugged into each other. It is a much more open and dynamic way of doing financial services, and it is one reason that we have seen an explosion of activity in DeFi and companies coming up with new opportunities, which can be very beneficial.

The problem is they do it without the kinds of restraints that we have in the traditional system. And some of those restraints are very important for all the reasons that my fellow witnesses and I talked about, whether it is about money laundering or about protecting investors. So the answer is not to go back to the banking system and to prevent DeFi from happening.

The question is first of all understanding what those risks are and also understanding what is happening in the marketplace. Because for example, there are DeFi insurance platforms are coming into existence that allow you to hedge against the risk that there is a hack on a DeFi service. But again, all of this is so new that we don't have an understanding of what it is.

Representative Peters. I appreciate it. My time has expired, but again thank you for the hearing. Thank you to the witnesses.

Chairman Beyer. Thank you very much, Congressman.

I next recognize the Congressman from Kansas, Mr. Estes.

Representative Estes. Thank you, Mr. Chairman. And thank you for all the witnesses for being here today. This is a great topic for us to be talking about. Obviously, when we look to the future there is a lot of technology out there and where we can possibly go with the country.

And I want to go back and we talked a little bit about this, but, you know, over the past 30 years we have seen a number of innovations tied directly to the internet, and a lot of rapid developments, and adaptation. And really it was impossible to really know how the internet would function back when it was first being formed.

So today we see that the blockchain technology and the capability there that gives Americans ability to reliably record information without having an intermediary to act as the recorder of that information. I think there is a whole host of potential applications from across the economy from land titles and ownership records, to contracts, to improving security over and above what we frequently have talked about in terms of crypto technology as being used as a currency. And I think there is a lot of decisions we have to make in both areas.

Just like when the internet was new, we need to be careful about how Congress approaches these new technologies and what regulations we put in place. Just like there were many false starts with

internet there in the dot.com bubble, but today it is really a critical tool that we have.

It is good that the Congress didn't regulate the internet out of existence in the 1990s before it was clear what all those uses could be. And I hope that, you know, as we work through this process we come up with a goal that makes sure that we don't impose unnecessary barriers to the innovation. I hope that along with looking for protection from bad actors, Congress is very deliberative in its process and coming up with those legislative decisions that will help this technology grow and expand for things we haven't thought of today or discussed today.

I do have a couple questions. Mr. Van Valkenburgh, what do you see are some of the exciting technologies that are citing applications that we can use with the blockchain technology going forward?

Mr. Van Valkenburgh. Thank you, Congressman. And your colleague, Mr. Schweikert was going down this avenue as well. I think I would like to talk about identity. So when we think of blockchain networks as you said just now, we often think mostly about money.

And cryptocurrencies are the scarce commodity tokens that power them are essential to the operation of these systems, because they create a fair reward for anyone who donates computing power to secure the blockchains and the data on that blockchain.

So you don't need permission who can secure that data, you have an open competition of people securing that data and doing it transparently and getting a fair reward on the blockchain.

With that said, one the blockchain is secure, you can put information in that blockchain that goes beyond merely a transaction where I paid Mr. Schweikert a bitcoin. You can put a transaction on that blockchain where I testified in front of Congressman Schweikert and I attested to my identity by using a unique cryptographic key in my phone when they let me in the front door. This kind of identity transaction is another intermediated transaction when it takes place on the internet today.

We rely on major corporations to run our social networks, to run our credit reporting agencies, to run all the tools and systems that identify us that permission our access to buildings. The OPM uses major enterprise identity providers in order to secure government buildings for personnel.

All of these ledgers are centralized and siloed and can ultimately be improved and decentralized by using open blockchain networks to secure identity transactional data, rather than trusting one corporation or company to do that. To that end, Microsoft has pioneered something called the ION network.

It is not Microsoft's technology, per se. They are developing an open standard and contributing along with other corporations to a decentralized identity standard that would actually anchor identity data into the bitcoin blockchain so it is more secure and less vulnerable as a centralized data repository would be to hacking, and ransomware, and such.

Representative Estes. What you have taken was very complex, trying to figure out how to deal with cryptocurrency and now made it even much more complex in terms of the other applications.

I am about out of time. I don't know if you can say a quick comment about cybersecurity and how that might effectively be positive through this.

Mr. Van Valkenburgh. Sure when we think of cryptocurrencies and cybersecurity we often jump to ransomware because it is used as a payment for ransomware. I think it is important to point out that Deputy Treasury Secretary Wally Adeyemo said in his speech last week, "ransomware is not a cryptocurrency problem in the same way online fraud schemes are not the fault of the internet."

In fact I would go further and say that cryptocurrency technologies are ultimately the solution to ransomware cybersecurity issues because the big tech paradigm of securing user data in a centralized database is what creates vulnerability to hacking.

If we decentralized control over that data, decentralized the social network, decentralized an identity provider you lose that single point of failure and that vulnerability from a ransomware and hacking perspective.

Representative Estes. You certainly give us a lot to think about in trying to figure out what we do.

Mr. Chairman, I yield back.

Chairman Beyer. Thank you, Mr. Estes, very much.

I now recognize the distinguished Congresswoman from Columbus, Ohio, Ms. Beatty.

Representative Beatty. Thank you, Mr. Chairman and thank you to our witnesses, and my colleagues. This is very intriguing. And I want to come back to it, but I want to say this before my times runs out. I am really interested in the capital gains issue in how that would work as we deal with it in crypto versus I know how it works in real money when you have capital gains and how you have to apply to it.

So I don't know if I have enough time. I will ask my questions, but I want to come back to that.

But I will stay with you Mr. Van. I have a large Somali immigrant population in my district. As a matter of fact, I have the second highest in the country next to Minnesota.

And I have worked with them, and many business individuals, and the Treasury for years to help them solve their remittances issue, because Somali does not have an adequate central banking system.

Can you describe how bitcoin and crypto can potentially help with remittances or not? Because right now, they are traveling to Dubai once a month and sometimes with incredibly large, millions of dollars in a briefcase to get it back to come to Somali.

Mr. Van Valkenburgh. So the value of bitcoin and other permissionless open blockchain networks for remittances is that it makes starting a new remittances business the barriers to entry to that field of endeavor much lower. You don't need to gain access to an ACH network, you don't need to have a well-functioning financial system in say the destination nation for the payment.

With that said, I want to be sober about this, you still may have last mile concerns. If the person at the other end of remittance is happy get a decentralized cryptocurrency then they may be able to receive that cryptocurrency using nothing more than a phone and an internet connection, which in many parts of the world may be

something you would be more likely to have than access to well functioning financial services.

However, if you want local currency, you will need to find someone willing to exchange the decentralized cryptocurrency for the local currency, and that is another point for potential failures or a place where regulation may be necessary because it is a trusted activity.

Representative Beatty. Mr. Werbach, I know you have gone around the country giving lectures to business folks, attorneys and in your book when you talk about this being the new architect. Any comments on that?

Because I think you hit on something. You have to have it on both ends and how advanced do we know for this population that I just mentioned, do we have any Intel on what is happening in Somali with this.

Mr. Werbach. Well, this is something that is developing in the marketplace. Early on when bitcoin came around and cryptocurrencies came into existence, people said obviously this is going to be the solution for remittances. It is so much cheaper and you don't have the intermediation.

Many companies went into the market thinking they would deploy these solutions and in most cases they failed or in most cases they were outcompeted by traditional kinds of services in part because of these last mile issues.

And in part because in many ways the transaction in the middle of the network is fairly efficient under modern financial systems.

So really what we need to see is how the market is developing and whether there are solutions as the technology evolves on both ends. And for example, as which have systems like the Lighting Network that Mr. Van talked about that may lead to more efficiency of these payments. It is certainly possible that a cryptocurrency-based remittances system will be a better solution but, we shouldn't prejudge.

We shouldn't be in favor of one technology over the other. We should encourage the so-called traditional financial technologies to evolve and develop as well and have a marketplace that ultimately is best for the people using it.

Representative Beatty. Thank you. I will try it get one more question in.

Mr. Massad, in your testimony you spent a great deal of time addressing the slow and expensive payment system that we have in the United States. You even say that cryptocurrency namely, Central Bank Digital Currency, is one way to address this, but the Federal Reserve has been working on a faster payment system for a few years and many other countries—with many other countries around the world have a real-time payment system without the use of the Central Bank Digital Currency.

Wouldn't the easiest route to address this outdated payment system be just to move into a real-time payment system which the Feds is already working on as opposed to creating a whole new system with Central Bank Digital Currency?

Mr. Massad. It is an excellent question, Congresswoman. The Fed initiative which is called FedNow will certainly help a lot. The question, though, is first is it going to take a little while before it

even comes online, but more importantly, will the benefits of FedNow really be widely decision contributed?

Banks have to decide if they can manage it, if their own systems are capable of using it? And will they pass on the benefits? My concern is we need more competition to ensure innovation. The other thing about FedNow is that technology probably doesn't have the throughput that blockchain type technologies have.

So I don't think it would be as good. And it is not clear you can develop smart contracts and so forth. So you know, it is one option, but I think we need to look at these others.

And if I may going back to your question on remittances also incredibly important it really should be as easy as sending an email to send money abroad. And I think again digital technologies—digital assets probably regulated could do that. I would favor stablecoins or CDBCs over something like bitcoin.

Representative Beatty. My time is up. Thank you, Mr. Chairman.

Chairman Beyer. Thank you, Congresswoman.

And now the gentleman from Texas, Mr.——

Representative Arrington. Bringing up the rear over here, Mr. Chairman. Thank you all for your insights. It was a great discussion so far. And the panel has certainty helped educate me on something that I am not so familiar with, so I admit that from the outset.

Mr. Van Valkenburgh, what an eloquent and powerful picture of America as the laboratory of innovation as a result of freedom, free people, free markets, unleashing creativity, ingenuity, and creating value for customers, not just here but around the world.

So thank you for that. I loved listening to the uniquely American ideal that I think we all subscribe to, by the way, at least that is what I am hearing from the other witnesses.

And I heard Mr. Werbach talk about a light touch. Maybe you said something like minimalistic legal construct. We want to all balance innovation and the need for having rules and basic safeguards. Because I don't know as much as I need to give any informed comments beyond this, I was a former regulator, chief of staff at the FDIC for many years. A lot of regulations there were derived from the risk to the deposit insurance. Right?

I mean, with that came a lot of risk management on the safety and soundness and then there were a lot of consumer protection regulations and rules to follow. Absent systemic risk and the deposit insurance for consumers that the taxpayers are ultimately accountable for as a backstop, what are the gaps here?

If there was one thing that you could all agree on in terms of filling the gaps to make sure we had basic safeguards, but we were not in any way I think you said in some ways regulation appropriately applied at the right time in the maturation process could support this not stifle it. I agree with that.

So what would you all agree on, one or two things that maybe kind of the 80/20 rule, a few things that could close the gap, most significantly where there would be common ground among my colleagues and I.

Mr. Van Valkenburgh. Thank you, Congressman. That is an excellent question. I think we would all actually agree on taxes. I

did want to bring up a point earlier about the bipartisan infrastructure legislation and the self-reporting—third-party reporting provisions, sorry, that were in that piece of legislation.

As I said, there is language that it was vague and therefore could stifle innovation and harm personal privacy. And so, I do think a fix to that language was important and there was a bipartisan fix in the Senate, it could just not be procedurally implemented. But I am not saying that because I am against third-party reporting.

In fact, folks in the cryptocurrency ecosystem have been asking for guidance from IRS, if they are running a company that helps someone buy Bitcoin, how can they do specifically third-reporting for their customers to make sure their customers can easily comply with taxes.

Because I agree with Ms. Goldstein. When I filed my crypto taxes, it is not easy. So clarity there is important. I just think we should be careful the way we draft these laws and there was some slight issues with the language in the infrastructure bill.

Again I would say *de minimis* exception from capital gains transaction for small transactions is essential to tax policy. And we can also have better tax policy with respect to assets that people receive because of cryptocurrency forks, which I will not dare explain at the moment, but Representative Emmer in the House you actually has proposed excellent legislation to address that issue.

Representative Arrington. Thank you.

Mr. Werbach, would you agree? And what you would add to that?

Mr. Werbach. Thank you, Congressman.

I would agree with that. I think we all agree that stablecoins are an area where there needs to be some investigation. We may not all agree on precisely what that should entail or whether additional legislation is needed, but I think we would agree that there are actors in that marketplace who are non-compliant, who purport not to do business in the U.S. and yet are listed on virtually every U.S. exchange.

So I think we might agree about something where there is a need for action. I think we might agree on this issue that Mr. Massad talked about in terms of the gap on spot market exchange regulation.

Again, not necessarily exactly what it looks like, but if there is third-party exchange then there needs to be some oversight for market integrity just as we have with other kinds of exchanges. And the fact that the split between the CFTC and the SEC is what it is, if that it just creates an unfortunate byproduct in this area.

Representative Arrington. Thank you.

Mr. Massad?

Mr. Massad. Yes.

Representative Arrington. And Ms. Goldstein in the final seconds here.

Mr. Massad. First I am pleased that Mr. Van Valkenburgh agrees on the stock market. And just to clarify, a lot of people think while it is either a security or a commodity so that means the SEC and the CFTC just have to decide how to regulate this, which one is going to do it. That is not the case.

The SEC can only regulate the digital assets that are securities. The CFTC regulates futures and swaps that are based on those

other digital tokens and even sometimes on digital tokens that are securities. But again, that means the CFTC can regulate bitcoin futures the same way it regulates cattle futures.

But the CFTC doesn't regulate the buying and selling of cows, nobody regulates the buying and selling of bitcoin, it just—other than the States, but that is a very light touch.

The other thing I think we might be able to agree on is the importance of KYC, know your customer an anti-money laundering. The system we have now is essentially trying to check that at what we call the on ramps and the off ramps. So as you go into the crypto market, or come out of crypto market and exchange that for dollars, that is good and I think FinCEN has done a pretty good job there.

But where we might start to differ is as the cryptomarket grows and you are able to do more and more things with crypto and you don't have to cash out, how do we prevent that illicit activity then? That is where it gets tougher, where what do we do about what is called unhosted wallets? What do we do about DeFi transactions?

How do we have reasonable KYC that is risk based, that doesn't try to, you know, regulate every single transaction, that recognizes people are entitled to some privacy and we still have to prevent that illicit behavior. That is tricky.

Representative Arrington. Thank you, Mr. Massad. Mr. Chairman.

Ms. Goldstein. If the chair might allow.

Representative Arrington. Would you indulge a final comment from the witness?

Chairman Beyer. Absolutely.

Representative Arrington. He is never this nice to me, by the way, when you are not around.

Ms. Goldstein. I appreciate the flexibility and I appreciate all the fellow witnesses' comments. I thank Mr. Van Valkenburgh and I certainly agree that crypto tech is very difficult. I think we may disagree about the solution. I would prefer the base infrastructure above tech.

I think two things we may all agree on, there are laws that apply currently to digital asset marketplaces and those laws should be enforced. And the other thing that maybe we could agree on is that the market data could be a lot better. Right now, we really rely on the exchanges themselves to self report. And I think some standardization of that market data is something we could potentially all agree on.

Representative Arrington. Excellent. Thank you.

Thank you, Mr. Chairman.

Chairman Beyer. And I want to announce our next hearing, it will be on cryptocurrency forks.

I recognize the penultimate questioner. Apparently Senator Cruz is on his way. And a vote has just been called in the House so the distinguished gentleman from Madison.

Representative Pocan. This has been a great education, perhaps I will say for someone like myself that isn't super well versed in cryptocurrency. I spend much of my time thinking about the 40 percent of the people who don't have $400 in the bank for emergency expense.

And so I guess the questions I am going to ask are more based on the calls we get into our office. I know that in about an 8-month period just recently I think from October 2020 to May 2021, 7,000 people reported scams to the tune of about $80 million in cryptocurrency or crypto scams really. It is not necessarily in currency.

Ms. Goldstein, I am just kind of curious, what are some of the inherent risks to digital assets that aren't necessarily in traditional investments? And specifically what are some of the areas as regulators should be in investigating in this space to protect consumers, that average person who calls a congressional office, who doesn't follow cryptocurrency anywhere near the level of discussion we had today?

Ms. Goldstein. Well, thank you for the question, Congressman, I think there is a lot of different risks in the digital asset marketplace that are particularly unique. One is that individual users are sort of—they need to manage the counterparty risk themselves in a way that you traditionally wouldn't in the banking system. Right? You have a bank account and FDIC insurance, you are not worrying about who is on the other side.

That is also true if you are trading stocks. Right? You might rely on SIPC. And you pretty much can guarantee that if you trade a stock at the end of the day you will probably get it. Right? And there are protections in place, because we have markets and those markets have rules. You don't necessarily know that that is true when in gauging in some of the cryptocurrency transactions.

I think some of the other risks are the kind of scams that you are getting calls about. Right? We mentioned the Squid coin. Right? The ability to create these tokens that you can buy and then never sell. And if you are not able to read the code to identify that when you are purchasing a token, you may fall prey to that scam.

There is also a potential for market manipulation. There is a lot of really big what they call whales, whether those are crypto hedge funds or exchanges that have prompt trading arms that are owned by CEOs, whatever it may be, there is real potential here for market manipulation.

There is even a whole technical term for it, minor extractable value, which is the ability of cryptocurrency minors to sort of rearrange transactions in a way that they profit from.

So all of this would benefit obviously from existing laws being enforced, but also perhaps to the extent that you and Congress see that there are gaps, making sure that the rules that we are used to in this sort of traditional markets are applied here so that individual investors aren't subject to these kinds of market manipulations.

Representative Pocan. If you crank it up a couple notches, so rather than an individual getting scammed, are we at any risk of having a broader more systemic risk to our country? And what specific kind of regulatory effects do we need to do in order to safeguard against that?

Ms. Goldstein. Well, Congressman, I think it is a great question and it is a hard one to answer because the market is very opaque right now. And there are a lot of entities that are private funds, whether they are family offices, or hedge funds—hedge funds do

some basic reporting, but they are not required to report their cryptocurrency transactions on the form 13-F that the SEC make them file every quarter. Family offices have no reporting requirements whatsoever.

So it is a little hard to tell that we have industry data. Right? We know that institutional investors are more and more interested, private funds in particular in getting in this space. And what I think about, what I worry about is contagion.

So I think about Archegos. Right? That was one family office that was—that was able to cost billions of dollars in losses to banks who all happen to be on the side of same basket of trades. If big—too big to fail banks are also counterparties to hedge funds who also have big cryptocurrency portfolios and there is volatility in that market that may lead them to sell noncrypto assets, and they are all selling noncrypto assets at the same time, you could lead to a spiral which could perhaps impact the economy.

So that is the way I am thinking about contagion given the limited data that we have to really understand the complete picture.

Representative Pocan. Well, I look forward to however this conversation, Mr. Chairman, continues. I know our colleague—former colleague, Jared Polis, was quite successful in this area. But he was quite successful to begin with.

You know, I think what I am looking for on that average call we get into the office, someone who didn't have a lot of money to begin with and tried something and got scammed, just make sure that we have the right regulatory network to protect that person.

So I yield back. Thank you very much.

Chairman Beyer. Thank you, Congressman Pocan.

Now the distinguished Senator from Arizona, Senator Kelly.

Senator Kelly. Thank you, Mr. Chairman and thank you everybody for being here today. I really appreciate it.

Ms. Goldstein, a question about stablecoins but first of all a new technology is something I am always very interested in innovation. I think it is one of the things our country does so well.

But and I am concerned about cryptocurrency and unstablecoins, and one aspect of stablecoins is that in theory provide a bit more stability, linking the coin to a reserve, but key issue to address as it relates to stablecoins is insuring sufficient transparency to protect the users, the folks who buy stablecoins.

So how do we ensure that there are—is sufficient transparency about the reserves utilized in stabilizing the coins value?

So could you talk a little bit about that transparency and the requirements for disclosure if there are some.

Ms. Goldstein. Thank you for the question, Senator. I think there are a lot of different ways that we could approach this problem and it sort of depends on the State locally. Right? Some stablecoins are algorithmic, and they have a basket of assets and they move around, some are meant to be pegged to the dollar or another Fiat currency.

And I think there are a lot of different places that regulators could approach this problem. Some stablecoins may be securities, but should be regulated by the SEC which would bring a substantial amount of transparency. The Presidential Working Group has

considered, you know, that the prudential regulators have asked Congress to look into doing some legislation around stablecoins.

There is also a role for FinCEN to play and make sure that stablecoin issuers who are doing redemptions and also issuing these new stablecoins aren't doing anything that involves any sort of financial crimes. There is also I think an important piece about stablecoins, which is that DeFi doesn't work without stablecoin.

And that is a new and emerging piece of this marketplace. It is operating in some cases without adherence to solve our existing laws, like know your customer, anti-money laundering, compliance and combating terrorist financing.

So I think unfortunately there is no easy answer. There is perhaps a role for every single regulator and of course the role for State Attorneys General. Right? I actually think that Tether might be a bit behind that they are supposed to give a quarterly disclosure of their reserves and I am not quite sure that they have done that on time. So there is also a goal for State law enforcement as well.

Senator Kelly. So in general, do you feel we need more transparency and disclosure than we have today with regard to stablecoins?

Ms. Goldstein. I think that that would be helpful, but I also think that the regulators have a number of tools to ensure that currently. And I would encourage them to use the tools they currently have to maybe have that happen.

Senator Kelly. Thank you, Ms. Goldstein.

And Mr. Chairman, I yield back the remainder of my time.

Chairman Beyer. Senator, thank you very much.

And our ultimate questioner, the distinguished Senator from Texas, Senator Cruz.

Senator Cruz. Thank you, Mr. Chairman. And I appreciate the adjective as the ultimate questioner. I will take that with a chuckle.

You know, I have to say, I think cryptocurrency and bitcoin mining provide enormous opportunities. They are creating vast amounts of wealth, they are creating a hedge for people against inflation. Inflation is a growing concern across the country. They are creating entrepreneurs in all 50 States.

I am also particularly proud that my home State of Texas is becoming an oasis for the blockchain community, for bitcoin miners, for innovators, and entrepreneurs in the crypto world. Unfortunately, the one thing that is capable of screwing all of this up is the United States Congress. And I have deep concerns that Congress is already in the process of doing so.

As most people watching this hearing know, in the recently passed so-called bipartisan infrastructure bill, there are provisions targeting and inflicting enormous harms on the crypto industry.

As originally drafted, the infrastructure packaged a provision that expands the definition of broker to nearly all participants in the cryptocurrency structure, treating them as a financial institution, which means they have to report consumer information to the IRS, even if those participants don't have access to that information.

Additionally, the infrastructure bill included language incorporating digital assets under section 6050I of the Internal Revenue Code which states that in a broad range of scenarios, any person who receives over $10,000 in digital assets must verify the sender's personal information, including Social Security number, and sign and submit a report to the government within 15 days. And failure to comply results in mandatory fines and can be a felony with up to 5 years in prison.

We have seen how crypto poses a threat to totalitarian regimes. For that reason, the Chinese communist government recently acted to ban bitcoin mining. And the sad reality of Congress legislating in this matter, I can speak at least for the Senate, I doubt there are five Members of the United States Senate that could tell you what the hell a Bitcoin is. And legislating is always a messy process, but when it comes to legislating in an area where most Members of this body have very little familiarity of the details, it is highly perilous.

