THE FUTURE OF DIGITAL ASSET REGULATION

HEARING

BEFORE THE

SUBCOMMITTEE ON COMMODITY EXCHANGES, ENERGY, AND CREDIT

OF THE

COMMITTEE ON AGRICULTURE
HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTEENTH CONGRESS

SECOND SESSION

JUNE 23, 2022

Serial No. 117–36

Printed for the use of the Committee on Agriculture
agriculture.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE
49–769 PDF WASHINGTON : 2022

COMMITTEE ON AGRICULTURE

DAVID SCOTT, Georgia, *Chairman*

JIM COSTA, California
JAMES P. MCGOVERN, Massachusetts
ALMA S. ADAMS, North Carolina, *Vice Chair*
ABIGAIL DAVIS SPANBERGER, Virginia
JAHANA HAYES, Connecticut
SHONTEL M. BROWN, Ohio
BOBBY L. RUSH, Illinois
CHELLIE PINGREE, Maine
GREGORIO KILILI CAMACHO SABLAN, Northern Mariana Islands
ANN M. KUSTER, New Hampshire
CHERI BUSTOS, Illinois
SEAN PATRICK MALONEY, New York
STACEY E. PLASKETT, Virgin Islands
TOM O'HALLERAN, Arizona
SALUD O. CARBAJAL, California
RO KHANNA, California
AL LAWSON, JR., Florida
J. LUIS CORREA, California
ANGIE CRAIG, Minnesota
JOSH HARDER, California
CYNTHIA AXNE, Iowa
KIM SCHRIER, Washington
JIMMY PANETTA, California
SANFORD D. BISHOP, JR., Georgia
MARCY KAPTUR, Ohio
SHARICE DAVIDS, Kansas

GLENN THOMPSON, Pennsylvania, *Ranking Minority Member*
AUSTIN SCOTT, Georgia
ERIC A. "RICK" CRAWFORD, Arkansas
SCOTT DESJARLAIS, Tennessee
VICKY HARTZLER, Missouri
DOUG LAMALFA, California
RODNEY DAVIS, Illinois
RICK W. ALLEN, Georgia
DAVID ROUZER, North Carolina
TRENT KELLY, Mississippi
DON BACON, Nebraska
DUSTY JOHNSON, South Dakota
JAMES R. BAIRD, Indiana
CHRIS JACOBS, New York
TROY BALDERSON, Ohio
MICHAEL CLOUD, Texas
TRACEY MANN, Kansas
RANDY FEENSTRA, Iowa
MARY E. MILLER, Illinois
BARRY MOORE, Alabama
KAT CAMMACK, Florida
MICHELLE FISCHBACH, Minnesota
MAYRA FLORES, Texas

ANNE SIMMONS, *Staff Director*
PARISH BRADEN, *Minority Staff Director*

SUBCOMMITTEE ON COMMODITY EXCHANGES, ENERGY, AND CREDIT

SEAN PATRICK MALONEY, New York, *Chairman*

STACEY E. PLASKETT, Virgin Islands
RO KHANNA, California
CYNTHIA AXNE, Iowa
BOBBY L. RUSH, Illinois
ANGIE CRAIG, Minnesota
ANN M. KUSTER, New Hampshire
CHERI BUSTOS, Illinois

MICHELLE FISCHBACH, Minnesota, *Ranking Minority Member*
AUSTIN SCOTT, Georgia
DOUG LAMALFA, California
RODNEY DAVIS, Illinois
CHRIS JACOBS, New York
TROY BALDERSON, Ohio
MICHAEL CLOUD, Texas
RANDY FEENSTRA, Iowa
KAT CAMMACK, Florida

EMILY GERMAN, *Subcommittee Staff Director*

CONTENTS

THE FUTURE OF DIGITAL ASSET REGULATION

THURSDAY, JUNE 23, 2022

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON COMMODITY EXCHANGES, ENERGY, AND CREDIT,
COMMITTEE ON AGRICULTURE,
Washington, D.C.

The Subcommittee met, pursuant to call, at 10:31 a.m., in Room 1300 of the Longworth House Office Building, Hon. Sean Patrick Maloney [Chairman of the Subcommittee] presiding.

Members present: Representatives Maloney, Plaskett, Khanna, Axne, Rush, Craig, Kuster, Fischbach, Austin Scott of Georgia, Balderson, Cloud, Feenstra, Cammack, Thompson (*ex officio*), Baird, and Mann.

Staff present: Lyron Blum-Evitts, Carlton Bridgeforth, Emily German, Josh Lobert, Brian Robinson, Paul Balzano, Caleb Crosswhite, Kevin Webb, John Konya, and Dana Sandman.

OPENING STATEMENT OF HON. SEAN PATRICK MALONEY, A REPRESENTATIVE IN CONGRESS FROM NEW YORK

The CHAIRMAN. Good morning, everyone. This hearing of the Subcommittee on Commodity Exchanges, Energy, and Credit entitled, *The Future of Digital Asset Regulation,* will come to order.

Welcome, and thank you for joining us at today's hearing. After brief opening remarks, Members will receive testimony from our witnesses today, and then the hearing will be open to questions. In consultation with the Ranking Member and pursuant to Rule XI(e), I want to make Members of the Subcommittee aware that other Members of the full Committee may join us today.

Again, thank you all for joining me. I would like to thank our erstwhile colleague, Antonio Delgado, for chairing this Subcommittee, and for his service to the country and to New York. I am delighted to be stepping into this role, even if briefly. Thank you all for joining me today in that first hearing as Chairman of the Commodity Exchanges, Energy, and Credit Subcommittee, and welcome to the hearing we are calling, *The Future of Digital Asset Regulation.*

Today's hearing is a good opportunity to engage market experts at the CFTC, digital asset stakeholders, and academics in a discussion on the effectiveness of current regulation of a continuously evolving digital assets market, and how to address regulatory concerns in any future framework.

Since the launch of Bitcoin in 2009 and the creation of the Ethereum blockchain in 2013, there has been, to put it mildly, rapid and expansive growth and innovation in both the diversity and volume of digital asset products available.

A digital asset can be a virtual currency, an investment opportunity, or traded on an exchange, and the novel nature of these assets, the complexity of them, and how investors and consumers use them should say a lot and will say a lot about how they should be regulated.

As the Committee of jurisdiction over the CFTC, of primary importance to today's hearing is digital commodity products available for trade in the derivatives and underlying spot markets, a primary access point for investors to the digital asset market. Digital assets are popular, very popular, but volatile, very volatile. We see this reflected in the substantial decrease in combined digital asset market capitalization from its peak of approximately $3 trillion in November of last year, to its current level of approximately $1 trillion: $3 trillion in November, $1 trillion today.

Polling also reveals that approximately 20 percent of American adults have invested in, traded, or used cryptocurrencies. Providing Congressional direction to establish the rules of the road to ensure American retail investors are informed and protected is as important as ever.

While the CFTC has dutifully exercised its role as a regulator and enforcement authority in digital asset markets, its authority is not unlimited. Indeed, its authority is specifically limited. When you couple the recent volatility with high retail participation in digital asset