So Mr. Van Valkenburgh, your testimony has addressed many of these concerns, but can you share what the impact is of the provisions in the bill just signed into law? And in particular address what I have this week introduced stand alone legislation that would repeal these crypto provisions. And should Congress legislate in this area? Almost certainly, but it should do so after an awful lot of hearings and awful lot of learning what is going on. And it should do so with an eye to not destroying this industry rather than simply using a machete and letting the consequences fall on the American people.

Mr. Van Valkenburgh. Thank you, Senator. I strongly agree the 6050 reporting requirement represents a rather grave threat to personal privacy and the fact I believe it is in contravention of our Fourth Amendment rights, to not have our personal papers searched without a warrant.

The Fourth Amendment protects our private papers when we keep them in our homes and when we have them on our persons. The Bank Secrecy Act which is our know your customers rules and anti-money laundering rules is constitutional because those reports are filed by third parties, by banks where the customer voluntarily provides their private information to the third party, and the third party holds it for a legitimate business purpose.

The U.S. Supreme Court found that to be constitutional then if the governments gets that information without a warrant which is the Bank Secrecy Act is constitutional to this day. It is also why the government can go to Google and get your gmail email history without a warrant. That was a compromise and a reading of the over the Fourth Amendment of the Supreme Court came up with in 1970 in *California Bankers Association* v. *Shultz and Miller*.

Now in the 6050I reporting context, please tell me who the third party is to a two-party transaction where someone received more than $10,000 worth of bitcoin? There is no third party so how can the third party doctrine make a warrant unnecessary for the collection of that very intimate information, a Social Security number.

Senator Cruz. And let me ask you if this new legislative provision particularly if it is enforced aggressively by the Biden Treasury Department and Biden IRS, if it succeeds in decimating the

bitcoin and crypto industry in driving it overseas, is that good or bad for America?

Mr. Van Valkenburgh. Well, I believe it would be bad. However, I am optimistic. The provision doesn't go into effect until 2024. There are very reasonable and I think strong constitutional arguments to invalidate it before that happens.

And I also think a lot of folks in Treasury have the right idea about this stuff and would actually agree that some level of privacy protections are important. So I don't think we are on the cusp of apocalypse as of yet.

Senator Cruz. Well, I hope you are right. And I hope Congress also acts to avoid apocalypse without rolling the dice and seeing if that prediction is right or wrong.

Chairman Beyer. Only appropriate that the ultimate questioner brings up the apocalypse.

Thank all of you very much for gathering with us. It has been a fascinating conversation. I promise every one of our other panelists up here, Democratic and Republican, really enjoyed learning a lot more about cryptocurrency. I personally would love to learn how to become a backup, a miner, Ms. Goldstein. Although, when I was in Glasgow last week, at least more than one were talking about the energy impacts of mining, and this contribution to climate change.

So formally let me thank you for this important conversation on a very complex topic, digital assets and cryptocurrencies have grown to become a globally significant financial market. Understanding these new and complicated forms of financial assets, activities, and products is necessary for Congress to address both the risks and benefits of this growing technology and hopefully to do it in a balanced way that doesn't stifle innovation, that doesn't chase it overseas, but it makes sure that we are doing all the kind of protections that we need.

I thank each of you for your timely contributions. Thank you for written remarks that are ten times longer than what you offer verbally which are excellent ideas. And thank all my colleagues who have all gone to vote for their part in this discussion.

This record will remain open for three days. This hearing is now adjourned.

[Whereupon, at 5:10 p.m., Wednesday, November 17, 2021, the hearing was adjourned.]

SUBMISSIONS FOR THE RECORD

PREPARED STATEMENT OF HON. DONALD BEYER JR., CHAIRMAN, JOINT ECONOMIC COMMITTEE

RECOGNITIONS

This hearing will come to order. I would like to welcome everyone to the Joint Economic Committee's hearing titled "Demystifying Crypto: Digital Assets and the Role of Government."

I want to thank each of our truly distinguished witnesses for sharing their expertise today. Now, I would like to turn to my opening statement.

STATEMENT

Since the introduction of Bitcoin in 2009, the market for cryptocurrencies and other digital assets has expanded from a niche product to a globally significant asset worth nearly three trillion dollars just last week. While this rapid rise in value has made some early adopters quite wealthy, it also poses an array of risks to both everyday investors and the broader financial system.

The purpose of this hearing is to explore emerging trends in the digital asset market and discuss prudent steps that Congress and the Federal Government can take to update our regulatory framework and bring much-needed clarity to issuers, ensure transparency for investors, and protect the integrity of our financial system—while also leveraging exciting developments in blockchain technology. Congress can promote responsible innovation in this market while also providing basic protections to the investing public.

Interest and involvement in the digital asset market has become increasingly mainstream in recent years. The growth of these products has been especially pronounced since the start of the coronavirus pandemic, as the reported total market value of all digital assets soared from two hundred billion dollars in January 2020 to nearly three trillion dollars today.

As the market has grown, we have seen digital asset investors broaden from a narrow group of true believers in cryptocurrencies to an expanding community that includes everyday investors. A Pew survey conducted this fall found that sixteen percent of American adults have personally owned or invested in a cryptocurrency at some point, up from just one percent who reported holding Bitcoin in 2015. While many early Bitcoin transactions occurred on little-known online platforms, today, investors can buy digital asset through Robinhood or Venmo, or on large exchanges run by publicly-traded companies like Coinbase.

But this growth in value and interest presents a number of challenges for our economy. The current digital asset market structure and accompanying regulatory framework are ambiguous and risky for both investors and the broader economy. Digital asset holders have been subjected to a market that is, as SEC Chairman Gary Gensler described it "rife with fraud, scams, and abuse".

The mainstreaming of digital assets is laying the foundation for huge swaths of the economy to invest in this market. Increased crypto market volatility or a digital bank-run could disrupt more mainstream financial institutions like pension funds or mutual funds. And the underlying assets can create significant consumer protection issues given existing patterns of financial fraud, hacks, and market manipulation.

Retail investors may be lured in by the hype around a new coin with improbably high rates of return, only to be caught on the wrong end of a speculative bubble and lose their entire investment. A recent example was "Squid", a blatant scam token that used the excitement around the popular TV show Squid Game to dupe unwitting investors out of 3.3 million dollars.

While all investments involve risk, the lack of disclosure and reporting requirements in many parts of the crypto asset industry tilt the playing field toward the largest investors who can leverage their size to exploit regulatory gaps at the expense of retail investors. It is currently difficult for regulators to prevent market manipulation by large players who can exploit their access to multiple sides of a trade, or trade on inside information.

Despite these issues, Congress has not yet weighed in on a comprehensive legal framework around these assets.

Updating the U.S. regulatory framework for digital assets would be in line with how officials have often responded to past financial innovations with stronger rules to protect consumers and market integrity. For example, Dodd-Frank created stronger rules on complex swaps and derivatives in the wake of the 2008 financial crisis.

Updated regulation can also reduce the likelihood that these emerging developments would destabilize financial markets and the broader economy. For example,

the largest stablecoin Tether was recently found to not hold sufficient reserves of cash and equivalents to fully back their seventy billion dollar value. Applying additional regulatory scrutiny to assets like Tether, and the platforms where they are used, could ensure that cracks in one asset don't spread to the broader economy.

Increasing reporting requirements for decentralized finance platforms will shine a light on a fast-growing but lightly regulated segment of the market. Increased information sharing would also improve tax compliance for capital gains from the sale of crypto assets.

The many issues we will discuss today are why I introduced the Digital Asset Market Structure and Investor Protection Act earlier this year. This legislation would establish much-needed guardrails and provide clarity to regulators and investors without stifling innovation. The present moment gives us an opportunity to take action before a potential crisis hits the broader economy.

I am looking forward to learning from each of our witnesses today.

PREPARED STATEMENT OF HON. MIKE LEE, RANKING MEMBER,
JOINT ECONOMIC COMMITTEE

Throughout the history of this great nation, entrepreneurs and creators have served as the heartbeat of the American economy and the engine of America's growth. Their advances into unknown frontiers of science and technology have transformed the quality of life for millions of Americans, and for people around the world.

Today, American innovators are advancing into the unknown frontiers of cryptocurrencies, using novel technologies to securely create and trade digitally scarce assets. Like the internet of the 1990s, cryptocurrencies are still in their infancy. This evolving technology has vast—and still untapped—potential to revolutionize established industries and create entirely new ones.

Cryptocurrencies are already democratizing finance by lowering costs and expanding access to an industry that has historically been hard to reach for millions of Americans, including hundreds of thousands of Utahns.

Beyond the better-known applications to finance, blockchain—the technology behind cryptocurrencies—has even broader potential. Blockchain can securely share health records, efficiently track cross-border transactions in global supply chains, and allow online consumers to verify the authenticity of pictures or videos.

I have great optimism that, like the internet before it, the technology behind cryptocurrencies will create a wealth of new opportunities, many of which we cannot yet imagine.

As new markets like this one emerge and grow, there is always a temptation in Washington to expand the Federal Government's reach—a temptation to centrally control the innovative process and regulate the products of those individuals who are at the forefront of American advancement.

This temptation must be resisted.

Rigid, one-size-fits-all regulation targeted at the cryptocurrency economy is unnecessary, and it will all but ensure that this next generation of technology companies moves to other countries. Americans could lose access to cryptocurrency markets and miss out on the potential economic and social benefits.

If we want the center of innovation to remain here in the United States, for the benefit of American workers and American families, Congress should focus on creating clarity around how existing rules apply to these new technologies. In the case that existing law proves outdated, we can assess the need for new rules. However, as it stands today, we just need to appropriately apply the rules we already have on the books.

The proper role of government is to empower innovation through clear rules with a light touch. The best approach is one where Congress acts in a manner that is tailored to its limited constitutional authority. It is one where the Federal Government acts with restraint, and in so doing, protects the creation and ingenuity that powers our great country.

In today's hearing, I hope that we can focus on policies that protect a flexible regulatory framework for the Americans who are building our future.

If we can resist centralizing power in Washington, and preserve the space for American innovation to flourish, entrepreneurs across the country stand ready to unleash the tremendous opportunity of new digital economies.

Thank you.

Written Testimony of Alexis Goldstein
Director of Financial Policy, Open Markets Institute

United States Congress
Joint Economic Committee

"Demystifying Crypto: Digital Assets and the Role of Government"

November 17, 2021

Chair Beyer, Ranking Member Lee, and Members of the Committee:

Thank you for inviting me to testify at this hearing. I am Director of Financial Policy at the Open Markets Institute, where my work focuses on financial regulatory policy and investor and consumer protection. Previously, I worked as a programmer at Morgan Stanley in electronic trading, and as a business analyst at Merrill Lynch and Deutsche Bank focused on equity derivatives. There, I worked primarily as a product manager for the trading and risk management software used by the global equity options flow trading desks.

I want to start by thanking the Committee for holding today's hearing. I would like to highlight several areas that the Committee may wish to examine further, including consumer and investor protections, concentration and centralization, cyber security, and national security concerns.

Broad Investor and Consumer Protection Concerns

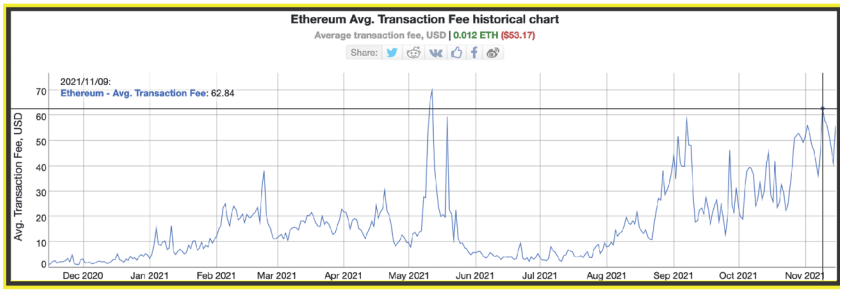
New Users with the Least Assets Often Pay Disproportionately High Fees

While crypto firms market their products as having the benefit of "democratizing" access to investments and credit, in truth, crypto markets often replicate the same problems present in traditional financial markets. For example, one of the problems with existing financial firms is that users with the least money often pay the highest proportional fees. This problem is largely replicated in the digital asset markets. For example, Coinbase has two cryptocurrency exchange platforms: Coinbase, and Coinbase Pro. Coinbase is aimed at newer users — but charges astronomically higher fees than its Coinbase Pro offering: it costs $0.99 to purchase $5 worth of Bitcoin on Coinbase, but only $0.02 to do so on Coinbase Pro. Another example is that users with smaller amounts to invest may face higher fees than they could overcome with trading returns or interest income. The crypto borrowing and lending platform Aave, which allows users to deposit crypto assets and earn rewards, and use their crypto as collateral for borrowing, is explicit about this in its FAQ, writing "You can deposit any amount you want, there is no

minimum or maximum limit. Still, it's important to take into account that for really low amounts it is possible that the transaction cost of the process is higher than the expected earnings. It is recommended that you consider this when depositing very low amounts".[1]

The Ethereum blockchain remains the dominant blockchain for DeFi, with an estimated 70% of all decentralized finance ("DeFi") activity, according to an analysis by JPMorgan.[2] Ethereum continues to face challenges of scalability, congestion, and extremely high fees that make DeFi transactions prohibitively expensive for users with smaller holdings.[3]

The average Ethereum transaction fee was $62.84 on November 9th, 2021, according to bitinfocharts.com[4]:



Via BitInfoCharts.com, accessed November 15, 2021

Ethereum network fees to merely transfer a crypto asset from one wallet to another were an estimated $22 on November 5th, and some $54 on November 11th.[5]

---

[1] https://docs.aave.com/faq/depositing-and-earning

[2] Joanna Ossinger, "JPMorgan Team Suggests Crypto's DeFi Boom Slower Than It Seems", Bloomberg, Nov 12, 2021, https://www.bloomberg.com/news/articles/2021-11-12/jpmorgan-team-suggests-crypto-s-defi-boom-slower-than-it-seems ("The Ethereum network now has about a 70% share of DeFi activity, versus a near-total lock at the start of the year, the team added.")

[3] See: Liesl Eichholz, "Avalanche: The New DeFi Blockchain Explained", Glassnode, February 10, 2021, https://insights.glassnode.com/avalanche-the-new-defi-blockchain-explained/. ("With the price of ETH on the rise, even basic token swaps on Ethereum are becoming prohibitively expensive for entry-level players, while interactions with more complex DeFi contracts can come attached with fees exceeding 0.1 ETH (over $170 at the time of writing)."); and Nivesh Rustgi, "Ethereum Miners Earn Record $110M Amid ETH Crash", Crypto Briefing, May 21, 2021, https://cryptobriefing.com/ethereum-miners-earn-record-110-million-amid-eth-crash/. ("The gas fees essentially rendered the [Ethereum] network unusable for users with smaller holdings, while those trying to save their loans or enter new positions suffered longer wait times due to the surge in activity").

[4] https://bitinfocharts.com/comparison/ethereum-transactionfees.html#1y

[5] https://etherscan.io/gastracker, accessed November 5, 2021, 6pm ET; and accessed November 11, 2021 at 9:45pm ET.

Insider Trading Concerns

A number of aspects of digital asset markets may help enable insider trading: lack of regulation and enforcement, failure to disclose potential conflicts, and pseudonymity — particularly in decentralized finance ("DeFi"), a term broadly used to refer to platforms that allow a user to trade, lend, or borrow cryptocurrency assets, typically without any Know Your Customer (KYC) or Anti-Money Laundering (AML) compliance.

This September, the head of Product for the largest NFT platform, OpenSea, was accused of insider trading. CNBC reported that Nate Chastain would purchase NFTs right before they were listed on the homepage.[6] He did so from an anonymous wallet, but users/analysts happened to notice the suspicious activity.[7]

In October, a blockchain analyst discovered that the venture capital firm Divergence Ventures extensively profited off insider information they obtained from one of their investments, by gaming an "airdrop." Airdrops are giveaways of newly created crypto tokens. Many projects give a portion of these airdrops to themselves and to their investors, and another portion to their historical users.[8] Ribbon Finance told its investors that an airdrop was coming in the future. One of their investors, Divergence Ventures, set up dozens of crypto wallets so they could receive dozens of airdrops. This technique is referred to in the crypto community as "sybil farming" an airdrop.[9]

The incident raised many questions, such as: how prevalent is this type of insider trading among venture capital investors. Divergence stated "we aren't the only one that has tried this tactic",[10] and the head of research for the crypto publication *The Block* tweeted "the world suddenly discovered that basically every fund/whale Sybil farms airdrops".[11]

Honeypots and Rug Pulls

Crypto firms purport to be on the cutting edge of technology, however a lack of regulatory oversight and legal accountability often leads to worse cybersecurity and data privacy outcomes

---

[6] MacKenzie Sigalos, "There was insider trading on NFT platform OpenSea, the $1.5 billion start-up admits", CNBC, Sep 15, 2021, https://www.cnbc.com/2021/09/15/opensea-insider-trading-rumors-are-true.html.
[7] https://twitter.com/0xZuwu/status/1437921263394115584
[8] One example of an historical airdrop is the one that the Uniswap platform did September 2020. They created, and then gave away, 1 billion UNI tokens to investors, the core development team, a newly-formed "Treasury", and historical users.
Of the 1 billion tokens, 100,613,600 of them were sent to 251,534 crypto wallets that used Uniswap prior to September 1, 2020. Each of these wallets received 400 UNI each, worth approximately $1,400 at the time.
[9] Liam Kelly, "How DeFi Airdrops Incentivize Multiple Ethereum Wallets", Decrypt, Oct 23, 2021, https://decrypt.co/84223/airdrops-are-inflating-the-number-of-defi-users.
[10] https://twitter.com/divdotvc/status/1446688802043359237 (From Divergence's posted statement, ""Look, you and I both know we aren't the only one that has tried this tactic").
[11] https://twitter.com/lawmaster/status/1447082960465928197 ("Now that the world suddenly discovered that basically every fund/whale Sybil farms airdrops, how accurate do you think those user numbers are now anon?")

for users of trading platforms. There is an attitude in crypto markets that some refer to as “do your own research” (often referred to by an acronym, “DYOR”) where users who are duped are often treated as if they should have known better. This deflects responsibility from the platforms who may have failed to adhere to regulatory protections.[12]

There are certain basic assumptions in traditional financial markets, including that, barring a serious liquidity crisis, you will be able to sell back a product that you buy. But in digital asset markets, malicious actors can design tokens that can be bought, but not sold. Such actors can then use DeFi platforms like Uniswap, SpookySwap, and Trader Joe to create a new “liquidity pool”: a pair of two tokens locked in a “smart contract” (these are digital contracts stored on a blockchain that automatically execute once certain conditions are met[13]). The liquidity pool is then used to facilitate trades between the two tokens on a decentralized exchange[14]. Once a liquidity pool exists, the makers of the so-called “honeypot” tokens[15] can attract new buyers, and once enough have purchased the token, the scammer pulls out all the liquidity, crashing the token price and making off with the money.

One recent example of this phenomenon is the Squid Game token, which was a token that could be purchased but not sold, but gained considerable popularity following a series of uncritical headlines in the financial press, touting its 83,000% gains, all before the anonymous development team pulled all the liquidity out of the project -- causing the price of Squid Coin to plummet to zero (a technique known as a “rug pull”).[16]

Scams are prevalent enough that some DeFi websites include an explicit warning on their website if you attempt to import a custom token (by searching for the token by its alpha-numeric address). For example, the Avalanche blockchain-based exchange Trader Joe displays the following warning when you import a custom token[17]:

---

[12] As the Binance Academy explains in its entry on DYOR, “Shilling is a common practice in cryptocurrency where people tend to advertise the coins that they own in hopes of positively affecting the price. Quite often, it can be difficult to distinguish the difference between a shill or an unbiased post...People with malicious intent can quickly create multiple fake accounts, attempting to trick investors into purchasing a cryptocurrency based on a ‘popular’ post within a social media platform.” https://academy.binance.com/en/glossary/do-your-own-research.

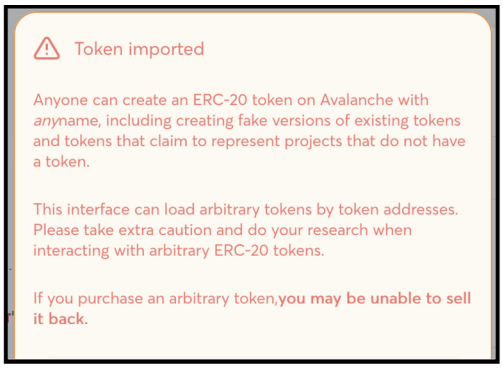
[13] IBM, “ What are smart contracts on blockchain?”, https://www.ibm.com/topics/smart-contracts.

[14] Gemini, “What Are Liquidity Pools?”, Cryptoacademy, https://www.gemini.com/cryptopedia/what-is-a-liquidity-pool-crypto-market-liquidity.

[15] John Biggs, “Clever Ethereum honeypot lets coins come in but won’t let them back out”, Tech Crunch, Feb 16, 2018, https://techcrunch.com/2018/02/16/clever-ethereum-honeypot-lets-coins-come-in-but-wont-let-them-back-out/.

[16] Matt Novak, “Squid Game Cryptocurrency Scammers Make Off With $3.3 Million”, Gizmodo, Nov 1, 2021, https://gizmodo.com/squid-game-cryptocurrency-scammers-make-off-with-2-1-m-1847972824.

[17] TraderJoe.xyz, accessed November 15, 2021.

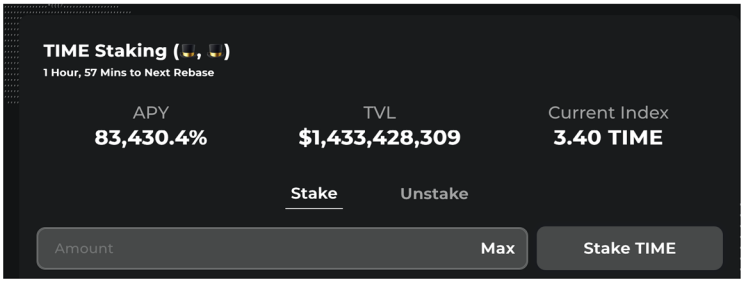


Fast-moving APRs with unclear terms

Many DeFi applications offer rewards to users if they lock (i.e., temporarily removing your ability to trade or move them) a single crypto asset, or a pair of assets, on the platform.[18] These rewards are billed as interest and listed with Annual Percentage Rates (APRs) or Annual Percentage Yields (APYs), and are sometimes paid in the same crypto you've locked, but may also be paid in another cryptocurrency entirely. According to self-reported industry data, these arrangements are increasingly popular: as of November 15, 2021, there was $111.93 billion locked into DeFi,[19] an over 130% growth from less than five months ago.[20]

One DeFi platform called Wonderland.Money, which is a fork of the Ethereum-based OlympusDAO project,[21] offers eye-popping, five-figure APRs in exchange for locking a crypto token called TIME into the platform:

[18] Brady Dale, "What Is Yield Farming? The Rocket Fuel of DeFi, Explained", Coin Desk, Jul 6, 2021, https://www.coindesk.com/defi-yield-farming-comp-token-explained.
[19] https://defipulse.com/, accessed November 15, 2021.
[20] Alexis Goldstein, Written Testimony, "America on "FIRE": Will the Crypto Frenzy Lead to Financial Independence and Early Retirement or Financial Ruin?", U.S. House of Representatives Committee on Financial Services Subcommittee on Oversight and Investigations, June 30, 2021, https://financialservices.house.gov/uploadedfiles/hhrg-117-ba09-wstate-goldsteina-20210630-u1.pdf ("According to DeFi Pulse, as of June 28th there are $48.23 billion in crypto assets locked in DeFi.")
[21] Owen Fernau, "OlympusDAO's Success Inspires Dozens of Forks", Yahoo, https://www.yahoo.com/now/olympusdao-success-inspires-dozens-forks-171914320.html. ("In the case of OlympusDAO, Daniele Sesta, who co-founded Wonderland, as well as the collateralized debt position protocol Abracadabra, told his 101,000 Twitter followers that he has plans to differentiate the forked product.")



Screenshot from Wonderland.Money (https://app.wonderland.money/#/stake), displaying a 83,430% APY for staking the crypto asset TIME, accessed November 15, 2021.

Wonderland runs on the Avalanche blockchain, and claims that its TIME token is backed by "a basket of assets" including the stablecoin "Magic Internet Money", and promises this gives it "an intrinsic value it cannot fall below", although it is unclear how the platform can make such a promise, nor do they disclose precisely what the level it cannot fall below.[22]

Other DeFi projects have shown these wild APRs to be either deeply misleading and/or extremely fleeting. For example, on June 28th at 9:09am ET, the Pancake Swap Twitter account tweeted a screenshot of an available 745,000% APR[23] if a user locked in a pair of stablecoins: US Dollar Coin[24] and Tether[25]. (Tether and the company that runs it, Bitfinex, have been barred from doing business in New York state under the terms of a settlement reached with Attorney General Letiticia James;[26] Tether and Bitfinex also paid $42.5 million in October to settle charges with the Commodity Futures Trading Commission of making untrue or misleading statements and omissions of material fact in connection with the Tether stablecoin[27])

[22] https://docs.wonderland.money/ ("Wonderland is the first decentralized reserve currency protocol available on the Avalanche Network based on the TIME token. Each TIME token is backed by a basket of assets (e.g., MIM, TIME-AVAX LP Tokens etc etc) in the Wonderland treasury, giving it an intrinsic value that it cannot fall below.")
[23] https://twitter.com/PancakeSwap/status/1409499271519297545
[24] USDC is a stablecoin jointly run by the cryptocurrency exchange Coinbase and the startup Circle. https://blog.coinbase.com/coinbase-and-circle-announce-the-launch-of-usdc-a-digital-dollar-2cd6548d23.
[25] Tether is a stablecoin run by Finex Inc., which operates the cryptocurrency exchange Bitfinex.
[26] "NY Bans Tether, Bitfinex Over False Statements About Dollar Backing and Losses", NBC New York, Feb 23, 2021, https://www.nbcnewyork.com/news/business/ny-bans-tether-bitfinex-over-false-statements-about-dollar-backing-and-losses/2904206/; and Attorney General of the State of New York, Investor Protection Bureau, https://ag.ny.gov/sites/default/files/2021.02.17_-_settlement_agreement_-_execution_version.b-t_signed-c2_oag_signed.pdf.
[27] Commodity Futures Trading Commission, "CFTC Orders Tether and Bitfinex to Pay Fines Totaling $42.5 Million", Oct 15, 2021, https://www.cftc.gov/PressRoom/PressReleases/8450-21.

Pancake Swap's Twitter account advertising an 745,000% APR if a user locked in a pair of stablecoins: US Dollar Coin and Tether, June 28th, 2021 at 9:09am ET.

Twitter users noted in the replies that when they visited the PancakeSwap website to try and obtain the staggeringly high APR, it was nowhere close to being in the same order of magnitude, but rather in the 30-38% APR range.[28] When I visited PancakeSwap's "Farms" page at 9:50am, less than an hour after the tweet was posted, I saw an APR of 15.77% for the USDC-USDT pair.

While PancakeSwap offers a rudimentary explanation of how these interest rates work in its documentation section,[29] this information is not presented on or linked to the main Farms page, nor does it present the user with any terms or conditions to evaluate. While other platforms offer better explanations of how and why the APR offered by liquidity providers in yield farms might fluctuate, even with considerable explanation it may not be clear to users just how highly variable the interest rates are.[30]

Prevalence of Forced Arbitration Clauses and Class Action Bans

In traditional financial markets, consumers and investors are often subject to forced arbitration clauses and bans on class action lawsuits. These forced arbitration clauses prevent users from suing financial firms in a court of law, instead conducting dispute resolution in private arbitration, where the outcomes are typically secret and there is no right to appeal. Curiously, many crypto websites, including DeFi sites, require users to sign forced arbitration agreements while also claiming to be decentralized autonomous organizations (DAOs) with no responsibility for

[28] See, e.g.: "Down 745 to 30% apr in 30 min." https://twitter.com/TomGuerrier/status/1409505537138565122.
[29] "Yield Farming", Pancake Swap, https://docs.pancakeswap.finance/products/yield-farming. ("Yield Farm APR calculation includes both the rewards earned through providing liquidity and rewards earned staking LP [liquidity provider] Tokens in the Farm. Previously, rewards earned by LP Token-holders generated from trading fees were not included in Farm APR calculations. APR calculations now include these rewards, and better reflect the expected APR for Farm pairs.")
[30] More thorough explanations of the variability of rates offered in yield farming are documented on other websites, such as Unsiwap's explanation of liquidity providers and impermanent loss https://uniswap.org/docs/v2/advanced-topics/understanding-returns/; as well as curve.finance's liquidity pools explanation https://resources.curve.fi/base-features/understanding-curve.

conduct occurring on the platform. A review of 12 major cryptocurrency platforms showed forced arbitration and class action bans present in every single one's terms of service:

Platform	Category	Link to Terms	Forced Arbitration?	Class Action Ban?
Binance.US	Exchange	https://www.binance.us/en/terms-of-use	yes	yes
Coinbase	Exchange	https://www.coinbase.com/legal/user_agreement/united_states	yes	yes
FTX.us	Exchange	https://ftx.us/TermsOfService.pdf	yes	yes
Kraken	Exchange	https://www.kraken.com/en-us/legal	yes	yes
Maker (via Oasis.app)	Borrowing/Lending	https://oasis.app/terms	yes	yes
Curve Finance	Borrowing/Lending	https://gov.curve.fi/tos	yes	yes
Aave	Borrowing/Lending	https://aave.com/term-of-use/	yes	yes
yearn.finance	Asset Aggregator	https://gov.yearn.finance/tos	yes	yes
Rari Capital	Asset Aggregator	https://rari.capital/terms-conditions.html	yes	yes
Fei Protocol	Asset Aggregator	https://assets.fei.money/docs/fei_terms_of_service_03_18_21.pdf	yes	yes
Uniswap	Exchange (DeFi)	https://uniswap.org/terms-of-service/	yes	yes
dydx	Derivatives Exchange (DeFi)	https://dydx.exchange/terms	yes	yes

Users self-manage counterparty risk and the risk of hacks and scams.

There are a long list of potential scams and hacks that digital asset users can fall prey to. As Bobby Ong, co-founder of cryptocurrency data provider Coin Gecko tweeted, "Crypto is a very dangerous and adversarial place".[31] Many users report having their crypto stolen when an attacker gains access to the private keys in their self-hosted wallet[32]. There are many attempts by scammers to pose as customer support for these wallets[33], or as admins in chat rooms[34] for particular cryptocurrency projects, in order to gain the trust of a potential victim, and convince them to click malicious links or take other steps to reveal their private keys.

[31] https://twitter.com/bobbyong/status/1403881080902471680?s=21
[32] Examples: https://twitter.com/0xflim/status/1459673602874249216; and XX.
[33] Steve Kaaru, "Beware of latest scam: MetaMask warns of new phishing bot", Coin Geek, May 5, 2021, https://coingeek.com/beware-of-latest-scam-metamask-warns-of-new-phishing-bot/.
[34] Mikhail Sytnik, "Cryptoscam in Discord", Kaspersky Daily, Feb 4, 2021, https://usa.kaspersky.com/blog/cryptoscam-in-discord/24193/. ("Scammers are luring Discord users to a fake cryptocurrency exchange with the promise of free Bitcoin or Ethereum")

Scams and hacks are prevalent enough that there are websites[35], guides[36], and services devoted to identifying them. These include suggestions that users read the smart contract code of any cryptocurrency token they wish to purchase, looking out for common pitfalls—a fairly high bar for non-programmers.[37] New tokens will often partner with firms that offer audits of their code to signal that the product is valid and safe.[38]

In the last four months alone, digital assets markets have been hit with over $1 billion in hacks, exploits, and erroneous payments:

- The cryptocurrency protocol **bZx** had its private key compromised due to a phishing scam targeted at a member of its development team.[39] As of this writing, $55 million in crypto assets have been lost, with the potential of more losses to come. (November 2021)
- The Ethereum based DeFi platform **Cream Finance** lost $130 million due to a flash loan exploit. This is the third hack suffered by the platform.[40] (October 2021)
- A bug in an upgrade to the borrowing and lending platform **Compound** put $147 million worth of the platform's funds at risk.[41] (October 2021)
- The Ethereum blockchain-based **Indexed Finance** lost $16 million in a smart contract exploit. The platform believed they identified the hacker, but the hacker refused to return the funds.[42] (October 2021)
- The Avalanche-blockchain based platform **Vee Finance** was hacked for a total of $35 million.[43] (September 2021)
- The Avalanche blockchain-based **Zabu Finance** was exploited for $3.2 million.[44] (September 2021)
- The Binance Smart Chain-based **pNetwork** lost $12 Million in a hack.[45] (September 2021)

---

[35] See, e.g. https://tokensniffer.com/.
[36] See, e.g. https://coinmarketcap.com/alexandria/article/how-to-identify-and-avoid-uniswap-scams and https://www.cylynx.io/blog/the-rise-of-cryptocurrency-exit-scams-and-defi-rug-pulls/.
[37] See, e.g.: https://twitter.com/ahmedismail/status/1426141622287298569?s=21.
[38] "DeFi Audit Firms Seeing 'Overwhelming Demand' Even Amid Token Price Slump", Coin Desk, Oct 15, 2020, https://www.coindesk.com/defi-audit-firms-swamped. ("The separation between audited projects and non-audited projects became palpable over DeFi's boom months – often referred to as "DeFi Summer" – as code flaws in some projects led to contracts being exploited by hackers.")
[39] "bZx - REKT", Rekt News, Nov 6, 2021, https://rekt.news/bzx-rekt/.
[40] Scott Chipolina, "Cream Finance Suffers Third Hack, Loses Over $130 Million", Decrypt, Oct 27, 2021, https://decrypt.co/84590/cream-finance-suffers-third-hack-losing-over-130-million.
[41] "Compound - REKT", Rekt News, Oct 4, 2021, https://rekt.news/compound-rekt/.
[42] Rahul Nambiampurath, " Indexed Finance Attacker Refuses to Return Stolen $16M, Team Approaching Authorities", Be In Crypto, Oct 20, 2021, https://beincrypto.com/indexed-finance-attacker-refuses-return-16-million-authorities/.
[43] Camomile Shumba, "Avalanche-based DeFi platform Vee Finance says it's lost $35 million in ether and bitcoin in a crypto hack", Business Insider, Sep 22, 2021, https://markets.businessinsider.com/news/currencies/avalanche-vee-finance-crypto-hack-ether-bitcoin-defi-platform-lost-2021-9.
[44] Jamie Crawley, "Avalanche-Based Zabu Finance Sees $3.2M Hack", Coin Desk, Sep 13, 2021, https://www.coindesk.com/tech/2021/09/13/avalanche-based-zabu-finance-exploited-in-32m-hack/.
[45] Liam Frost, "DeFi Bridging Protocol pNetwork Suffers $12 Million Hack", Decrypt, Sep 20, 2021, https://decrypt.co/81301/defi-bridging-protocol-pnetwork-suffers-12-million-hack.

- **SushiSwap**'s token platform MISO lost $3 million due to a hack.[46] (September 2021)
- The cryptocurrency exchange **Bitfinex** (whose owners are also the issuers of the stablecoin Tether) paid over $23 million in Ethereum gas fees (7,676.61 ETH) in order to move $100,000 worth of Tether to deversifi.com[47], in a single transaction.[48] While the miner returned the majority of the gas fee, they appear to have kept 291 ETH – worth some $850,000.[49] (September 2021)
- **Poly Network** initially lost $613 million to a hacker exploiting a bug in their smart contract.[50] Many crypto market participants blacklisted the hackers address, leading to most of the funds eventually being returned.[51] (August 2021)

In a sign that exploits are increasing in severity and frequency, this is more than three times the amount lost to hackers in DeFi hacks and exploits from 2019 - April 2021.[52]

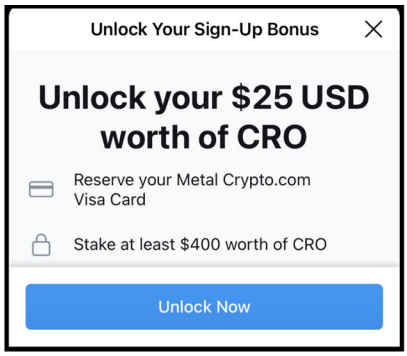
By contrast, in traditional financial markets, market intermediaries like broker-dealers and exchanges are subject to a host of cybersecurity and data privacy regulations and ongoing examinations.

Concerns Surrounding Potential False Advertising or Misleading Claims

There are also false advertising concerns in the space. For example, the exchange Crypto.com tells its users that it can get "$25 USD" if it refers a friend to its platform. But this referral bonus marketing in its mobile app makes it seem that the bonus is "$25 USD", when it is actually $25 in Crypto.com's own coin, CRO, and the user must meet certain criteria before accessing this CRO reward: either by signing up for the Crypto.com credit card, or purchasing a total of $400 worth of this CRO coin and "staking" it -- locking the CRO into the Crypto.com site for a certain period of time.[53]

---

[46] Andrew Asmakov, "SushiSwap's Token Launchpad Hacked for Over $3M in Ethereum", Decrypt, Sep 17, 2021, https://decrypt.co/81120/sushiswaps-token-launchpad-hacked-over-3m-ethereum.
[47] Harry Robertson, "A crypto exchange accidentally paid a $24 million fee for a $100,000 ethereum transaction - but the miner agreed to return it", Markets Insider, Sep 28, 2021, https://markets.businessinsider.com/news/currencies/crypto-exchange-bitfinex-ethereum-tether-transaction-fees-error-deversifi-2021-9.
[48] https://etherscan.io/tx/0x2c9931793876db33b1a9aad123ad4921dfb9cd5e59dbb78ce78f277759587115
[49] https://etherscan.io/tx/0x85294effd53126b3bfa9e7f655267e00ac1ae2ef76f4569644670bf5403637d6
[50] Gertrude Chavez-dreyfuss and Michelle Price, "Explainer: How hackers stole and returned $600 mln in tokens from Poly Network", Reuters, Aug 12, 2021, https://www.reuters.com/technology/how-hackers-stole-613-million-crypto-tokens-poly-network-2021-08-12/.
[51] Nicholas Weaver, "Disrupting Cryptocurrencies 2: Lessons From the Poly 'Hack'", Law Fare Blog, Aug 25, 2021, https://www.lawfareblog.com/disrupting-cryptocurrencies-2-lessons-poly-hack.
[52] Rahul N., "Messari: DeFi Exploits Total $284 Million Since 2019", Yahoo, Apr 29, 2021, https://finance.yahoo.com/news/messari-defi-exploits-total-284-091600754.html. ("over $284 million has been lost to hackers from decentralized finance (DeFi) hacks and exploits since 2019.")
[53] The actual conditions (available on the website) of even accessing this $25 in CRO coin are that the user must either stake $400 in CRO, or sign up for the Crypto.com credit card. The only way to turn this into $25 USD would be to meet the conditions, trade it for USD (ostensibly after paying a fee), and only if the price of CRO hasn't depreciated from the $25 USD level after meeting the conditions. See: https://help.crypto.com/en/articles/3124990-bg25-referral-program.



Crypto.com app, accessed November 15, 2021

Concentration and Centralization Concerns

Is Decentralized Finance Truly Decentralized?

Some DeFi proponents claim that their systems are purely peer-to-peer and operate without intermediaries.[54] However, market participants, including crypto metrics providers, have raised questions as to whether or not DeFi is truly decentralized given factors such as protocol fees, governance token control, and platform treasuries.[55]

Most tellingly, while marketing oneself as "decentralized" may be opportune from regulatory, legal and marketing standpoints, when crises happen that warrant quick action many DeFi platforms take actions with many indicia of centralized control.

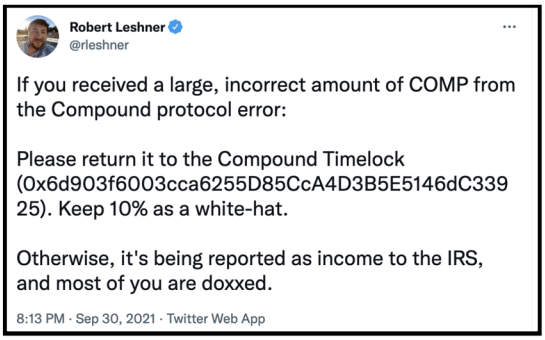
Compound threatening to report user's income to the IRS following a bug

A bug in the crypto borrowing and lending DeFi platform **Compound** led to erroneously large rewards of their crypto token COMP being distributed to certain users.[56] (One user allegedly was able to claim some $28 million worth of COMP tokens[57]).

---

[54] "DeFi vs. Traditional Finance", Ethereum Foundation, https://ethereum.org/en/defi/. (See: "One of the best ways to see the potential of DeFi is to understand the problems that exist today...There's a premium to financial services because intermediary institutions need their cut.")
[55] Liesl Eichholz, "The UNI Token: Is Uniswap Really Decentralized?", Glassnode Insights, Sep 24, 2020 , https://insights.glassnode.com/uni-token-is-uniswap-really-decentralized/.
[56] Andrew Ross Sorkin, Jason Karaian, Sarah Kessler, Stephen Gandel, Michael J. de la Merced, Lauren Hirsch and Ephrat Livni, "The limits of decentralization", NYTimes Dealbook, Oct. 26, 2021, https://www.nytimes.com/2021/10/04/business/dealbook/facebook-whistleblower-frances-haugen.html#link-1567b404.
[57] https://etherscan.io/tx/0xf4bfef1655f2092cf062c008153a5be66069b2b1fedcacbf4037c1f3cc8a9f45

During the infrastructure bill negotiation, the crypto industry was adamant that they didn't possess the technological capability to ensure tax reporting among its users. However, in response to this bug in their protocol's code, the CEO of Compound Robert Leshner demanded that users who received large sums of COMP tokens return them. He said they could keep 10% should they return them -- but if they didn't return the rest, he threatened that they would be reported to the IRS:



This stands in stark contrast to claims that tax reporting in DeFi wasn't possible. Indeed, it is clearly viewed as possible when such tax reporting can be viewed as a coercive attempt to have users self-correct bugs in Compound's code. This makes it clear that the lack of tax reporting is a design decision, not a technical limitation.[58]

Curve Finance Shutting Down a Competitors' Presence on their System via an "Emergency DAO"

Curve Finance is a major crypto borrowing and lending platform. Like many DeFi protocols, Curve uses a decentralized autonomous organization (DAO), to govern the project and allow users to vote on its future. Part of the motivation of creating DAOs is to argue that decision-making is not controlled by a single institution.[59] But recent events have called into question just how "decentralized" Curve truly is.

Curve allows external projects to add their own liquidity pools, and attempt to lure in more users to the liquidity pool by offering better rewards than competitors. Recently, a new project called Mochi Finance created a new liquidity pool on Curve, and through exploiting a series of loopholes, was able to amass a huge amount of voting power in Curve's governance system.

[58] Alexis Goldstein, "Crypto Doesn't Have to Enable Tax Cheats", Boomberg, Aug 26, 2021, https://www.bloomberg.com/opinion/articles/2021-08-26/crypto-doesn-t-have-to-enable-tax-cheats.
[59] Nathan Reiff, " Decentralized Autonomous Organization (DAO)", Investopedia, Sep 24, 2021, https://www.investopedia.com/tech/what-dao/.

Curve accused them of taking advantage of their governance system,[60] called the incentives that Mochi offered "bribes", and raised "serious security and decentralization" concerns.[61] As a result, Curve called a meeting of what they called its "Emergency DAO" and shut down Mochi's liquidity pool entirely.[62] The move received criticism[63] for being against the ethos of decentralization.[64]

Major Cryptomarket Players control key Sushi Swap Wallet

Certain platforms have "Development Funds" that are meant to further the growth of the platform's ecosystem; typically, users who hold governance tokens in the platforms can vote on how to spend these funds. However, some of these Development Funds are controlled by a core group of people, via multi-signatures ("multi-sig") wallets—cryptocurrency wallets that require two or more people to digitally "sign" and execute a particular transaction. SushiSwap is a DeFi platform whose Development Fund is controlled by a multi-sig wallet, which includes some very prominent crypto market actors as signers, including[65]:

- Sam Bankman-Fried: CEO of FTX and co-founder of Alameda Research, a crypto proprietary trading fund;
- Robert Leshner: The CEO of the crypto lending and borrowing DeFi firm, Compound Labs;
- CMS Holdings: a proprietary cryptocurrency investment firm co-founded by former executives from Circle and crypto trading firm DRW/Cumberland (Daniel Matuszewski, Julien Collard-Seguin, and Bobby Cho); and
- Matthew Graham (Sino Global Capital).

Concentration

While cryptocurrency industry insiders promote the "democratized" benefits of digital assets, in truth, crypto concentrations of money and power match or surpass those in traditional financial markets.

---

[60] Brooks Butler and Mike Dalton, "Curve Blocks Mochi After Alleged Attempted Governance Attack", Crypto Briefing, Nov 12, 2021, https://cryptobriefing.com/curve-blocks-mochi-after-alleged-attempted-governance-attack/.
[61] "The Curve Emergency DAO has killed the USDM gauge", Curve, Nov 11, 2021, https://gov.curve.fi/t/the-curve-emergency-dao-has-killed-the-usdm-gauge/2307.
[62] Andrew Thurman, "'Curve Wars' Heat Up: Emergency DAO Invoked After 'Clear Governance", Attack'", Nov 11, 2021, https://www.coindesk.com/business/2021/11/11/curve-wars-heat-up-emergency-dao-invoked-after-clear-governance-attack/.
[63] https://twitter.com/mewn21/status/1458771401381486600 ("im saying its a bad precedent to discriminate against a user, any user, who accrued voting rights over your protocol without exploiting or breaking a mechanism. either ur mechanism is broken or its not defi")
[64] Andrew Thurman, *supra* note 62. ("the decision from the decentralized autonomous organization, or DAO, has prompted much community debate, as some have argued that the protocol should not single out any one user and that blacklisting another protocol runs against DeFi's open, permissionless ethos.")
[65] https://docs.sushi.com/governance/current-governance-model

The concentration of particular cryptocurrency assets into a small handful of addresses raise concerns about power concentrations. A paper by Igor Makarov and Antoinette Schoar found that, in the last five years, the top 10% of Bitcoin miners controlled 90% of all mining capacity, while 0.1% of miners (about 50 of them) controlled close to 50% of mining capacity.[66] In addition, many of the so-called "governance tokens", which provide holders the ability to vote on proposals affecting the future of certain cryptocurrency projects, are owned by a very small portion of token holders. According to the crypto metrics provider Glassnode, as of November 15, 2021:

- Over 98% of the governance tokens (COMP) for the crypto lending and borrowing platform Compound are on by the top 1% of token holders[67] — Glassnode specifies that "Exchange addresses, smart contract addresses, and other special asset-specific addresses (e.g. team fund addresses) are excluded".[68]
- Over 96% of the governance tokens (UNI) for the exchange Uniswap are held by the top 1% of token holders.[69]

Venture Capitalists and other private investors are a significant presence in cryptocurrency markets, and appear to hold considerable market power—and their investment in the space is growing fast. Venture Capital firms invested $17 billion in digital asset firms in the first six months of 2021, more than three times what they invested in all of 2020.[70]

---

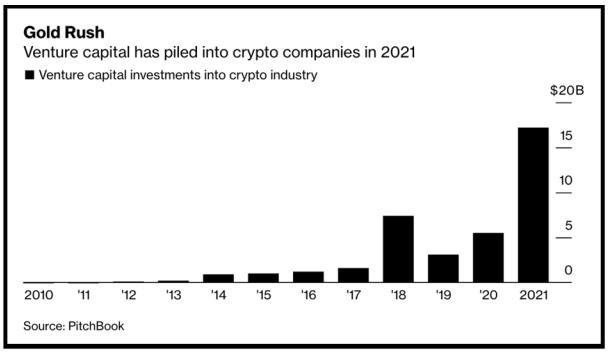
[66] Igor Makarov and Antoinette Schoar, "BLOCKCHAIN ANALYSIS OF THE BITCOIN MARKET", NATIONAL BUREAU OF ECONOMIC RESEARCH, October 2021, https://www.nber.org/system/files/working_papers/w29396/w29396.pdf.

[67] Glassnode, metrics for Compound's COMP token: Percent of Supply Held by Top 1% Addresses, https://studio.glassnode.com/metrics?a=COMP&category=&m=distribution.Balance1PctHolders&modal=loginForm

[68] https://docs.glassnode.com/api/distribution#supply-of-top-1-addresses

[69] Glassnode, metrics for Uniswap's UNI token: Percent of Supply Held by Top 1% Addresses, https://studio.glassnode.com/metrics?a=UNI&category=&m=distribution.Balance1PctHolders&modal=loginForm

[70] Brandon Kochkodin, "Venture Capital Makes a Record $17 Billion Bet on Crypto World", Bloomberg, Jun 18, 2021, https://www.bloomberg.com/news/articles/2021-06-18/venture-capital-makes-a-record-17-billion-bet-on-crypto-world.



This summer, PayPal co-founder and billionaire venture capitalist Peter Thiel, along with Galaxy Digital CEO Mike Novogratz, and billionaire hedge fund manager Alan Howard led a $10 billion investment in a new crypto exchange called "Bullish" that will utilize the EOS blockchain.[71]

Some venture capital firms may be using retail investors as "exit liquidity" — investors to sell their tokens to once they're ready to exit. The *NYTimes* reported on one such potential offloading by insiders onto retail in a report about the collapse of the Internet Computer (ICP) token. According to the *NYTimes*, a number of wallet addresses presumed to be insiders "deposited 10 million ICP tokens worth more than $2 billion to exchanges after the initial coin offering, giving the impression they were transferred for trading, not safeguarding. These transfers coincided with significant drops in the price of ICP, the report said. Small investors, left out of the process, were stuck."[72] Among Internet Computers' large investors were the venture capital firm Andreessen Horowitz (a16z).

Many industry participants are deliberately aiming for monopoly-levels of power and concentration. Barry Silbert, the head of the digital assets conglomerate Digital Currency Group (which boasts dozens and dozens of crypto portfolio companies) told the *Wall Street Journal* that "the model I use as an inspiration is Standard Oil."[73] This is a particularly troubling comment, as Standard Oil was an archetype monopoly that routinely exploited anemic legal restrictions, flagrantly engaged in law breaking activities, and implemented destructive and unfair market practices such as mergers, predatory pricing, and other coercive tactics to fortify its market dominance.[74] Stephen Stonberg, the COO of crypto exchange Bittrex, told the

[71] "Thiel-backed Block.one injects billions into cryptocurrency exchange", Bloomberg, May 12, 2021, https://www.pionline.com/markets/thiel-backed-blockone-injects-billions-cryptocurrency-exchange.
[72] Ephrat Livni and Andrew Ross Sorkin, "The Dramatic Crash of a Buzzy Cryptocurrency Raises Eyebrows", NYTimes, Jun 28, 2021, https://www.nytimes.com/2021/06/28/business/dealbook/icp-cryptocurrency-crash.html.
[73] Paul Vigna, "Digital Currency Group Wants to Be Crypto's Standard Oil", Wall Street Journal, Nov 1, 2021, https://www.wsj.com/articles/digital-currency-group-wants-to-be-cryptos-standard-oil-11635764400.
[74] Naomi R. Lamoreaux, "The Problem of Bigness: From Standard Oil to Google," https://www.aeaweb.org/articles?id=10.1257/jep.33.3.94.

podcast BlockCrunch, "when I first saw crypto, I thought, this is gonna be like hedge funds were in the 1980s, you're going to be able to charge whatever fees you want." Stonberg went on to describe that "there's always this period of lots of companies and then consolidation. And that's like the internet in the 90s, and now you have three companies that control the whole world."[75]

Outsized Impact of Very Wealthy Crypto Users

Digital asset markets appear particularly susceptible to very large users moving their funds in and out of various projects. To take one example, prior to October, the DeFi borrowing and lending platform Aave was consistently ranked first in terms of "total value locked" – the amount of crypto assets reportedly locked into the platform.

But on October 29, 2021, a single user withdrew $4.2 billion in crypto assets from Aave, causing lending and borrowing interest rates to spike, and their total crypto locked to plummet ~18% in a matter of hours. Aave fell from being ranked first in TVL to third. The event raised questions about whether other platforms are similarly dependent on very wealthy users, and what sorts of volatility may follow should those users decide to remove their crypto assets.

National Security Concerns

National security concerns arise when considering any transfer of money - including within the banking system. Cryptocurrency, however, raises unique concerns given the lack of illicit financing controls on many platforms, the borderless nature of transactions and the dispositional fondness for anonymity among crypto users and firms.

Ransomware attacks are increasing in number, and cryptocurrency assets are often used to layer and obscure ransomware payments. An October 2021 FinCEN report found that cryptocurrency exchanges with lax Know Your Customer/Anti-Money Laundering ("KYC/AML") compliance are the preferred cash-out points for ransomware payments.[76] Case in point, a recent Department of Justice arrest of two foreign nationals over ransomware attacks[77] included a warrant posted showing that up to $13 million was held by one of the foreign nationals at the cryptocurrency exchange FTX.[78]

---

[75] The Amazon Moment for Crypto Exchanges - Stephen Stonberg, Bittrex Global, Ep. 126, https://podcasts.apple.com/us/podcast/amazon-moment-for-crypto-exchanges-stephen-stonberg/id1350649166?i=1000504410789

[76] "FinCEN Issues Report on Ransomware Trends in Bank Secrecy Act Data", FinCEN, Oct 15, 2021, https://www.fincen.gov/news/news-releases/fincen-issues-report-ransomware-trends-bank-secrecy-act-data.

[77] "Ukrainian Arrested and Charged with Ransomware Attack on Kaseya", Department of Justice, Nov 8, 2021, https://www.justice.gov/opa/pr/ukrainian-arrested-and-charged-ransomware-attack-kaseya.

[78] "Warrant to Sieze Property Subject to Forfeiture", https://www.justice.gov/opa/press-release/file/1447131/download.

The October FinCEN report also found that "Ransomware-related payments are being converted to other types of [cryptocurrency] through decentralized exchanges or other DeFi applications."[79]

One crypto mining pool, Marathon Digital Holdings, attempted to introduce a "sanctions-compliant" mining pool. However, many in the crypto community complained, and Marathon reversed course.[80] Marathon CEO Fred Thiel told *The Block* "you have groups in the bitcoin community who are all about maximum decentralization. They are against the whole concept of doing anything that has to do with financial regulatory compliance or government regulation."[81]

In October, the Treasury Department's Office of Foreign Assets Control (OFAC) clarified this October that miners (and all other actors in the digital asset markets) are expected to comply with OFAC's new guidance on sanctions compliance.[82] In the guidance, they wrote that "All companies in the virtual currency industry, including technology companies, exchangers, administrators, miners, and wallet providers, as well as more traditional financial institutions that may have exposure to virtual currencies" should consider incorporating the controls outlined in OFAC's guidance into their sanctions compliance programs.[83]

Cities that have been considering adopting city-specific crypto tokens, in partnership with the CityCoins project[84] which is built on the Stacks platform, should pay particular attention to the national security concerns of doing so. While it's unclear if the Stacks project's definition of "mining"[85] bears any meaningful resemblance to what is currently considered crypto mining, the publicly-available details of the project[86] nevertheless raise particular national security questions, including how CityCoins plan to adhere to the new OFAC guidance, and ensure that

---

[79] "FinCEN Issues Report on Ransomware Trends in Bank Secrecy Act Data", FinCEN, Nov 15, 2021, https://www.fincen.gov/news/news-releases/fincen-issues-report-ransomware-trends-bank-secrecy-act-data. ("Ransomware-related payments are being converted to other types of [Convertible Virtual Currencies] through decentralized exchanges or other DeFi applications. Some DeFi applications allow for automated peer-to-peer transactions without the need for an account or custodial relationship. FinCEN analysis of transactions on the BTC blockchain identified ransomware-related funds sent indirectly to addresses associated with open protocols for use on DeFi applications.")

[80] Kollen Post, "FinCEN Issues Report on Ransomware Trends in Bank Secrecy Act Data", The Block, Jun 2, 2021, https://www.theblockcrypto.com/linked/106865/marathon-ofac-bitcoin-mining-pool-taproot.

[81] *Id.*

[82] "Publication of Sanctions Compliance Guidance for the Virtual Currency Industry and Updated Frequently Asked Questions", Treasury Department, Oct 15, 2021, https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20211015.

[83] "Sanctions Compliance Guidance for the Virtual Currency Industry (Brochure)", Office of Foreign Assets Control, Oct 2021, https://home.treasury.gov/system/files/126/virtual_currency_guidance_brochure.pdf.

[84] "CityCoins FAQ:, https://www.citycoins.co/citycoins-faq.

[85] https://github.com/citycoins/citycoin/blob/main/citycoin-prd.md#mining. ("The act of mining a CityCoin is defined by someone sending Stacks tokens (STX) to the smart contract created for the city, using the following criteria.")

[86] https://github.com/citycoins/citycoin/blob/main/citycoin-prd.md#trading-and-open-markets. ("CityCoins is an open source project and any CityCoin can be listed and available for trading on centralized and decentralized exchanges at any time after mining has begun.")

they aren't allowing crypto addresses on OFAC's Specially Designated Nationals and Blocked Persons List to participate in the project.

Climate and Supply Chain Concerns

The two largest cryptocurrencies, Bitcoin and Ether, currently use a "Proof of Work" consensus mechanism to validate transactions. Proof of Work crypto mining creates a number of extensive climate harms, which include annual energy consumption akin to that of entire nations[87], 30,700 tons of electronic waste annually, higher electricity bills for residents of states with crypto mining[88], and quality of life issues.[89] Over 70 climate, economic, racial justice, business and local organizations recently wrote to Congress, asking them to mitigate the considerable contribution portions of the cryptocurrency markets are making to climate change.[90]

In addition, Proof of Work cryptocurrency mining has been exacerbating the shortages of semiconductors.[91] Senators Maggie Hassan and Joni Ernst recently introduced a bill calling on the Treasury Department to compile a report on how cryptocurrency mining operations are impacting semiconductor supply chains.

Systemic risk concerns

Systemic risk arises when the scope, size, scale or interconnectedness of certain activities can metastasize and spread contagion to other market participants or the broader financial system. Certain indicia of potential systemic risk - including leverage, opacity in market data, and poorly understood interlinkages between market participants - is currently present in digital asset markets.

Leverage

While US-based exchanges have reduced the amount of leverage available to smaller investors as of this summer, DeFi platforms offer many ways for users to lever up:

---

[87] Cristina Criddle, "Bitcoin consumes 'more electricity than Argentina'", BBC, Feb 10, 2021, https://www.bbc.com/news/technology-56012952.
[88] Laura Counts, "Power-hungry cryptominers push up electricity costs for locals", BerkeleyHaas, Aug 3, 2021, https://newsroom.haas.berkeley.edu/research/power-hungry-cryptominers-push-up-electricity-costs-for-locals/.
[89] Jeff Keeling, "Bitcoin mine spokesman says dealing with noise issue 'our number one priority'", WJHL, Jul 16, 2021, https://www.wjhl.com/news/local/noisy-bitcoin-mines-neighbors-hope-monday-meeting-yields-answers-from-power-provider/.
[90] " Large Coalition of Public Interest and Environmental Groups Come Together to Urge Leaders to Address Climate Damages of Crypto", Open Markets Institute, Oct 7, 2021, https://www.openmarketsinstitute.org/publications/large-coalition-of-public-interest-and-environmental-groups-come-together-to-urge-leaders-to-address-climate-damages-of-crypto.
[91] "Crypto-miners are probably to blame for the graphics-chip shortage", The Economist, Jun 19, 2021, https://www.economist.com/graphic-detail/2021/06/19/crypto-miners-are-probably-to-blame-for-the-graphics-chip-shortage.

Flash Loans

Flash loans are unsecured loans where capital is borrowed and repaid in a single transaction, through the use of smart contracts. As the crypto platform Monolith describes it, flash loans allow users to "potentially borrow huge sums of money at a marginal cost."[92] They are offered by the Aave platform, and there is no upper limit to the size of the flash loan one can obtain[93]: the largest flash loan processed to date was about $200 million. Flash loans are typically used to try and take advantage of arbitrage opportunities such as discrepancies between the price of a given cryptocurrency on different exchanges.[94] However, these loans have also been increasingly used to exploit vulnerable DeFi protocols, and steal millions of dollars. As of June 2021, Aave had issued almost $4 billion in flash loans. Flash loans that result in a profit are typically charged a mere 0.09% fee.[95]

Leveraged Borrowing

Many DeFi platforms allow customers to use their crypto assets as collateral against loans denominated in other crypto assets. One example is Teddy Cash, a platform on the Avalanche blockchain, which allows users to pledge their AVAX tokens -- the native token of the Avalanche blockchain -- as collateral. Teddy Cash alleges to lend users the TSD stablecoin "interest free" (the TSD stablecoin is supposedly pegged to the U.S. dollar). In their FAQ, Teddy Cash explains how to user their website to lever up eleven times:

> "Borrowers speculating on future AVAX price increases can use the protocol to leverage their AVAX positions up to 11 times, increasing their exposure to price changes. This is possible because TSD can be borrowed against AVAX, sold on the open market to purchase more AVAX — rinse and repeat.*
>
> *Note: This is not a recommendation for how to use Teddy Cash. Leverage can be risky and should be used only by those with experience."[96]

---

[92] Monolith, "Understanding DeFi: flash loans explained", Medium.com, Jan 10, 2021, https://medium.com/monolith/understanding-defi-flash-loans-explained-1a5928a4a612.
[93] *Id.* ("Unlike a regular loan, though, there's no limit to the amount the user can borrow, and it can be taken out instantly, as long as it's paid back in the same transaction — at a flash speed. This is made possible by smart contracts. They're programmed to ensure that the loan is returned, otherwise the transaction gets blocked. The revolutionary part is how quickly it all happens, and the borrower only needs to shell out for a transaction fee to pay for the whole process.")
[94] Alyssa Hertig, "What is a Flash Loan?", Coin Desk, Feb 17, 2021, https://www.coindesk.com/learn/2021/02/17/what-is-a-flash-loan/.
[95] Adriana Hamacher, "What Are Flash Loans? The DeFi Lending Phenomenon Explained", Decrypt, Jun 28, 2021, https://decrypt.co/resources/what-are-flash-loans-the-defi-lending-phenomenon-explained.
[96] Teddy Cash, FAQ: Borrowing, https://docs.teddy.cash/borrowing.

Certain borrowing platforms, such as Aave, also fail to disclose the full terms of the loan at the time the loan is taken out. Aave's website displays an interest rate the borrower will be charged (measured in a variable APY), and notes that there is a "health ratio" — a level if collateralization that must be maintained to avoid liquidation. But it is only in Aave's FAQ, but at the point of the loan, are the terms of liquidation fully disclosed — including the fact that there is a variable fee (in the ~10% range) charged upon liquidation. This raises loan disclosure concerns—they may be deceiving users about the true cost of the loan by under disclosing all the fees. The FTC, for example, has taken the position that hidden disclosures are like no disclosures at all.[97]

Opacity

As noted by Professor Sarah Hammer of the Wharton School, there is "no official U.S. public data source for cryptocurrency prices, market size, or volatility. This lack of data is a significant problem."[98] This leaves regulators, lawmakers, and the public alike dependent on the self-reported data from the industry, which may be subject to double-counting, as some users are moving cryptoassets from one blockchain to another via "bridges", or lending their crypto assets to others. Currently, there is no centralized data repository, reporting nomenclature or regulatory oversight into crypto metrics. This lack of data makes it difficult for users to evaluate whether to participate on a trading platform and for regulators, researchers and the public to understand wider crypto risks. Indeed, one key lesson from the 2008 financial crisis was that poor data and oversight of market participants' positions in credit default swap markets led to the mispricing of risk and a poor understanding of counterparty exposures or risks to the broader market.

Interconnections: Family Offices, Hedge Funds, and Large Banks

While crypto proponents claim that the digital asset market is a refuge from the practices of traditional financial markets, the Too Big To Fail banks are a growing presence in the crypto currency market. Goldman Sachs plans to open a cryptocurrency trading desk,[99] BNY Mellon allows its clients to hold Bitcoin as of February[100], Wells Fargo will offer professionally managed

---

[97] "LendingClub Agrees to Pay $18 Million to Settle FTC Charges", Federal Trade Commission, Jul 14, 2021, https://www.ftc.gov/news-events/press-releases/2021/07/lendingclub-agrees-pay-18-million-settle-ftc-charges.

[98] Written Testimony of Sarah Hammer, Managing Director of the Stevens Center for Innovation in Finance at the Wharton School, U.S. House Financial Services Committee, Oversight and Investigations Subcommittee, Jun 30, 2021, https://financialservices.house.gov/uploadedfiles/hhrg-117-ba09-wstate-hammers-20210630.pdf.

[99] Hugh Son and Natasha Turak, "Goldman Sachs internal memo unveils new cryptocurrency trading team", CNBC, May 7, 2021, https://www.cnbc.com/2021/05/07/goldman-sachs-unveils-new-cryptocurrency-trading-team-in-employee-memo.html.

[100] Thomas Franck, "BNY Mellon to offer bitcoin services, a validation of crypto from a key bank in the financial system", CBNC, Feb 11, 2021, https://www.cnbc.com/2021/02/11/bny-mellon-to-offer-bitcoin-services-a-validation-of-crypto-from-a-key-bank-in-the-financial-system.html.

cryptocurrency funds for qualified investors.[101] Morgan Stanley's Europe Opportunity Fund reported owning 28,298 shares of the Grayscale Bitcoin Trust,[102] according to a June 28 filing.[103] As digital assets continue to migrate into the banking perimeter, it would greatly exacerbate any future crises in digital asset markets, and could metastasize to the full economy.

Cryptocurrency exchanges and DeFi platforms alike are also trying to attract institutional business. The London-based Aave, which offers lending and borrowing of cryptocurrency,[104] is creating a private pool to allow large institutions to try out their platform.[105] Signs indicate the presence of hedge funds in cryptocurrency is growing. An Intervest survey of hedge funds managing an average of 7.2 billion showed that North American funds expect to have a 10.6% average exposure to cryptocurrency by 2026.[106] If, as the survey suggests, the majority of hedge funds with billions in assets under management hold ten percent or more of their positions in cryptocurrency, downturns in cryptocurrency markets may have spillover effects to the rest of the economy: should these hedge funds also be prime brokering with large banks, sharp swings in the volatile cryptocurrency markets could lead to forced liquidations of other assets at these private funds.

Conclusion

Congress should continue to examine if there are regulatory gaps that require new legislation to ensure consumer and investor protection in the cryptocurrency space. Congress should as ensure there are mechanisms for the regulators to have a complete picture of systemic risk in the space. Regulators should continue to monitor digital asset markets and ensure compliance with existing regulations.

---

[101] "Wells Fargo: US bank set to offer crypto fund to rich clients", BBC, May 19, 2021, https://www.bbc.com/news/business-57147386.
[102] Robert Stevens and Tim Copeland, "GBTC: Everything You Need To Know About The Grayscale Bitcoin Trust", Decrypt, Apr 9, 2021, https://decrypt.co/resources/gbtc-everything-you-need-to-know-about-the-grayscale-bitcoin-trust.
[103] Sam Bourgi, " Morgan Stanley equity fund owns 28.2K shares of Grayscale Bitcoin Trust, per SEC", Coin Telegraph, Jun 28, 2021, https://cointelegraph.com/news/morgan-stanley-equity-fund-owns-28-2k-shares-of-grayscale-bitcoin-trust-per-sec.
[104] "What is Aave? (AAVE)", Kraken, https://www.kraken.com/en-us/learn/what-is-aave-lend; and "FAQ: Introduction to Aave", Aave, https://docs.aave.com/faq/.
[105] Chris Williams, "Aave Has a Private Pool for Institutions Testing DeFi", Crypto Briefing, May 12, 2021, https://cryptobriefing.com/aave-has-private-pool-institutions-testing-defi/.
[106] Laurence Fletcher, "Hedge funds expect to hold 7% of assets in crypto within five years", FT, Jun 15, 2021, https://www.ft.com/content/4f8044bf-8f0f-46b4-9fb7-6d0eba723017.

DEMYSTIFING CRYPTO: DIGITAL ASSETS AND THE ROLE OF GOVERNMENT

Joint Economic Committee
November 17, 2021

Testimony of Timothy Massad[1]

Chair Beyer, Ranking Member Lee, and members of the committee, thank you for inviting me to testify at this hearing on "Demystifying Crypto: Digital Assets and the Role of Government." It is an honor to be here.

This hearing is a very helpful step toward developing appropriate policies that can encourage innovation, but also protect against excessive risks, with respect to digital assets. I also want to thank Chair Beyer for introducing a thoughtful legislative proposal in this regard.

I would like to begin by making eight brief points, and then elaborate on a few of them.

Executive Summary

First, there is no question that digital asset innovation is incredibly important and beneficial overall. But there should also be no question that the time to strengthen and clarify regulation of digital asset markets is long overdue. If done responsibly, it will support, not suppress, innovation.

Second, stablecoins are one of the most urgent challenges. If properly regulated, they might help modernize payments, but today they pose significant risks and they have grown rapidly, as described in the report just released by the President's Working Group on Financial Markets (PWG). I support its findings, but while it calls on Congress to adopt legislation that limits stablecoin issuers to insured depository institutions, I would prefer a more tailored regulatory approach. I think this can be a better way to address risk and foster competition and innovation, as I describe below.

Third, I agree with the PWG report on the need to regulate stablecoin arrangements generally, not just the issuer, and the report's focus on DeFi or decentralized finance. Once issued, stablecoins trade on decentralized blockchains pursuant to smart contracts, as well as on centralized exchanges. This means there is no single authority responsible for overall operation of a stablecoin. We need to regulate these stablecoin arrangements and other actors as well. As a general matter, while decentralization can be a good thing, calling something DeFi should not make it a regulatory-free zone. The point is not to regulate the technology, but to have appropriate standards for financial market activities conducted on such platforms.

Fourth, Bitcoin is neither a widely accepted means of payment or a stable store of value today; it is a highly volatile, speculative investment. It might be tempting to just say caveat emptor,

let the buyer beware. But the continued growth of a largely unregulated crypto market poses risks to society—including risks of illicit activity, tax evasion, ransomware and potential harm to broader financial markets.

We do not have sufficient information or transparency about this market. Neither the SEC nor the CFTC has authority today to regulate the cash market for digital assets that are not considered securities. That is where most trading activity occurs today.[2] We should expand that authority and increase the resources of both agencies to exercise their responsibilities. We should also consider the best way to make sure our regulatory policies are adequately informed by technological expertise, so that we balance innovation with protecting the public interest.

Fifth, in regulating crypto generally, we must balance reasonable expectations of privacy in transactions with the government's legitimate interests, such as preventing illicit activity and tax evasion. FinCEN has done a great job but this continues to be a challenge.

Sixth, the evolution of digital assets has made it clear that we need to modernize our payments system. It is relatively slow and expensive. A central bank digital currency is one way of doing so, but there may be other ways. My concern is we are not moving fast enough to develop and implement the best strategy, for reasons I will discuss.

Seventh, CBDCs, stablecoins and digital assets generally are often cited as a means to achieve greater financial inclusion. We should consider their potential for doing so, but we should also act to improve access to financial services now through other means. The need is too great and should not be deferred.

Finally, the challenge we face today is not unusual, because the financial sector constantly innovates and our regulatory system has to catch up. The early days of subprime mortgages improved access to the American dream of homeownership for many Americans; but it later gave rise to destructive products. The swaps industry created a lot of beneficial hedging, but the industry resisted regulation and eventually generated excessive risks that substantially intensified the 2008 financial crisis. It was only after that we took action.

The U.S. should exercise leadership globally. The path to regulating the swaps industry started with core principles that the G-20 leaders endorsed, which each country then implemented. The same approach could be taken here. A national strategy to modernize our payments system will also be critical for continued U.S. leadership in the global economy.

I elaborate below on a few of these points.

Innovation and Regulation

First, the innovation launched by bitcoin has been dramatic. It has shown the need to modernize our payments system, and led to stablecoins and central bank digital currencies,

which could be tools for that modernization. Blockchain, distributed ledger technology and smart contracts are all dynamic innovations whose potential value goes well beyond payment mechanisms. Our economy generally is becoming more and more digital. But innovation should not cause us to refrain from creating sensible regulation. Digital asset markets today pose significant risks to investors and society at large due to a regulatory framework that is inadequate and sometimes confusing. This includes risks of investor fraud, malfeasance and illicit behavior, tax evasion and potentially broader risk to financial markets. The time to strengthen regulation is long overdue.

The U.S. financial markets have been the envy of the world for decades in part because we have created sensible regulatory policies within which a strong private sector could operate and innovation could take place. We need the same here – policies that provide clarity, and permit and encourage our dynamic private sector to continue to innovate, while at the same time ensuring transparency and integrity in markets, prohibition of illicit activity, financial stability and investor and consumer protection.

Digital assets used for financial activities do not fit neatly into our existing financial regulatory scheme. Trying to regulate digital assets solely under existing laws is a bit like trying to force a round peg through a square hole. But the principles behind the laws that govern other financial instruments and markets – transparency, integrity and fairness in trading, adequate disclosure and reporting, and prevention of fraud and illicit activity – are still applicable.

Developing appropriate standards requires careful thought and ingenuity. It needs to be thoroughly informed by technological expertise, not just by debates about policy principles. While we may need legislation in some areas as noted below, Congress may also want to direct an executive branch entity to focus on these issues. The Financial Stability Oversight Council could also create a standing committee, coordinate the work of different regulators and make appropriate recommendations to Congress. I would also note that the legislation introduced by you, Mr. Chairman, calls for a number of useful studies in this regard.

Stablecoins

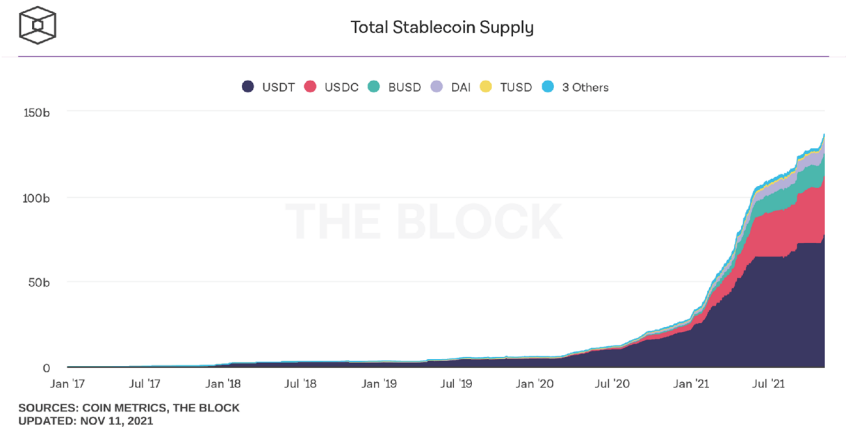
Stablecoins present one of the most promising opportunities as well as most urgent challenges in the digital assets world. I will discuss why they have grown dramatically, the risks and opportunities they pose, and what we should do to regulate them.

Stablecoins are digital tokens whose value is pegged to the dollar (or another currency or asset). Today, they serve to grease the wheels of the crypto industry, enabling investors to easily transfer value between different crypto exchanges and cryptocurrencies without converting back and forth into dollars or another fiat currency. This is particularly useful because of arbitrage opportunities that exist between the many crypto exchanges and platforms, given the absence of any routing system or combined centralized order book. It is also useful given the many cryptocurrencies that exist and the high degree of volatility.

Settlement of stablecoins is instant, consistent with how cryptocurrencies trade. This avoids the delays of traditional means of payment.

In addition, some investors may be using stablecoins to evade taxes, avoid legal or regulatory constraints on trading crypto, or engage in illicit activity. The fact that many banks, for regulatory or other reasons, may be reluctant to fund customers trading crypto may have also contributed to the popularity of stablecoins.

These attributes, coupled with the explosive growth of the crypto market, explain why the market capitalization of stablecoins has increased from $20 billion twelve months ago to over $130 billion today, as shown by the chart below.



The following chart lists the largest stablecoins by market capitalization:

Ranking	Coin	Market Cap
1	Tether (USDT)	$72.68B
2	USD Coin (USDC)	$34.43B
3	Binance USD (BUSD)	$13.55B
4	DAI	$6.48B
5	Terra USD (UST)	$4.02B
6	TrueUSD (TUSD)	$1.20B
7	Pax Dollar (USDP)	$949.37M
8	FRAX	$899.93M
9	Liquidity USD (LUSD)	$720.17M
10	Neutrino USD (USDN)	$567.46M

Source: coincodex.com, Stablecoins by Market Cap and Volume, as of 11/12/2021

The volume of trading of stablecoins is also quite large. The trading volume of Tether, the largest stablecoin by market cap, is roughly twice that of bitcoin. The velocity of dollar stablecoins—the number of times one unit changes hands over a given time period—was said to average over 100 times a year. By comparison, the velocity of the dollar (M2) is in the low single digits according to a Federal Reserve report.

Although their use is largely confined to the crypto industry today, stablecoins have the potential for broader applicability. That is because they are a means for faster payments. The recent report of the President's Working Group on Financial Markets recognized this in saying that stablecoins, if properly regulated, "could support faster, more efficient, and more inclusive payments options."

The risks and opportunities related to broader use of stablecoins were first widely raised by Meta's (Facebook Inc.'s) proposal for Libra in June of 2019. It wanted to create a "simple global currency" or stablecoin that would be pegged to a basket of fiat currencies. The proposal met harsh reaction. It has since been revised to be a series of stablecoins, each pegged by a single fiat currency (and renamed as Diem), but it is not yet operational because regulators have not approved it. (I discuss the Libra proposal in detail, and related issues of mobile payments, CBDCs and financial inclusion, here.)

The PWG report is a clear and comprehensive summary of the risks of stablecoins. (I have also written about these risks, here and here.) I agree with the report's call for standards to guard against stablecoin runs, to minimize payment system risk, to prevent use of stablecoins for illicit activity, and to address concerns about systemic risk. I believe bringing this activity within the

general rubric of bank regulation makes sense. While money market mutual fund regulation is another approach, stablecoins are really payment instruments, not investments.[3]

I have two concerns with the report's primary recommendation, which is that we adopt legislation that would require a stablecoin issuer to be an insured depository institution, and be subject to existing supervisory standards. The first is the time it may take to enact legislation, and what happens in the meantime. I urge Congress to prioritize this issue. I also urge the FSOC to act in the meantime. The report notes its power to do so. It could commence a review to determine whether stablecoins are, or are likely to become, a systemically important payment activity. If it then reached such a conclusion, the Federal Reserve would have the responsibility for developing risk management standards. In addition, while individual agencies have certain powers with respect to stablecoins as well, the FSOC can help coordinate the exercise of such authorities so that we avoid conflicting actions.

My second concern pertains to the substance of the recommendation. I believe we should consider developing a more tailored model of regulation for stablecoin issuers, which would enable us to design standards that are more specific to the risks posed and which would also facilitate more competition in the payments industry.

We should require that stablecoins are at all times fully backed by cash that is deposited with a bank, or in a master account with the Federal Reserve. This will eliminate the risk that exists today where stablecoin reserves may be invested in other assets that could lose value, or be difficult to liquidate, or whose sudden liquidation might drive asset prices down. Such a requirement would effectively prohibit maturity transformation by stablecoin issuers—the practice of taking demand deposits, which are short-term liabilities, and using them to fund longer-term loans or investments. We could also restrict the activities of a stablecoin issuer so that it does not engage in many of the activities that a traditional IDI might engage in. We should require some capital, even if the tokens are fully backed by cash, because there can be operational or other losses. This approach could be implemented through novel or special purpose charters.

The PWG report refers to the possibility of "access to appropriate components of the federal safety net." While it is unclear whether or on what terms this might include deposit insurance, we should consider whether that is necessary if the tokens are fully reserved with cash, the entity's activity is sufficiently isolated and other safeguards are in place. Deposit insurance has been an important protection against bank runs, particularly given the inherent risks in maturity transformation-- or what former Bank of England Governor Mervyn King called the "alchemy" of banking. But if the stablecoin activity is effectively ringfenced and not combined with a variety of other bank activities, query whether deposit insurance is appropriate.

I am also concerned that the recommendation to limit stablecoin issuers to IDIs under present supervisory standards could result in limiting competition as a practical matter. It is likely to favor existing banks over new entrants because of the length of time it could take new entrants to get a charter and deposit insurance. It could also mean that the largest banks are favored

over all other banks because of capital advantages as well as technological advantages (they may be more able to create the platforms to issue and manage stablecoins, which settle instantly, as discussed below). The more tailored regulatory approach described above would allow new entrants, provided they can meet requirements of the type noted above, which would facilitate more competition in payments. (An existing bank holding company could still enter the stablecoin business by creating a ringfenced subsidiary that meets the requirements.)

Some may object to allowing special purpose payment entities to have master accounts at the Federal Reserve, particularly if they are not FDIC-insured and do not have the same business models as traditional banks. But in fact, the Fed has already granted master accounts to uninsured entities whose business models are very different from traditional banks. Two derivatives clearinghouses have master accounts with over $100 billion on deposit on a combined basis, which monies represent customer funds.[4] They are not regulated as banks nor insured by the FDIC. They are permitted to have master accounts because they were designated by the FSOC as systemically important financial market utilities under Article VIII of the Dodd Frank Wall Street Reform and Consumer Protection Act. They are subject to Federal Reserve oversight as a result of that designation.

The Federal Reserve has already commenced a review of access to Fed accounts; how we regulate stablecoins should inform, and be informed by, that review. The Fed could develop specific requirements for access to master accounts by stablecoin issuers beyond those standards noted earlier, to ensure that appropriate risk management standards with respect to liquidity, operations and technology are met. In this regard, we must keep in mind that stablecoins settle instantly. An issuer must be able to reconcile its books in real-time; end of day or twice a day reconciliation would not be sufficient, and actually could expose the payment system to greater risk. Many existing IDIs may not have the technological platforms necessary to enter the stablecoin business.

I am in agreement with the thrust of the PWG report with respect to other areas in which regulatory oversight is needed, such as consumer protection standards including standards on how a customer's data can be used, and the need to prevent illicit behavior and tax or regulatory evasion. I want to comment in particular on the issues posed by the broader arrangements involved with stablecoins and decentralized finance.

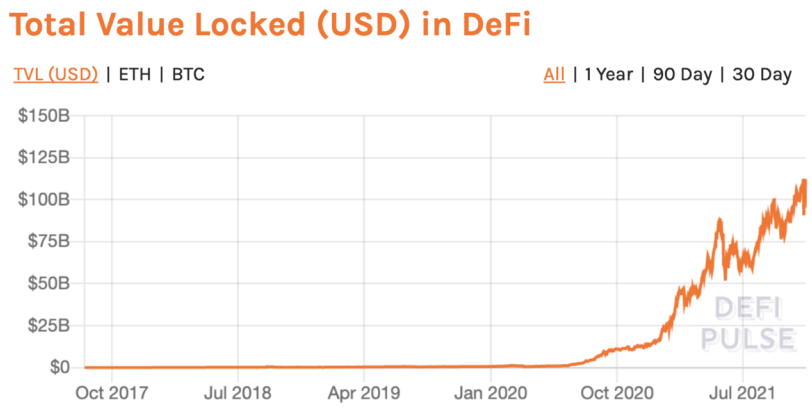
Stablecoin Arrangements and DeFi

The PWG report wisely notes the need to regulate not just the stablecoin issuer, but the other "arrangements" that facilitate the operation of stablecoins. Once issued, a stablecoin can be traded on centralized crypto exchanges as well as on decentralized blockchains pursuant to smart contracts. This means there is no single entity responsible for operation of the stablecoin. Therefore, it is not enough to ensure that the stablecoin issuer complies with reasonable requirements; we need standards for that trading as well, to ensure transparency overall, and to address in particular operational resilience. The software for the various layers

of operation in the case of decentralized blockchains using smart contracts could have flaws or could be vulnerable to attack. The largest stablecoins run on multiple blockchains but are separate and distinct tokens on each such blockchain, as a recent post by Neha Narula of MIT explains. That means risks associated with the integrity and reliability of the blockchains and software are multiplied. In addition, a stablecoin could become too large in relation to the capacity of the blockchain itself. The regulatory framework must address these risks as well.

In addition, we must make sure that there are adequate mechanisms to ensure compliance with KYC, AML and CFT standards in the trading and exchange of stablecoins, regardless of trading platform, to minimize the risk that stablecoins are used for illicit behavior, ransomware, tax evasion or other improper activities..

These stablecoin risks raise the broader question of how we protect the public interest with DeFi platforms generally. DeFi has no single meaning. There are degrees of decentralization and different models. DeFi platforms typically have governance arrangements which in some cases mean that in practice, a small group of validators or other entities or individuals can exercise control. There has been a dramatic growth in DeFi platforms, both for trading as well as in lending and related arrangements. The amount of digital assets "locked" in DeFi protocols has increased dramatically and is reported to exceed $100 billion.



Source: https://defipulse.com/

We need to regulate the *activities* that take place on DeFi platforms—as distinct from the technology itself—when those would otherwise be subject to financial market regulation. Much of what goes on today may implicate securities and derivatives laws. The lack of transparency heightens the concern about risk from multiple rehypothecation of digital assets. Existing regulatory agencies need to examine this activity. I note that Chair Beyer's legislation calls for a report on this which would be very helpful.

The Need to Strengthen Regulation of Digital Assets Generally

Stablecoins represent only about 5% of the total market capitalization of crypto today. Bitcoin is by far the largest non-backed coin, but there are thousands of others. The continued growth of the market poses investor protection risks, as well as risks to society. I would like to explain some of the gaps in regulation generally, and the risks that this creates.

It is often said that from a financial regulatory point of view, a digital asset is either a security or a commodity. [5] Some may therefore conclude that digital assets can be regulated by either the SEC or the CFTC, and the two agencies simply need to get together to resolve any regulatory ambiguity. But that is not an accurate depiction of the situation.

The reality is that neither the SEC nor the CFTC has sufficient authority to regulate the "cash" market for digital assets that are not classified as securities (such as Bitcoin and Ethereum)—the buying and selling of such digital assets and the intermediaries that operate in that market. The SEC only has authority if a digital asset is a security. During my tenure at the CFTC, we declared that cryptocurrencies were commodities. That means the CFTC has authority to regulate *derivative contracts* (that is, futures, swaps and options) based on a cryptocurrency, including the intermediaries involved in their distribution and trading. But the CFTC has very little authority over the cash market for that underlying commodity. It's the same with all commodities: for example, the fact that the CFTC has jurisdiction over cattle *futures* doesn't give it the power to set standards for the buying and selling of cows. [6]

As a result, the crypto industry has not been subject to federal regulation that is comparable to what we have for our securities and derivatives markets. This has meant that the industry has given rise to a whole new class of intermediaries that are largely not regulated at the federal level, including exchanges such as Binance, Coinbase or Kraken. They may be licensed at the state level as money transmitters, but this is not at all equivalent to the federal standards imposed on securities and derivatives exchanges. There are no federal reporting requirements, prohibitions on conflicts of interest, standards to prevent fraud and manipulation, requirements on order execution, or investor protection standards, among others.

The irony of this is that when Bitcoin was launched, the idea was to create a peer-to-peer system that would eliminate the need to rely on large trusted intermediaries. In fact, it has created a whole new class of large, potentially untrustworthy intermediaries.

This was illustrated by a recent enforcement action by the CFTC pertaining to Coinbase. The CFTC imposed a small fine on Coinbase related to wash trading—a form of market manipulation where an investor simultaneously buys and sells the same financial instrument in order to inflate volume, distort pricing or otherwise feed false information to the market. The CFTC has the power to bring a manipulation case in the "cash" market for a commodity because such manipulation could corrupt the derivatives market. But the agency does not regulate Coinbase.

It is not registered with the agency, nor required to comply with its investor protection standards. One CFTC Commissioner explained all of this in a thoughtful statement.

Moreover, what is particularly troubling is this was not a case where Coinbase failed to detect wash trading by a customer. This was wash trading by *Coinbase itself*. The absence of any meaningful regulation means that the entity that owns and operates a crypto exchange can engage in proprietary trading on its own exchange. That, of course, creates a risk of front-running a customer's trades, among other things. We prohibit wash trading on securities and derivatives exchanges, and we do not permit those exchanges to even engage in proprietary trading.

The absence of a federal regulatory framework for crypto intermediaries also creates the risk that they can be used to facilitate or obfuscate illicit activity. This includes funding of black market activity, terrorism or ransomware. The work of FinCEN has been critical in reducing this risk, and U.S. exchanges appear to have stepped up their KYC and AML measures as a result. Still, our ability to prevent and detect such activity would be enhanced if we had regulatory standards that required greater transparency and reporting, as well as prohibitions on fraud and manipulation and in particular activities such as wash trading. A Chainalysis study, for example, found that criminal groups typically make thousands of transfers—often through exchanges or other platforms—to avoid detection of illicit profits.

In addition, over the last decade, we have significantly strengthened cybersecurity requirements for entities that play critical roles in our financial infrastructure. We should require crypto exchanges (as well as decentralized platforms engaged in financial market activities) to meet similar standards. The risk of a hack or other failure could have consequences not just for the exchange or platform; it could also result in collateral damage to other financial infrastructure.

Finally, the continued growth of an unregulated market can create financial stability risks, particularly as more and more investors and institutions participate and there are increasing interconnections. This can occur as a result of a sudden and significant movement in price, particularly if there is significant leverage in the system, as was recently discussed by the Deputy Governor of the Bank of England. (He notes that the subprime mortgage market was $1.2 trillion in size before the 2008 crisis; the crypto market is more than twice that today.) A related concern is that Bitcoin ownership is highly concentrated, and mining capacity even more so, according to a recent MIT paper. All of this argues for greater transparency.

Exchanges and other intermediaries can of course voluntarily adopt standards that address some of the risks I have mentioned, and certainly some are better than others in their policies and practices. Industry self-regulatory groups can also play important roles in defining and promoting adoption of standards. But competitive pressures can undercut good intentions. We need a stronger regulatory framework to lift all exchanges and intermediaries to higher standards and to bring the necessary transparency.

Even without providing new legislative authority, we should make sure that regulators have adequate resources to use their existing powers in this area. We cannot expect them to fulfill their responsibilities in a nearly $3 trillion market today without additional resources.

Central Bank Digital Currencies and Modernizing the Payments System

I noted at the outset the need to develop a national strategy to modernize our payments system, as it is relatively slow and expensive.[7] The Federal Reserve should be commended for the actions it has taken to date—including its FedNow initiative and commencing policy discussion as well as technological research and development on CBDCs. But I believe a more aggressive approach is needed. (I also note the Chairman's legislation would give the Fed clear authority to issue a CBDC, which is good.)

The Fed is expected to issue a report any day on CBDCs, which is not expected to take a position on whether we should create a CBDC, but will presumably discuss the various advantages and disadvantages and possible design choices. The Board of Governors' paper is expected to be followed by a progress report on Project Hamilton, the collaboration between the Boston Federal Reserve Bank and MIT to develop a hypothetical CBDC platform. It will describe the platform architecture and provide some metrics on throughput, speed, resilience and so forth. In addition, the actual code will be made available for inspection. That will enable third parties to give their own assessments of—and suggestions for—the architecture.

This is a good start, but we need a much more intensive effort to design and develop a hypothetical CBDC in order to decide whether we should create one. There is no single way to design a CBDC, and there is debate about potential objectives: how to address Americans' reasonable expectations of privacy in their personal transactions with government's legitimate oversight interests, how to balance financial inclusion with the risk of disintermediating banks, and how to maintain the importance of the dollar in international payment systems. That debate can become too abstract unless coupled with a major effort to design and determine what might be possible. We need an iterative process, a continuous feedback loop between technological work and policy discussion. Moreover, the design and development work will likely generate some policy issues we haven't even thought of.

The fact that China has launched a CBDC does not necessarily mean we must do so, but it should cause us to accelerate our efforts. As other countries explore CBDCs, we must accelerate our development so that we have the technological capability to be at the table in discussions of how to make different national payment systems interoperable and what standards should govern.

The government should involve the best talent from the private sector as well as academia in this effort. It is not quite like putting a man on the moon, but it is certainly of great national importance.

One objective often cited for a CBDC (and stablecoins) is improving access to financial services. While a more intensive development effort will help determine whether a CBDC is a good solution, we should prioritize that goal regardless, because the need is so great. According to the most recent FDIC survey found 5.4% of American households were unbanked, and an additional 17.2% were underbanked, meaning they have a bank account but still use nonbank services such as check cashing firms or payday lenders. The problem is greatest among Black and Latino households. Moreover, lower-income households represent a higher percentage of the unbanked in the United States than they do in other countries.

A slow payments system contributes to the problem in a few ways. Households who live paycheck to paycheck often cannot afford to wait the two or three days it may take for a bank to clear a check. By going to a check cashing service, they may pay a fee, but they get cash right away and the service may even pay their bills for an additional charge. The fee may be high but it avoids the risk of overdraft charges which are typically even higher. Federal Reserve data found that 70% of those who use check cashing services have bank accounts, and people with bank accounts present a majority of the checks cashed by such services.

There have been many suggestions as to how to tackle the financial inclusion challenge that do not require development of a CBDC or a regulated stablecoin.[8] We should make it a priority now to address the problem, one way or another.

Conclusion

I noted at the beginning of my remarks that our situation today is similar to what happened with the swap industry. We did not act to create regulatory standards until the industry created excessive risks that intensified the 2008 global financial crisis. I was part of a small group of attorneys that drafted the initial master agreements for interest rate swaps over 30 years ago, and I saw how swaps could create beneficial hedging. Later, as chairman of the Commodity Futures Trading Commission, I oversaw the agency responsible for implementing the regulatory framework to address the damage caused by an unregulated industry. There is no question that the industry is healthier today because of it.

We are faced today with a wave of innovation that is similarly creating benefits as well as risks. We should act now to make sure our regulatory framework is one where investors are protected, legitimate government interests are met, financial stability is not compromised, and innovation can continue to flourish.

[1] I am a Research Fellow at the Harvard Kennedy School and an Adjunct Professor of Law at the Georgetown Law Center. I also provide advisory services on financial regulatory and fintech matters. I was previously Chairman of the U.S. Commodity Futures Trading Commission, 2014-2017; Assistant Secretary for Financial Stability of the U.S. Treasury Department, 2010-2014; General Counsel, Office of Financial Stability, 2009-2010; and a partner in the law firm Cravath, Swaine & Moore.

[2] I discuss this in my paper, "It's Time to Strengthen the Regulation of Crypto-Assets," The Brookings Institute, March, 2019, https://www.brookings.edu/research/its-time-to-strengthen-the-regulation-of-crypto-assets/

[3] I suggested in one article that the SEC could regulate stablecoins as money market mutual funds to be consistent with the theme of the article, which was that stablecoins could "break the buck" just as the Reserve Primary Fund had in September 2008, but I do not think it is the best way to regulate them for the reasons noted above.

[4] The figure is as of December 31, 2020 and is from the Form 10-K reports of CME Group Inc. at https://www.sec.gov/ix?doc=/Archives/edgar/data/1156375/000115637521000020/cme-20201231.htm (page 64) and Intercontinental Exchange, Inc. at https://www.sec.gov/ix?doc=/Archives/edgar/data/1571949/000157194921000003/ice-20201231.htm (page 16).

[5] I am not suggesting that the security/commodity classifications are meant to cover all digital assets, especially the category of what are often called "utility tokens", which represent a right to access digitally a blockchain application. I am simply noting that this is frequently how the regulatory picture is explained.

[6] As noted in my 2019 paper, the CFTC can pursue cases of fraud and manipulation in a cash commodity market, and those pertaining to retail leveraged transactions, but this is not a viable means to set standards generally for trading in that market.

[7] See, for example, Christian Catalini and Andrew Lilly, "Why is the United States Lagging Behind in Payments?", July 27, 2021. While the authors are affiliated with the Diem Association, the paper is nevertheless a very concise explanation of the issues.

[8] The ways in which CBDCs and stablecoins could potentially help address financial inclusion are discussed in many papers, including the FedAccounts proposal by Morgan Ricks, J. Crawford and L. Menand which proposes creating FedAccounts without waiting for new technology, and my own writing. For a discussion of other means to address financial inclusion, see Aaron Klein, "Can fintech improve health?", The Brookings Institute, September 24, 2021.

Wharton
University of Pennsylvania

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.*

Wharton
UNIVERSITY of PENNSYLVANIA

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.

Wharton
University of Pennsylvania

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/.

Wharton
University of Pennsylvania

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.

TESTIMONY OF

Peter Van Valkenburgh

Research Director of Coin Center[1]

BEFORE THE

United States Congress Joint Economic Committee

"Demystifying Crypto: Digital Assets and the Role of Government"

November 17, 2021

On Halloween 13 years ago, an email to a public mailing list shared a link to a pdf.[2] It was the Bitcoin white paper: 3,192 words, a handful of simple illustrations, and some C++ computer code. The following January, a 2 MB computer program was made freely available for download to the same public mailing list.[3] Less than five years later, the person or persons sending these emails, under the pseudonym Satoshi Nakamoto, sent their last message and has not been heard from since.[4]

---

[1] Coin Center is an independent nonprofit research and advocacy center focused on the public policy issues facing cryptocurrency technologies such as Bitcoin. Our mission is to build a better understanding of these technologies and to promote a regulatory climate that preserves the freedom to innovate using open blockchain technologies.We do this by producing and publishing policy research from respected academics and experts, educating policymakers and the media about blockchain technology, and by engaging in advocacy for sound public policy.

[2] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," White Paper, October 31, 2008, https://www.coincenter.org/bitcoin.pdf.

[3] Satoshi Nakamoto, "Bitcoin v.01 released," Cryptography Mailing List, January 8, 2009, *available at*: https://www.metzdowd.com/pipermail/cryptography/2009-January/014994.html.

[4] The final email from Satoshi Nakamoto was sent on December 13, 2010, the day after his final post on the BitcoinTalk forums. No other communication came from Satoshi until 2014, when he activated another old forum account to write that he was "not Dorian Nakamoto," in response to a debacle wherein a *Newsweek* reporter had claimed to have unmasked the true identity of Satoshi. *See*: Satoshi Nakamoto, "[bitcoin-list] Bitcoin 0.3.19 is released," bitcoin-list, December 13, 2010, available at: https://sourceforge.net/p/bitcoin/mailman/message/26744510/; Satoshi Nakamoto, "Added some DoS limits, removed safe mode (0.3.19)," BitcoinTalk forum, December 12, 2010, https://bitcointalk.org/index.php?topic=2228.msg29479#msg29479; Satoshi Nakamoto, "Bitcoin open source implementation of P2P currency," P2P Foundation forum, March 7, 2013, http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source?commentId=2003008%3AComment%

Today, a few thousand words, a computer file smaller than a cat video, and a missing author, have brought about an economic revolution. Over three trillion dollars[5] worth of economic activity recorded and secured on blockchains: shared ledgers that no single person, corporation, or government permissions or controls.[6]

Who can we thank for that remarkable, utterly unpredictable outcome? Not just the person or persons who went by Satoshi Nakamoto. They stood on the shoulders of brilliant cryptographers and computer scientists.[7] Perhaps above all they were inspired by another shared and open network that no single person controls: the internet. A place where a good idea shared anonymously and publicly can stand on its merits, spread to a community of like-minded innovators, and flourish.

America grew rich because of our openness, the ingenuity of immigrants, entrepreneurs, explorers, and technological pioneers. We don't like permissioned systems in this country because we know you can't prejudge genius. We want open systems. We afford dignity and access even to people we don't yet know or understand. As Steve Jobs would have put it, "The crazy ones. The misfits. The rebels."

So I'm not going to tell you *who* is going to show up on the Bitcoin blockchain or the coming decentralized web or *what* they are going to build. I couldn't tell you that today any more than I could have told you in 1990 that Satoshi will show up on the internet alongside Sergey and Larry with Google and Jimmy Wales with Wikipedia.

All I'm going to tell you is that we've finally built a tool that can make money work without banks,[8] make organizations work without corporations and courts,[9] make sharing and

---

3A52186; Leah McGrath Goodman, "The Face Behind Bitcoin," *Newsweek*, March 6, 2014, https://www.newsweek.com/2014/03/14/face-behind-bitcoin-247957.html.

[5] A rough estimate of the current capitalization of the cryptocurrency economy is available at: https://coinmarketcap.com/.

[6] Peter van Valkenburgh, "Open Matters: Why Permissionless Blockchains are Essential to the Future of the Internet," *Coin Center*, December 2016, https://www.coincenter.org/open-matters-why-permissionless-blockchains-are-essential-to-the-future-of-the-internet/.

[7] The digital signature algorithms, Merkle trees, and hash functions that undergird networks like Bitcoin and Ethereum were researched and developed by several scientists and mathematicians going back to the 1950s. Satoshi's primary contribution was to arrange these mechanisms into a system that could do something entirely novel, create scarce digital units that could be sent and received online, person-to-person without any trusted institution acting as a middle man.

[8] Jerry Brito, "The Case for Electronic Cash," *Coin Center*, February 2019, https://www.coincenter.org/the-case-for-electronic-cash/.

[9] Houman Shadab, "Smart Contracts, *Coin Center*, December 15, 2014, https://www.coincenter.org/education/key-concepts/smart-contracts/.

transacting online work without Big Tech,[10] and that because of that change there's a better chance that tomorrow's misfits will be able to speak, share, and innovate.

This truly American ideal, however, isn't about anarchy. It's about opportunity and equality under the *law*. Bitcoin and follow-on cryptocurrencies are not unregulated.[11] Sensible, technology-neutral regulations have protected consumers[12] and investors,[13] and prevented money laundering and illicit finance.[14] The American approach is to regulate activities, not to ban or blacklist the publishing of new ideas and tools.

Anyone can freely write and share the open source software that makes these technologies work, and any prior restraint on sharing that expressive content violates our First Amendment rights.[15] However, if you promise an investor you'll invent and build them a new, future cryptocurrency, we expect you to register as the issuer of a security.[16]

No one is made to open their homes and private bitcoin wallets to a search by the police without a warrant.[17] But if you provide a service to help people buy and sell bitcoin as a third party, you are expected to know your customers and apply anti-money laundering controls.[18]

---

[10] Muneeb Ali, "How can blockchains improve the internet's infrastructure?" *Coin Center*, April 18,2017, https://www.coincenter.org/education/crypto-regulation-faq/how-can-blockchains-improve-the-internets-infrastructure/.
[11] Jerry Brito, "Is Bitcoin regulated?" *Coin Center*, January 13, 2015, https://www.coincenter.org/education/blockchain-101/is-bitcoin-regulated/.
[12] Peter Van Valkenburgh and Jerry Brito, "State Digital Currency Principles and Framework," *Coin Center*, March 2017, https://www.coincenter.org/app/uploads/2020/05/statevirtualcurrencyprinciplesandframeworkv2.0.pdf.
[13] Peter Van Valkenburgh, "An Updated Framework for Securities Regulation of Cryptocurrencies," *Coin Center*, August 18, 2018, https://www.coincenter.org/an-updated-framework-for-securities-regulation-of-cryptocurrencies/.
[14] US Department of the Treasury, Financial Crimes Enforcement Network, "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies," Guidance FIN-2013-G001 (Mar. 18, 2013) https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf; and US Department of the Treasury, Financial Crimes Enforcement Network, "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies," Guidance FIN-2019-G001 (May 9, 2019) https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20CVC%20Guidance%20FINAL.pdf.
[15] Peter Van Valkenburgh, "Electronic Cash, Decentralized Exchange, and the Constitution," Coin Center, March 2019, https://www.coincenter.org/app/uploads/2020/05/e-cash-dex-constitution.pdf.
[16] *Supra* note 12.
[17] *Supra* note 14.
[18] Peter Van Valkenburgh, "FinCEN's new cryptocurrency guidance matches Coin Center recommendations," *Coin Center*, May 9, 2019, https://www.coincenter.org/fincens-new-cryptocurrency-guidance-matches-coin-center-recommendations/.

There are some gaps in America's crypto public policy. The gaps are not, contrary to popular belief, a central bank digital currency gap with China. The CCP is more interested in banning permissionless tools like Bitcoin[19] and substituting a surveillance tool[20] that will give them even more control over the misfits within their borders. We should not emulate that policy.

The gaps are much more mundane; they deal with securities and commodities futures policies and tax issues. Below we will discuss them in turn by category.

A. Securities and commodities futures policy

On the margin, securities and commodities futures laws can be improved and there are well-drafted bills in the House that address those issues. They fall into two major baskets: clarity for the developers of new cryptocurrencies and cryptocurrency secondary market oversight.

1. Clarity for developers of new cryptocurrencies.

First, pre-sales of future cryptocurrencies, often called "initial coin offerings" or "ICOs", already meet the definition of securities and, indeed, investors protections and disclosures afforded by the securities laws are sensible and should be fairly applied in the context of promises of future cryptocurrencies. However, once a cryptocurrency has launched, the application of securities laws is no longer appropriate.[21] Once the network has launched, anyone can participate in maintaining the ledger and anyone can see and propose changes to the cryptocurrency's protocol software.[22] As such, information asymmetries meant to be addressed by securities laws disclosures are no longer present and no person or persons is in a position to make disclosures on behalf of the open network. While other investor protection measures may continue to apply and remain relevant and appropriate, the disclosure regime inherent in securities issuance regulation is a poor fit.[25]

Nonetheless, there can be some ambiguity regarding whether a newly developed cryptocurrency continues to meet the flexible definition of a security even after the software has been developed and the network is live. We believe that the SEC has avoided overbroad interpretation of this ambiguity thus far but prefer a legislative solution for the long term.

---

[19] Andrey Sergeenkov, "China Crypto Bans: A Complete History," *CoinDesk*, September 29, 2021, https://www.coindesk.com/learn/china-crypto-bans-a-complete-history/.
[20] Alex Gladstein, "Financial Freedom and Privacy in the Post-Cash World," *Cato Journal*, Spring/Summer 2021, https://www.cato.org/cato-journal/spring/summer-2021/financial-freedom-privacy-post-cash-world#.
[21] *Supra* note 12.
[22] *Id.*
[25] See *infra* subsection A.2. on secondary market supervision.

Chairman McHenry has introduced a safe harbor for developers of new cryptocurrencies[24] based on an earlier proposal from SEC Commissioner Hester Peirce.[25] Under the proposal, if developers pre-sold a new cryptocurrency in a manner compliant with securities laws[26] and if they register under the safe harbor provisions, which require sensible, technology-appropriate disclosures,[27] then the SEC will commit to forbearance for three years. This approach has the advantage of not altering the necessarily flexible[28] definition of a security in the law while also providing some assurance that innovators acting in good faith will not be the target of a surprise enforcement action. Congressman Emmer has introduced a bill that would subtly alter the definition of securities to limit its applicability such that it could not include truly open source, open network cryptocurrencies.[29]

2. Secondary market supervision.

While cryptocurrency exchanges here in the U.S. are currently regulated as state money transmitters[30] or state chartered banks or trust companies,[31] these regulatory forms focus primarily on prudential and consumer protection controls (*e.g.* minimum capital and permissible investment requirements) rather than market integrity (*e.g.* prevention of market manipulation and systemic risk). The SEC and CFTC both have competency supervising trading venues for market integrity but neither has jurisdiction over trading venues dealing exclusively in cryptocurrencies (the CFTC supervises commodities derivatives markets while the SEC supervises securities markets; cryptocurrency exchanges are typically commodities spot markets only[32]). Last session, Chairman Conoway introduced legislation that would grant the

---

[24] "Clarity for Digital Tokens Act of 2021," HR 5496, 117th Congress (2021-2022), https://www.congress.gov/bill/117th-congress/house-bill/5496/text.

[25] Hester Peirce, "Token Safe Harbor Proposal 2.0," U.S. Securities and Exchange Commission, April 13, 2021, https://github.com/CommissionerPeirce/SafeHarbor2.0.

[26] "Framework for 'Investment Contact' Analysis of Digital Assets," U.S. Securities and Exchange Commission, April 3, 2019, https://www.sec.gov/files/dlt-framework.pdf.

[27] *E.g.* the source code, transaction history, transaction economics, development plan, and token history relating to the project.

[28] Almost a hundred years of securities regulation confirms the need for a flexible approach that is based on the economic realities of a transaction. If merely avoiding certain magic words, like equity or bond, within the four corners of an investment contract was sufficient to avoid securities laws, then avoiding disclosure would be trivially easy. This has proven true even in the context of cryptocurrencies where mere claims of decentralization and non-reliance on a promoter or third party can be revealed to be fraudulent, and the securities laws can and should then be applied.

[29] "Securities Clarity Act," HR 8378, 116th Congress (2019-2020), https://www.congress.gov/bill/116th-congress/house-bill/8378; "Securities Clarity Act," HR 4451, 117th Congress (2020-2021), https://www.congress.gov/bill/117th-congress/house-bill/4451.

[30] Marco Santori, "What is Money Transmission and Why Does it Matter?" *Coin Center,* April 2015, https://coincenter.org/entry/what-is-money-transmission-and-why-does-it-matter.

[31] *For example*: https://www.kraken.com/en-us/learn/finance/spdi-bank-charter.

[32] "Bitcoin Basics," U.S. Commodity Futures Trading Commission, December 2019, https://www.cftc.gov/sites/default/files/2019-12/oceo_bitcoinbasics0218.pdf.

CFTC authority to supervise cryptocurrency spot markets.[33] It provides a flexible approach that would make CFTC regulation optional but would require that newly launched cryptocurrencies (where early investors may exert outsized market power) must initially be traded to the retail public only on CFTC supervised exchanges.[34]

B. The Infrastructure Investment and Jobs Act

The recently passed infrastructure bill included rushed language that could unintentionally stifle innovation and invade personal privacy. In the Senate there was a bipartisan solution with widespread support but procedurally it was impossible to implement before the bill's passage.[35] Ideally, new legislation would address two problems:

1. "Broker" definition and third party reporting.

The infrastructure package amended the definition of "broker" in the tax code.[36] This definition determines who must perform third party reporting of capital gains.[37] The new definition should be tightened so that it could not inadvertently place reporting obligations on persons within the cryptocurrency ecosystem who have neither customers nor any reason to obtain private information about other cryptocurrency users. It is entirely reasonable to expect custodial cryptocurrency exchanges to do third party tax reporting. However, it is inappropriate to ask non-custodial persons such as cryptocurrency miners and software developers to surveil persons who are not their customers.[38]

2. 6050I reporting.

The 6050I provision of the U.S. tax code obligates businesses to file reports (including names and Social Security numbers) about their counterparties whenever they receive more than

---

[33] "Digital Commodity Exchange Act of 2020," HR 8373, 116th Congress (2019-2020) https://www.congress.gov/bill/116th-congress/house-bill/8373.
[34] *Ibid.*
[35] "Portman, Warner, Toomey, Sinema, Lummis Announce Agreement on Digital Asset Reporting Requirements in the Bipartisan Infrastructure Bill," Press Release, August 9, 2021, https://www.banking.senate.gov/newsroom/minority/toomey-warner-lummis-sinema-portman-announce-agreement-on-digital-asset-reporting-requirements-in-infrastructure-bill.
[36] "Infrastructure Investment and Jobs Act," HR 3684, 117th Congress (2021-2022) https://www.congress.gov/bill/117th-congress/house-bill/3684.
[37] 26 U.S.C. § 6045.
[38] Peter Van Valkenburgh, "When does a company actually control customer bitcoins?" *Coin Center*, March 24, 2016, https://www.coincenter.org/education/policy-and-regulation/custody/.

$10,000 in cash.[39] Amendments in the infrastructure package will require similar reporting when businesses receive more than $10,000 in cryptocurrencies.[40] Typically Coin Center does not object to equal treatment of cash and cryptocurrencies, but the §6050I reporting provision is a draconian surveillance rule that should have been ruled unconstitutional long ago.

Warrantless private data collection is tolerated under the fourth amendment when it is performed by third parties (*e.g.* banks or money transmitters) who have obtained that information from their customers voluntarily and retained that information for a legitimate business purpose.[41] 6050I reports are just as intrusive of personal privacy as the warrantless data collection performed by banks and other third parties but, in the case of a 6050I report, there is no third party and therefore the third party doctrine of the 4th Amendment could not possibly exempt the search from a warrant requirement. Under 6050I, one person to a two person transaction is obligated to collect sensitive information from her counterparty and hand that to government officials without any warrant or reasonable suspicion of wrongdoing. In the case of two persons exchanging two different cryptocurrencies, they each would have to report on the other. The law literally asks one American citizen to inform on another if the transactions in which the two are engaged are "business" and if they take place using cash or cryptocurrencies. We believe that a constitutional challenge to 6050I will eventually succeed in overturning the requirement, however we prefer a legislative fix.

C. Other issues

Existing IRS policy leaves taxpayers uncertain of their obligations with regard to cryptocurrency transactions. Three common sense measures can be taken by congress to address this issue.

1. *De minimis* tax exemption from capital gains treatment.

Every time a cryptocurrency user purchases a good or a service using cryptocurrency she will have a taxable event. She must account for any capital gains or losses in cryptocurrency from the time she first purchased the cryptocurrency to the time she used it to purchase a good or service. While this is reasonable for large purchases with substantial gains, it imposes unreasonably high transaction and accounting costs for small transactions. A similar problem existed for purchases made using foreign currency and Congress passed a de minimis

---

[39] Peter Van Valkenburgh, "An unworkable and arguably unconstitutional tax change tucked away in the infrastructure bill," *Coin Center*, September 17, 2021, https://www.coincenter.org/an-unworkable-and-arguably-unconstitutional-tax-change-tucked-away-in-the-infrastructure-bill/.
[40] *Ibid.*
[41] *Supra* note 15; *Carpenter v. United States*, 585 U.S. __ (2018) https://supreme.justia.com/cases/federal/us/585/16-402/.

exemption from capital gains treatment for transactions where the gain is less than $300.[42] A similar exemption should exist for cryptocurrency transactions. In the House, Representatives DelBene and Schweikert have introduced legislation that would create that exemption.[43]

2. Clarity for assets derived from cryptocurrency forks

Cryptocurrency networks can fork when disparate factions of network participants cease to agree regarding the foundational rules of the cryptocurrency protocol's software.[44] After a fork occurs, users who had cryptocurrency before now *may* have access to cryptocurrency on both sides of the fork. If they had previously held their cryptocurrency directly (by personally controlling the private keys that correspond to addresses on the cryptocurrency network) they would be able to use these keys to spend cryptocurrency on both sides of the fork. If, on the other hand, a user has entrusted a company to secure their cryptocurrency, then they will have access to cryptocurrency on both sides of the fork if, and only if, their service-provider chooses to support both forks. In either case, spending cryptocurrency on one side of the fork does not spend cryptocurrency on the other side. Therefore, the taxpayer will have obtained access to new assets more akin to a stock split than a trade. However, the open nature of cryptocurrency networks and network software means that this split could occur by virtue of the actions of anyone on the network with sufficient followers to go their own way. Moreover, the user may be unaware of the split and may have no knowledge that their private keys can access a new forked asset.

If a cryptocurrency user sells some of their forked assets they likely owe capital gains, that much is clear and uncontroversial. However, there are several additional questions: did the fork itself create an income event for cryptocurrency users or is it more like a stock split which is not treated as income? What is the basis for the forked asset; is it a zero-basis windfall or a division of the asset's previous value like a stock split? Representative Emmer has introduced legislation that would create a safe harbor from penalties for taxpayers who made a good faith effort to pay taxes related to forked assets in the past, despite the lack of clarity.[45] It would also instruct the IRS to not treat forks as income events in and of themselves because that policy would create unreasonable liabilities for taxpayers.[46] As mentioned, a taxpayer may not even be aware that a

[42] "Foreign Tax Credit Compliance Tips," U.S. Internal Revenue Service, accessed November 12, 2021, https://www.irs.gov/individuals/international-taxpayers/foreign-tax-credit-compliance-tips.
[43] "Virtual Currency Tax Fairness Act of 2020," HR 5636, 116th Congress (2019-2020), https://www.congress.gov/bill/116th-congress/house-bill/5635/; "H.R.3708 - To amend the Internal Revenue Code of 1986 to exclude from gross income de minimis gains from certain sales or exchanges of virtual currency, and for other purposes," HR 3708, 115th Congress (2017-2018), https://www.congress.gov/bill/115th-congress/house-bill/3708.
[44] Peter Van Valkenburgh, "Hard Fork," *Coin Center*, October 9, 2019, https://www.coincenter.org/education/key-concepts/forks/.
[45] "Safe Harbor for Taxpayers with Forked Assets Act of 2021," HR 3273 117th Congress (2021-2022), https://www.congress.gov/bill/117th-congress/house-bill/3273.
[46] *Ibid.*

fork has occurred and may take no action to claim newly forked assets. No tax should be owed under those circumstances and liabilities should apply later, when the taxpayer exercises dominion and control over the assets by selling them.

3. Taxation of mining and staking rewards

The IRS has determined that cryptocurrency mining and staking rewards should be taxed as income when they are generated.[47] For the reasons below, this is a bad policy and should be corrected by Congress.

Cryptocurrency stakers and miners dedicate costly computing resources to securing and sharing the public data that makes these technologies work, the public blockchains of Bitcoin, Ethereum, and other permissionless networks. In return, the protocols are designed to allow these participants to create new units of cryptocurrency according to set release schedules. This is the incentive that makes an open network viable; if there was no reward to honest participation, then some other mechanism, like permissioning which computers can and cannot have access, would be required to secure the data.

These rewards are not, however, equivalent to being paid wages for labor. There's no person or company that is making a payment, the "payment" is the creation of new property by mixing one's own labor with one's own property. The better metaphor for these rewards would be to liken them to crops growing on one's property. Every additional ear of corn in one's field is a windfall to be certain, but taxing them at the moment of their creation would be an absurdity and an accounting nightmare. In that context we tax the farmer when she sells her corn at market for a profit. Cryptocurrency rewards from staking and mining should be treated the same. Treating them like income creates perverse incentives to sell the new cryptocurrency immediately as it is produced in order to cover tax liabilities. Any delay could risk a decline in the market price and an inability to cover past nominal income tax obligations. Moreover, some cryptocurrency networks afford several thousand small rewards every day; taxing each at its moment of creation with its own unique accounting basis is a recipe for complexity and poor compliance.

The simple solution is simply to tax the sale of mining and staking rewards rather than taxing their creation as income. If the early Internet is any indication, simplified tax regimes do not mean less revenue for governments. Quite the opposite, as clear rules lead to better compliance and the growth of profitable industry here in America rather than abroad.

---

[47] Peter Van Valkenburgh, "Congress to IRS: Proof-Of-Stake block rewards should not be taxed as income," *Coin Center*, August 4, 2020, https://www.coincenter.org/congress-to-irs-proof-of-stake-block-rewards-should-not-be-taxed-as-income/.

4. Safe harbor for non-custodial uses

State money transmission licensing laws are broadly drafted and carry harsh penalties for failure to comply. There is no reason for these laws to ever apply to persons who facilitate cryptocurrency use but who do not hold other people's coins. Only custodians present a risk of loss that would be sensibly addressed through licensing.[48]

But clarifying this particular interpretation of each state's unique money transmission statute is a slow and inconsistent process, even with great model legislation from the ULC available.[49] A federal safe harbor would instantly make the entire U.S. a welcoming home for developers and technologists who are designing, building, and operating the fundamental infrastructure behind cryptocurrency and open blockchain networks.[50] To that end, the Blockchain Regulatory Certainty Act sponsored by Reps. Emmer and Soto would create a safe harbor from state licensing requirements for non-custodial entities in the cryptocurrency space.[51]

There's no reason why America can't continue to be a home for permissionless innovation while also enriching its treasury. We did it with the early internet and we will do it again with cryptocurrency networks.

---

[48] Peter Van Valkenburgh, "When does a company actually control customer bitcoins?" *Coin Center*, March 24, 2016, https://www.coincenter.org/education/policy-and-regulation/custody/.

[49] Peter Van Valkenburgh, "The ULC's model act for digital currency businesses has passed. Here's why it's good for Bitcoin." *Coin Center,* July 19, 2017, https://www.coincenter.org/the-ulcs-model-act-for-digital-currency-businesses-has-passed-heres-why-its-good-for-bitcoin/.

[50] Peter Van Valkenburgh, "Congress should create a blockchain technology safe harbor. Luckily they already figured it out in the '90s." *Coin Center,* April 6, 2017, https://www.coincenter.org/congress-should-create-a-blockchain-technology-safe-harbor-luckily-they-already-figured-it-out-in-the-90s/.

[51] Abby Rime, "Emmer Introduces Legislation to Provide Clarity for Blockchain Innovators," Press Release, August 17, 2021, https://emmer.house.gov/2021/8/emmer-introduces-legislation-to-provide-clarity-for-blockchain-innovators.

RESPONSE FROM MS. ALEXIS GOLDSTEIN TO QUESTIONS FOR THE RECORD SUBMITTED BY CHAIRMAN BEYER

1. Given the increasing number of countries exploring digital currencies, including China, do you think that the Federal Reserve should be given explicit authority issue a digital dollar? If the Fed does not issue a digital dollar, are you concerned about the U.S. dollar losing its role as the world's reserve currency?

- To the extent that the Federal Reserve ("Fed") needs additional authorities to issue a digital dollar, Congress should contemplate granting it. Some cryptocurrency market actors have implied they do intend to challenge the primacy of the U.S. dollar[1] or that so-called stablecoins and so-called decentralized finance enable participants to "get rid of their fiat."[2] The CEO of the cryptocurrency exchange Kraken has also made derisive statements about Federal Reserve notes,[3] suggesting that market participants would like to overtake U.S. dollars as a mode of exchange, despite Kraken applying for a master account with the Fed.[4] The Fed should monitor for any current, potential, and ongoing risks to the dollar, including the introduction of private money.

2. It is my understanding that thousands of transactions a day for millions of dollars are not recorded on the blockchain and are instead settled "off-chain". Are "off chain" digital asset transactions a problem and should regulators require that these transactions are reported to a central repository?

- One of the purported benefits of various blockchains and distributed ledgers is transparency—including that transactions are publicly viewable. Off-chain transactions lack this transparency, and leave both the public and regulators reliant on the firms and/or entities conducting the off-chain transactions to provide full and fair disclosure. One indicator of potential systemic risk is opacity (in addition to leverage and interlinkages between market participants), and the prominent of off-chain transactions raise this risk. The opacity of off-chain transactions does raise risks. Regulators and Congress alike should consider ways to bring more transparency, not just to off-chain transactions, but to the crypto asset markets broadly.

3. The CFTC just fined Tether—the issuer of USDt—$41 Million for making false and misleading statements about its reserve holdings, after finding that USDt was only backed one for one with dollars just 27 percent of the time. Given that USD Tether is the most actively traded digital asset in the World, should the CFTC fine have been bigger to discourage similar activities by other fiat based stablecoin issuers in the future?

- All regulators, including the Commodity Futures Trading Commission (CFTC), should ensure that settlement fines are sufficiently large to deter future offenses, rather than being seen as merely the cost of doing business by the offending firm. I would also note that transaction volumes in cryptocurrency markets need to be viewed skeptically, as the market lacks regulatory oversight to allow for reliable market data reporting.

4. In 2018 senior SEC officials announced that Bitcoin and Ethereum, the two largest digital assets by market capitalization, would not be treated as securities. The CFTC has taken the position that both Bitcoin and Ethereum are commodities and permitted CFTC exchanges to offer futures and swaps contracts on both digital assets. However, the regulatory status

---

[1] *Investor Presentation*, CIRCLE (Jul. 7, 2021), *https://www.sec.gov/Archives/edgar/data/0001824301/000121390021036070/ea143875ex99093_concordacq.htm* at 23. (In the Investor Presentation included in Circle's July 2021 8-F SEC filing, Circle states that the "opportunity" and "long-term addressable market" for USDC is all $130 trillion of the M2 money supply.)

[2] Jake Chervinsky, head of policy for the Blockchain Association (@jchervinsky), TWITTER (Aug. 27, 2021, 3:09 PM), *https://twitter.com/jchervinsky/status/1431333014907277312*. ("I mean sure, that's a cute retort, but the point of decentralized exchange is to let people get rid of their fiat & buy bitcoin without relying on a centralized intermediary to execute the trade. You need a decentralized fiat instrument to do that.")

[3] Jesse Powell, CEO of Kraken (@jespow), TWITTER (Aug. 29, 2021, 2:48 AM), *https://twitter.com/jespow/status/1431871317138018306*. ("Except #bitcoin is issued by the public, transparently, predictably according to math and code that is freely available for all to audit. Contrast this with the privately issued, unpredictable, shadowy, Federal Reserve Note, operated by the elite, without independent audit.")

[4] Robert Stevens, *Kraken Will Be First US Crypto Bank. Here's Why It Matters*, DECRYPT (Sep. 16., 2020), *https://decrypt.co/42077/kraken-first-us-crypto-bank-heres-why-matters*.

of many other digital assets remains unclear. Should Congress mandate that the SEC and CFTC work together to clarify the status of other major digital assets?

- The Commodity Futures Trading Commission (CFTC) and the Securities and Exchange Commission (SEC) have multiple avenues for ongoing dialog and collaboration, including but not limited to formal MOUs and informal modes of engagement. As previously noted by CFTC Commissioner Dan Berkovitz, the Commodity Exchange Act "does not contain any exception from registration for digital currencies, blockchains, or 'smart contracts.'"[5] SEC Chair Gensler has stated that "It doesn't matter whether it's a stock token, a stable value token backed by securities, or any other virtual product that provides synthetic exposure to underlying securities. These products are subject to the securities laws and must work within our securities regime."[6] The SEC and the CFTC should continue to enforce all existing laws and regulations.

RESPONSE FROM MS. ALEXIS GOLDSTEIN TO QUESTION FOR THE RECORD SUBMITTED BY SENATOR CASSIDY

Discussions around cryptocurrency, especially at this hearing, focus on what the Federal Government's role in cryptocurrency regulation should be. While the Federal Government considers its approach, states are starting to take action. Some examples include Wyoming setting up regulations allowing for cryptobanks, while New York has introduced its BitLicense. From the different approaches taken by states toward digital currency, what lessons can the Federal Government take away?

- A number of states take different approaches to crypto asset oversight. State based regulation is often inadequate to mitigate national risks, including systemic risks, and may also lead to market fragmentation. The Federal Government should focus its attention on oversight, ensuring there is adequate enforcement of existing securities and derivatives laws, as well as identifying if there are any regulatory gaps that require action to ensure consumer and investor protection in the cryptocurrency space—including the ability for regulators to monitor for systemic risk.

RESPONSE FROM MS. ALEXIS GOLDSTEIN TO QUESTIONS FOR THE RECORD SUBMITTED BY SENATOR KLOBUCHAR

1. As mentioned in your testimony, late last month, developers of a new cryptocurrency sought to take advantage of the popularity of Netflix's Korean thriller "Squid Game" and introduced a "Squid" coin. Between October 26 and November 1, the value of a Squid coin rose by more than 23 million percent, from a little more than a mere cent to $2,861.80.

Early on the morning of November 1, the value of a Squid coin collapsed from a high of just over $2,860 to effectively zero as cryptocurrency traders watched the token's unknown creators clean out some $3.3 million in funds, according to digital records. The maneuver, known as a "rug pull" in cryptocurrency circles, occurs when a token's creators abandon the project by exchanging many virtual coins for real-world cash. They quickly drain liquidity from the product, effectively driving 3 the coin's value to zero and leaving other investors holding the bag in an apparent scam.

With the anonymity and complexity of cryptocurrency, what protections do American investors, particularly retail investors, have from predatory creators of digital currencies?

- Retail investors should receive the same protections when they trade crypto assets as they do when they trade equities and/or derivatives. Regulators have noted that there are no exceptions from existing laws for crypto assets. For example, former CFTC Commissioner Dan Berkovitz has noted that the Com-

---

[5] CFTC Commissioner Dan M. Berkovitz, *Keynote Address Before FIA and SIFMA-AMG, Asset Management Derivatives Forum*, COMMODITY FUTURES TRADING COMMISSION (Jun. 8, 2021), *https://www.cftc.gov/PressRoom/SpeechesTestimony/opaberkovitz7*.

[6] SEC Chair Gary Gensler, *Remarks Before the Aspen Security Forum*, SECURITIES AND EXCHANGE COMMISSION (Aug. 3, 2021), *https://www.sec.gov/news/public-statement/gensler-aspen-security-forum-2021-08-03*.

modity Exchange Act "does not contain any exception from registration for digital currencies, blockchains, or 'smart contracts.'"[7] Securities and Exchange Commission Chair Gensler has also noted in remarks before the SEC's Investor Advisory Committee that many crypto asset tokens "may be unregistered securities, without required disclosures", further clarifying that "to the extent that there are securities on these trading platforms, under our laws they have to register with the Commission unless they meet an exemption."[8] All investors in crypto assets deserve the protections that Americans have come to expect when trading in U.S. markets.

2. There are many national security concerns in this space, from ransomware to illicit payments and financial crimes. This October, the Treasury's Office of Foreign Assets Control (OFAC), which publishes lists of individuals and companies owned or controlled by, or acting for or on behalf of, countries subject to U.S. sanctions, released new guidance—clarifying that all digital market participants are expected to monitor their users against the sanctions list.

What are the challenges for the industry in complying with this guidance?

- The October guidance from Treasury's Office of Foreign Assets Control noted that Specially Designated Nationals and Blocked Persons List (the "SDN List") has included virtual currency addresses since 2018, and this list is downloadable across a variety of formats. The accessibility of this list, and the further clarity provided in the October guidance, should make it straightforward for the cryptocurrency industry to comply, and ensure their platforms and protocols are not interacting with virtual currency addresses on the SDN list. Further, as noted in the guidance, the industry should also conduct historical lookbacks of past transactional activity "after OFAC lists a virtual currency address on the SDN List to identify connections to the listed address."[9]

RESPONSE FROM MR. TIMOTHY MASSAD TO QUESTIONS FOR THE RECORD SUBMITTED BY CHAIRMAN BEYER

1. Given the increasing number of countries exploring digital currencies, including China, do you think that the Federal Reserve should be given explicit authority issue a digital dollar? If the Fed does not issue a digital dollar, are you concerned about the U.S. dollar losing its role as the world's reserve currency?

The critical issue is ramping up our research and development to determine exactly how we should design a U.S. CBDC and whether its net benefits make it worthwhile. The Fed will ultimately want explicit authority to issue a digital dollar. But I would be concerned that if we focus on that issue now, the process of building the consensus to grant that authority may raise all the issues of what would it look like, how would it work, is it worth it, would it disintermediate the banks, etc. I have no objection to granting the authority now if it can be done; I am simply suggesting that it is not the most urgent task, because we have not answered these other questions about CBDC design and benefits.

I don't think there is a near term risk of the dollar losing its role as the world's reserve currency but we cannot afford to be complacent either. The role of the dollar

---

[7] CFTC Commissioner Dan M. Berkovitz, *Keynote Address Before FIA and SIFMA-AMG, Asset Management Derivatives Forum*, COMMODITY FUTURES TRADING COMMISSION (Jun. 8, 2021), *https://www.cftc.gov/PressRoom/SpeechesTestimony/opaberkovitz7*.

[8] SEC Chair Gary Gensler, *Remarks before the Investor Advisory Committee*, SECURITIES AND EXCHANGE COMMISSION (Dec. 2, 2021), *https://www.sec.gov/news/statement/gensler-iac-statement-120221*.

[9] *Sanctions Compliance Guidance for the Virtual Currency Industry (Brochure)*, OFFICE OF FOREIGN ASSETS CONTROL, (Oct. 2021), *https://home.treasury.gov/system/files/126/virtual_currency_guidance_brochure.pdf*. (See, e.g.: "OFAC's inclusion of virtual currency addresses on the SDN List may assist the industry in identifying other virtual currency addresses that may be associated with blocked persons or otherwise pose sanctions risk, even if those other addresses are not explicitly listed on the SDN List. For example, unlisted virtual currency addresses that share a wallet with a listed virtual currency address may pose sanctions risk because the sharing of a wallet may indicate an association with a blocked person. Similarly, virtual currency companies may consider conducting a historic lookback of transactional activity after OFAC lists a virtual currency address on the SDN List to identify connections to the listed address.").

as the world's reserve currency is attributable to a number of factors, many of which are not directly tied to the technological form of money, such as the size and liquidity of the U.S. Treasury market (so that investors can obtain "safe" assets in times of stress), the stability of our government, the size and resilience of our economy, the strength of the rule of law, etc.

The dollar's prominence in international payment systems is sometimes thought of as part of its role as the world's reserve currency, but in many ways, it is distinguishable and more directly tied to the speed and efficiency of our payments system. That is why I think modernizing our payments system, and making sure it is interoperable with other countries' systems, is critical. A CBDC is potentially one way to do that; there may be other means as well. That is why we need to accelerate our research and design of CBDCs.

2. It is my understanding that thousands of transactions a day for millions of dollars are not recorded on the blockchain and are instead settled "off-chain." Are "off chain" digital asset transactions a problem and should regulators require that these transactions are reported to a central repository?

You are correct that there are a lot of transactions involving crypto-assets that are not recorded on any blockchain and are instead settled off-chain. The most common form of this is transactions made on a centralized exchange, which are recorded in the exchange's ledger. The exchange itself has a master account(s) on the blockchain which contains all of the particular crypto-asset that its customers own. But the absence of a regulatory framework for these exchanges means there is no assurance that the amount of say, bitcoin, held by the exchange on the blockchain is even equal to all of its customers holdings on the ledger. The general absence of transparency is a problem. I would focus first on creating an overall framework of regulation, particularly for crypto exchanges and other intermediaries, that requires reporting, disclosure and transparency similar to what we have in the derivatives and securities market. Exchanges should be required not only to keep a record of all bids, offers and transactions, but make that record available for appropriate regulatory and law enforcement purposes, and provide adequate pre and post-trade transparency to investors. I would do that first, and then consider whether we need a central repository.

3. The CFTC just fined Tether—the issuer of USDt—$41 Million for making false and misleading statements about its reserve holdings, after finding that USDt was only backed one for one with dollars just 27 percent of the time. Given that USD Tether is the most actively traded digital asset in the World, should the CFTC fine have been bigger to discourage similar activities by other fiat based stablecoin issuers in the future?

I cannot comment on how the CFTC determined the size of its fine, but I would say that I do not think the CFTC has sufficient authority to discourage similar activities by other stablecoin issuers. The CFTC's action was based on application of its anti-fraud authority under Section 6(c) of the Commodity Exchange Act. The CFTC does not have general power to regulate stablecoins or to set standards for stablecoin issuers. The best way to discourage bad actors is to create such a regulatory framework. CFTC Commissioner Dawn Stump expressed this very well in her concurring statement. She explained that while the action was an appropriate application of the anti-fraud provisions of Section 6(c) of the CEA, it was likely to cause confusion about the CFTC's role, since the agency does not regulate stablecoins. Specifically, she said the CFTC action may give investors a "false sense of comfort that we are overseeing those who issue and sell these coins such that they are protected from wrongdoing." See *https://www.cftc.gov/PressRoom/SpeechesTestimony/stumpstatement101521.*

We need to create a regulatory framework for stablecoin issuers that requires them to keep all reserves in cash (or, possibly, other highly liquid assets), guarantee redemption at par, and restrict their other activities, among other things, as I discussed in my testimony.

4. In 2018 senior SEC officials announced that Bitcoin and Ethereum, the two largest digital assets by market capitalization, would not be treated as securities. The CFTC has taken the position that both Bitcoin and Ethereum are commodities and permitted CFTC exchanges to offer futures and swaps contracts on both digital assets. However, the regulatory status of many other digital assets remains unclear. Should Congress mandate

that the SEC and CFTC work together to clarify the status of other major digital assets?

I believe the key problem is a lack of regulatory authority over the cash or spot market, not whether any particular token is a commodity or a security. The fact that Bitcoin and Ethereum are regarded as commodities gives the CFTC authority over derivatives pertaining to Bitcoin and Ethereum; it does not give the agency plenary authority to regulate Bitcoin and Ethereum, just as it does not have plenary authority to regulate any other commodity. Instead, it regulates derivatives based on commodities. Congress has given the CFTC limited power to prevent fraud and manipulation in the commodities markets themselves because of concern that fraud and manipulation would undermine the derivatives market, but that does not constitute general power to set standards for the trading of commodities.

Moreover, the derivatives the CFTC regulates includes derivatives on securities. Thus, while it would certainly be helpful for the SEC to clarify which crypto-assets it views as securities, there would still be a gap in regulation of those that are not securities. Congress should provide authority to the SEC or the CFTC to regulate the cash market for crypto-assets that are financial instruments. I would be happy to provide more information about that.

RESPONSE FROM MR. TIMOTHY MASSAD TO QUESTION FOR THE RECORD SUBMITTED BY SENATOR CASSIDY

"Discussions around cryptocurrency, especially at this hearing, focus on what the Federal Government's role in cryptocurrency regulation should be. While the Federal Government considers its approach, states are starting to take action. Some examples include Wyoming setting up regulations allowing for cryptobanks, while New York has introduced its BitLicense. From the different approaches taken by states toward digital currency, what lessons can the Federal Government take away?"

The Federal Government can certainly examine what the states are doing and learn from it, and I think there are areas where the states should retain their traditional primary jurisdiction, such as in uniform commercial code issues and how those might apply to digital currency, how State banking laws and regulations apply to digital assets, and so forth. But I think we need a Federal framework of regulation for digital assets that are financial instruments generally, just as we have in securities, derivatives, banking and other core financial markets. For example, although some might say that stablecoins are adequately regulated by State money transmitter laws or the specific digital laws of certain states, I think that we need a uniform national approach that protects against run-risk and other risks to financial stability, and ensures a basic level of investor protection. In addition, market development will be hampered if we have variations in approaches on those basic issues.

RESPONSE FROM MR. TIMOTHY MASSAD TO QUESTION FOR THE RECORD SUBMITTED BY SENATOR AMY KLOBUCHAR

A report by the President's Working Group on Financial Markets (PWG), the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency on cryptocurrency stated in part that stablecoins, which are cryptocurrencies pegged to a central currency like the dollar, have failed to maintain a stable value and could expose users to unexpected losses.

- **Can you explain why the recommendations made in the report are so important, and what if any changes you would make to the report's recommendations?**

The recommendations are important because of the risks that stablecoins pose today, as well as their potential for broader use. But I would make significant changes to those recommendations.

First, regarding the risks: stablecoins have grown enormously in value in a short time (from around $20 billion a year ago to over $130 billion today in market capitalization) because they facilitate trading of other crypto-assets. They have the potential for much broader use, as payment mechanisms generally. The risks they pose are described at length in the report. A primary one is run risk: similar to a

money market fund, a stablecoin issuer might not have sufficient liquid reserves to redeem tokens particularly if there were a spike in demand for redemption. This could trigger a run on that issuer or potentially other stablecoin issuers as well (as happened with money market funds in September 2008), and that could create stresses in interconnected markets or financial products. For example, sales of assets to meet redemption demands in a run could create downward pricing pressure on those asset markets. Inability to meet redemption demands could cause holders to default on obligations, and to the extent those holders have leveraged positions, that can increase the stress and damage. There are other risks as well related to the fact that stablecoins operate on decentralized blockchains that may have varying degrees of security, resilience etc.

But at the same time, stablecoins have the potential to improve the speed and efficiency of payments, outside of the crypto sector. They are effectively privately issued digital dollars. This could be a great benefit to individuals and businesses. Our payments system is based on bank deposits, and while it is reliable, safe and relatively efficient, it is actually slower and more expensive than the systems in many other developed countries, and probably much slower than what a digitized system could be.

That is why we need to create a sound regulatory framework. The report calls for legislation that would limit stablecoin issuers to insured depository institutions subject to appropriate supervision and regulation. It also calls for oversight of custodial wallet providers and for appropriate risk-management standards for other entities that perform activities critical to the functioning of the stablecoin arrangements. Finally, it calls for stablecoin issuers to comply with restrictions to limit affiliation with commercial entities and for standards to promote interoperability.

My primary disagreement is with the recommendation that we limit stablecoin issuers to IDIs. I believe we should develop a more tailored model of regulation for stablecoin issuers, with standards that are more specific to the risks posed and which would also facilitate more competition and innovation in the payments industry.

We should require that stablecoins are at all times fully backed by cash that is deposited with a bank, or in a master account with the Federal Reserve. This will eliminate the risk that exists today where stablecoin reserves may be invested in other assets that could lose value, or be difficult to liquidate, or whose sudden liquidation might drive asset prices down. Such a requirement would effectively prohibit maturity transformation by stablecoin issuers—the practice of taking demand deposits, which are short-term liabilities, and using them to fund longer-term loans or investments. We could also restrict the activities of a stablecoin issuer so that it does not engage in many of the activities that a traditional IDI might engage in. We should require some capital, even if the tokens are fully backed by cash, because there can be operational or other losses. This approach could be implemented through novel or special purpose charters.

The PWG report refers to the possibility of "access to appropriate components of the Federal safety net." While it is unclear whether or on what terms this might include deposit insurance, I am not persuaded that is necessary if the tokens are fully reserved with cash, the entity's activity is sufficiently isolated and other safeguards are in place. I believe it would be better to design a regulatory framework that does not include deposit insurance.

I am concerned that the recommendation to limit stablecoin issuers to IDIs under present supervisory standards would not sufficiently address the particular risks that stablecoins pose, and could result in limiting competition as a practical matter. Let me address the second point first.

Limiting stablecoin issuers to IDIs is likely to favor existing banks over new entrants because of the length of time it could take new entrants to get a charter and deposit insurance. (None have that today.) It could also mean that the largest banks are favored over all other banks because of capital advantages as well as technological advantages (they may be more able to create the platforms to issue and manage stablecoins, which settle instantly, as discussed below). The more tailored regulatory approach described above would allow new entrants, provided they can meet requirements of the type noted above, which would facilitate more competition in payments. (An existing bank holding company could still enter the stablecoin business by creating a ringfenced subsidiary that meets the requirements.)

As to the risks, simply saying an issuer should be an IDI does not ensure it has the technological platform to manage instantly settled stablecoins (most banks do

not). Moreover, it means the stablecoin activity would be co-mingled with all the other activities that many IDIs engage in, such as making loans and other investments. That makes it far more difficult to isolate the stablecoin activity.

Because this is a new activity, it would be much better to isolate it, and design regulations specific to the risk.

Some may object to allowing special purpose payment entities to have master accounts at the Federal Reserve, particularly if they are not FDIC-insured and do not have the same business models as traditional banks. But in fact, the Fed has already granted master accounts to uninsured entities whose business models are very different from traditional banks. Two derivatives clearinghouses have master accounts with over $100 billion on deposit on a combined basis, which monies represent customer funds. They are not regulated as banks nor insured by the FDIC. They are permitted to have master accounts because they were designated by the FSOC as systemically important financial market utilities under Article VIII of the Dodd Frank Wall Street Reform and Consumer Protection Act. They are subject to Federal Reserve oversight as a result of that designation.

I would be happy to elaborate on any of these issues.

RESPONSE FROM MR. KEVIN WERBACH TO QUESTIONS FOR THE RECORD SUBMITTED BY CHAIRMAN BEYER

1. Given the increasing number of countries exploring digital currencies, including China, do you think that the Federal Reserve should be given explicit authority issue a digital dollar? If the Fed does not issue a digital dollar, are you concerned about the U.S. dollar losing its role as the world's reserve currency?

Mr. Chairman, thank you for holding the hearing on Demystifying Crypto, and for your ongoing interest in the digital asset market. I am pleased to respond to your questions.

I believe the Federal Reserve should be given authority to issue a digital dollar. However, whether the Fed should actually do so, and what exactly a "digital dollar" would involve, are questions that require further study. The Fed should be given encouragement and a green light because the development of central bank digital currencies forces consideration of essential attributes of the next evolution of money and payments. Concerns such as interoperability, privacy, scalability, and financial stability, as well the transformative potential of programmable money, will not be adequately explored unless the Fed engages aggressively.

I am not worried about the U.S. dollar losing its reserve currency status to a CDBC in the near term. Given its tight capital controls and limitations on exchange rates, as well as the absence of central bank independence, China's effort to internationalize the RMB will run into limits regardless of how advanced its eCNY initiative is relative to the rest of the world. However, over time, there is no question that existing U.S. and global payments systems will need to evolve and be further digitized. They are too slow, too inefficient, too inflexible, and too reliant on established intermediary firms. If the U.S. fails to participate actively in the global effort to rethink money which cryptocurrencies and CBDCs have kicked off, in time the primacy of the dollar will be in jeopardy.

2. It is my understanding that thousands of transactions a day for millions of dollars are not recorded on the blockchain and are instead settled "off-chain". Are "off chain" digital asset transactions a problem and should regulators require that these transactions are reported to a central repository?

It is true that many digital asset transactions are not recorded on the blockchain. On-chain transactions can be costly, slow, and lacking in finality, especially on the most prominent blockchains such as Bitcoin and Ethereum. Custodial cryptocurrency exchanges, for example, typically net transactions among their customers in a manner similar to conventional stock exchanges. Payment intermediaries may similarly not record each transaction on-chain. Also, with layer–2 solutions such as the Bitcoin Lightning Network, transactions are conducted on temporary off-chain connections, with the net results recorded on the blockchain when the channel is closed. On the other hand, the rise of decentralized finance (DeFi) a financial services ecosystem operating completely in the form of on-chain smart contracts, could point the way toward more transactional activity on-chain.

Put simply, an off-chain transaction is not decentralized in the same manner as an on-chain one, and it should not be treated as such. Whether off-chain transactions are a problem depends on what concern is being raised, and on how the off-chain activity is happening. If, for example, an exchange handles transactions through its own records, that exchange can and should provide analogous reporting to conventional securities exchanges. The issues may be different if the question is tax avoidance, AML/CFT compliance, market surveillance for securities and commodities regulation, or something else. A universal rule that all transactions be reported to a central repository would far exceed how conventional financial services are treated, and would likely be inconsistent with the Fourth Amendment and American norms of financial privacy.

3. The CFTC just fined Tether—the issuer of USDt—$41 Million for making false and misleading statements about its reserve holdings, after finding that USDt was only backed one for one with dollars just 27 percent of the time. Given that USD Tether is the most actively traded digital asset in the World, should the CFTC fine have been bigger to discourage similar activities by other fiat based stablecoin issuers in the future?

There are grave concerns about Tether's role in the digital asset trading ecosystem. The proven accusations in the CFTC action and the New York Attorney General case alone would be sufficient to undermine trust in any normal financial instrument, and its backers. The opacity of Tether's reserves, regulatory status, and practices are deeply alarming for a coin whose entire purpose is to be a stable underpinning for the market. And there are even more serious allegations than those considered by the CFTC, such as evidence presented in peer-reviewed academic research suggesting that Tether was deliberately used to manipulate the Bitcoin market; questions about the veracity of Tether's current reserve disclosures; and purported transactions among Tether, related entities, and a small number of influential market actors. These allegations have not, to my mind, been convincingly disproven. The fact that Tether nominally does not operate in the U.S. seems inconsistent with the reality that USDT the dominant trading pair for most cryptocurrencies on most U.S.-based exchanges. Tether also provides large volumes of USDT for undisclosed collateral directly to U.S.-based market-makers and cryptocurrency lenders.

The CFTC, the Department of Justice, and other U.S. financial enforcement agencies should seriously investigate these claims, and the relationships among Tether, its related entities, and the large digital asset firms it appears to do significant transactions with. While I cannot prejudge what the evidence will show in such investigations, if even some of the more serious accusations are trust, a fine of any size is an insufficient penalty. Moreover, the penalties should not be limited to Tether alone if, in fact, its transaction partners knew and deliberately capitalized on fraudulent or otherwise illegitimate business arrangements. Finally, U.S. regulation of the stablecoin market should cover any stablecoin provided, held, or listed as a trading pair on U.S. based exchanges and other digital asset platforms, regardless of its nominal place of incorporation.

4. In 2018 senior SEC officials announced that Bitcoin and Ethereum, the two largest digital assets by market capitalization, would not be treated as securities. The CFTC has taken the position that both Bitcoin and Ethereum are commodities and permitted CFTC exchanges to offer futures and swaps contracts on both digital assets. However, the regulatory status of many other digital assets remains unclear. Should Congress mandate that the SEC and CFTC work together to clarify the status of other major digital assets?

Congress should seek to ascertain whether the gaps between the SEC and CFTC on cryptocurrency regulation are an artifact of coordination failures under the prior Administration; an enduring turf battle; or a reflection of flaws in our regulatory structure. For example, the limits on the CFTC's authority to regulate spot markets in commodities mean that only digital assets classified as securities are subject to the full range of market integrity and other oversight. Telling the agencies to coordinate will not address this legal gap; only Congress can.

In my estimation, while coordination between the SEC and CFTC would be valuable, it is not the central problem today. An asset can be both a security (or more precisely, the consideration for an investment contract) and a commodity, depending on the circumstances. Both agencies could provide significantly greater clarity in how they apply the relevant classifications in the digital asset context. It is distressing that the definitive SEC statement on Ethereum is a 2018 speech by a staff

member, which did not even explicitly the status of the original Ether crowdsale. (In some ways, Ether is the most important digital asset because of its foundational role for decentralized applications, and because other tokens are generally issued in a manner much closer to Ether than bitcoin.) I personal find the "sufficiently decentralized" concept articulated by Director Hinman in that speech quite promising. However, it has not been taken up by the Commission in any meaningful way.

RESPONSE FROM MR. KEVIN WERBACH TO QUESTION FOR THE RECORD SUBMITTED BY SENATOR CASSIDY

"Discussions around cryptocurrency, especially at this hearing, focus on what the Federal Government's role in cryptocurrency regulation should be. While the Federal Government considers its approach, states are starting to take action. Some examples include Wyoming setting up regulations allowing for cryptobanks, while New York has introduced its BitLicense. From the different approaches taken by states toward digital currency, what lessons can the Federal Government take away?"

Thank you, Senator, for your interest in this topic.

The financial services sector is an area of shared responsibility between states and the Federal Government. Corporate and commercial law requirements are determined primarily at the state level, and states play a major role in regulation of money transmitters, banks, and trust companies. State attorneys general also play an essential part in enforcement actions. The challenge is to balance the experimentation that multiple state regimes allow with the need for consistency and minimum standards for activities that are not just national but, in some senses, global in scope.

New York is to be commended for moving early to develop a regulatory regime for digital assets, with the adoption of the BitLicense in 2015. Unfortunately, the BitLicense was written and interpreted in such a way that, for some time, it was too difficult for firms to meet the licensure requirements. Many firms left the State because they found the BitLicense too onerous. The New York Department of Financial Services has in recent years taken a somewhat more flexible approach. The BitLicense also may have been too early. The digital asset market at the time had not yet developed the level of sophistication and integration with traditional finance that it now enjoys. A safe harbor mechanism, a longer compliance window, or a carve-out for smaller entities, might have made the BitLicense more viable.

Wyoming and several other states have more recently adopted a variety of laws to create a viable environment for digital asset activity. The Wyoming Special Purpose Depository Institution framework, in particular, offers a pathway forward for the provision of narrow banking services to cryptocurrency firms that seeks to address the major risk areas regulators and banks have expressed. Without taking a position on any of the specific provisions of these state laws, the question is whether having varied state regimes for crypto-native banks represents the best solution, or is necessary only because Federal entities such the FDIC, Fed, and OCC have made it artificially difficult for conventional banks to participate in these markets. There is also the question of how State rules interact with the Federal system, such as whether state-chartered institutions can access Federal Reserve master accounts.

Important lessons from the history state activity in this area include the following. First, bespoke regimes may be necessary to tailor rules to the distinctive aspects of digital asset markets. Second, there are many different issues under the umbrella of cryptocurrency regulation, which will not all have the same solutions. Third, policymakers should clearly identify the problems they are trying to address, and how the specified requirements address them. Fourth, as noted earlier, rules should reflect the maturity of the industry and the nature of the entities subject to their requirements.

RESPONSE FROM MR. PETER VAN VALKENBURGH [1] TO QUESTIONS FOR THE RECORD SUBMITTED BY CHAIRMAN BEYER

1. Given the increasing number of countries exploring digital currencies, including China, do you think that the Federal Reserve should be given explicit authority to issue a digital dollar? If the Fed does not issue a digital dollar, are you concerned about the U.S. dollar losing its role as the world's reserve currency?

That other countries are exploring central bank digital currencies is not a sufficient reason for the Federal Reserve to be given authority to issue one. Historically most money has been issued by private entities rather than by the Federal Reserve itself, and the mere fact that money can be digital is not reason to change this policy.[2] If the Fed does not issue a digital dollar there's no greater or lesser chance that the dollar will lose its role as the world's reserve currency. Currencies are strong when they are backed by nations that have strong rule of law, stable and accountable institutions, and transparent monetary policies.[3] On these margins America is well ahead of, for example, China, whose recent announcement of a digital yuan has driven headlines. Indeed, China's motivations for issuing a digital yuan are likely based on the need to retain power over its population through surveillance and central control;[4] it may serve only to weaken protections for human rights and the certainty of business relationships in China thereby undermining rather than strengthening the yuan.

2. It is my understanding that thousands of transactions a day for millions of dollars are not recorded on the blockchain and are instead settled "off-chain". Are "off chain" digital asset transactions a problem and should regulators require that these transactions are reported to a central repository?

Off-chain transactions are no different from internal transactions between customers within a major bank or a payment intermediary such as PayPal or Venmo. Neither leave any record outside of the internal records of the institution, and both are potentially subject to existing recordkeeping and reporting rules here in the U.S. A transaction between two users of a money transmitter like PayPal is subject to the same state money transmission licensing rules and requirements and Federal anti-money laundering reporting requirements as transactions between two users of a cryptocurrency exchange.

3. The CFTC just fined Tether—the issuer of USDt—$41 Million for making false and misleading statements about its reserve holdings, after finding that USDt was only backed one for one with dollars just 27 percent of the time. Given that USD Tether is the most actively traded digital asset in the World, should the CFTC fine have been bigger to discourage similar activities by other fiat based stablecoin issuers in the future?

I do not have an opinion regarding the size of the fine. Any issuer or redeemer of a backed stablecoin to American users is engaging in a regulated activity. Depending on the specific circumstances, the stablecoin may be a security (requiring registration with the SEC),[5] a commodities derivative (subject to CFTC oversight),[6] or money transmission and/or deposit-taking activities triggering state and/or fed-

---

[1] Peter is Director of Research at Coin Center, the leading independent non-profit research and advocacy group focused on the public policy issues facing cryptocurrency technologies such as Bitcoin. *http://coincenter.org*.

[2] Randal K. Quarles, "Parachute Pants and Central Bank Money," *Speech before the 113th Annual Utah Bankers Association Convention*, Sun Valley, Idaho, June 28, 2021, *https://www.federalreserve.gov/newsevents/speech/quarles20210628a.htm*.

[3] Henry M. Paulson Jr., "The Future of the Dollar," *Foreign Affairs*, May 19, 2020, *https://www.foreignaffairs.com/articles/2020-05-19/future-dollar*; Jerry Brito, "China's digital yuan is not a threat to the dollar," blog, January 13, 2020, *https://blog.jerrybrito.com/2020/01/13/chinas-digital-yuan-is-not-a-threat-to-the-dollar/*.

[4] Samantha Hoffman et al., "The flipside of China's central bank digital currency," *Australian Strategic Policy Institute*, Policy Brief No. 40, 2020, *https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2020-10/Digitalcurrency_1.pdf*.

[5] "Stablecoin Regulation," *Coin Center Tangents Podcast*, October 15, 2021, *https://www.youtube.com/watch?v=5wJtM52G9_w*.

[6] "CFTC Orders Tether and Bitfinex to Pay Fines Totaling $42.5 Million," *Commodity Futures Trading Commission*, Press Release Number 8450–21, October 15, 2021, *https://www.cftc.gov/PressRoom/PressReleases/8450-21*.

eral licensing and/or bank chartering obligations.[7] There is also no reason that the issuer could not be subject to multiple overlapping rules from any of these regulatory structures. All in all, the CFTC fine is certainly not likely to be the last or largest penalty for non-compliant issuers, and there will likely be more significant deterrent effects from the collection of enforcement actions taken as a whole.

4. In 2018 senior SEC officials announced that Bitcoin and Ethereum, the two largest digital assets by market capitalization, would not be treated as securities. The CFTC has taken the position that both Bitcoin and Ethereum are commodities and permitted CFTC exchanges to offer futures and swaps contracts on both digital assets. However, the regulatory status of many other digital assets remains unclear. Should Congress mandate that the SEC and CFTC work together to clarify the status of other major digital assets?

Ultimately the question of whether an asset is a security is one for the courts, which almost 70 years ago saw fit to create a flexible test for investment contracts.[8] I believe that judge-made test remains a good fit even when these assets are digital.[9] That said, judge-made tests take time to apply to new facts as cases only gradually make their way to the courts and eventually into clarifying precedent from new judicial holdings building on old.

The best way to reduce uncertainty in this realm would be either (1) to press the SEC to take more cases to court, rather than settling them (which does not leave a precedential record in the form of new judge-made law), (2) to offer a safe harbor from arbitrary enforcement actions for token issuers who register and perform sensible disclosures,[10] or else (3) to overrule the courts and replace the flexible definition of securities with something more rigid in legislation.[11] Mandating that the SEC and CFTC work together will not inject any certainty into this arena because it would merely empower the two agencies to make policy arbitrarily, without guidance from congress, without judicial oversight, without binding precedent, and with all of the inconsistencies and transience inherent in periodic political upheavals within the executive branch.

RESPONSE FROM MR. PETER VAN VALKENBURGH TO QUESTION FOR THE RECORD SUBMITTED BY SENATOR CASSIDY

"Discussions around cryptocurrency, especially at this hearing, focus on what the Federal Government's role in cryptocurrency regulation should be. While the Federal Government considers its approach, states are starting to take action. Some examples include Wyoming setting up regulations allowing for cryptobanks, while New York has introduced its BitLicense. From the different approaches taken by states toward digital currency, what lessons can the Federal Government take away?"

The greatest lesson that the Federal Government can take from the states is that we don't need new regulatory systems or even new rules to effectively regulate activities performed using these technologies. If a company is performing money-transmission-like services using bitcoins rather than dollars, there's no reason to regulate that entity any differently than a traditional money transmitter. When states have attempted to create cryptocurrency-specific regulatory structures the result has been both (a) disruptive and (b) ultimately not particularly dissimilar from the existing regulatory systems in place for equivalent activities performed using non cryptocurrency assets. It ends up being much ado about nothing.

---

[7] *See e.g.* "NYDFS Grants First Charter to a New York Virtual Currency Company," *New York Department of Financial Services*, Press Release, May 7, 2015, *https://www.dfs.ny.gov/reports_and_publications/press_releases/pr1505071.*

[8] *SEC v. Howey Co.*, 328 U.S. 293 (1946), *https://supreme.justia.com/cases/federal/us/328/293/.*

[9] Peter Van Valkenburgh, "Framework for Securities Regulation of Cryptocurrencies," *Coin Center*, August 2018, *https://www.coincenter.org/framework-for-securities-regulation-of-cryptocurrencies/.*

[10] *See e.g.* "Clarity for Digital Tokens Act of 2021," H.R. 5496, 117th Congress (2021–2022), *https://www.congress.gov/bill/117th-congress/house-bill/5496/text*; Hester Peirce, "Token Safe Harbor Proposal 2.0," U.S. Securities and Exchange Commission, April 13, 2021, *https://github.com/CommissionerPeirce/SafeHarbor2.0.*

[11] *See e.g.* "Securities Clarity Act," H.R. 8378, 116th Congress (2019–2020), *https://www.congress.gov/bill/116th-congress/house-bill/8378*; "Securities Clarity Act," H.R. 4451, 117th Congress (2020–2021), *https://www.congress.gov/bill/117th-congress/house-bill/4451.*

Take, for example, the New York BitLicense. The New York Department of Financial Services went through an exhaustive process of creating a new license type soliciting multiple rounds of comments and several drafts of new regulations.[12] Ultimately, however, ambiguous terms and uncertain language in those rules made New York a less welcoming environment for new cryptocurrency businesses.[13] Meanwhile, the nature of the license was, nonetheless, not much different from a typical money transmission license as far as protections afforded the customers of licensees. More recently, the DFS has been chartering trust companies to deal in cryptocurrencies just as they would charter any trust company irrespective of the assets in which they deal.[14] This technology-neutral approach has, it seems, borne more fruit from an innovation and investor protection standpoint than the de novo BitLicense approach.

○

[12] "Regulation and History," New York Department of Financial Services, accessed December 3, 2021, *https://www.dfs.ny.gov/apps_and_licensing/virtual_currency_businesses/regulation_history*; Peter Van Valkenburgh and Jerry Brito, "New York BitLicense Comment," *Coin Center*, October 14, 2014, *https://www.coincenter.org/new-york-bitlicense-comment/*; Peter Van Valkenburgh and Jerry Brito, "Comments to the New York Department of Financial Services on the Revised Virtual Currency Regulatory Framework," Coin Center, March 27, 2015, *https://www.coincenter.org/app/uploads/2020/05/Coin-Center-BitLicense-Comment-March-2015.pdf*.

[13] Peter Van Valkenburgh, "Our thoughts on the BitLicense: California is Winning," *Coin Center*, June 3, 2015, *https://www.coincenter.org/our-thoughts-on-the-bitlicense-california-is-winning/*.

[14] *See e.g.* "NYDFS GRANTS FIRST CHARTER TO A NEW YORK VIRTUAL CURRENCY COMPANY," *New York Department of Financial Services*, Press Release, May 7, 2015, *https://www.dfs.ny.gov/reports_and_publications/press_releases/pr1505071*.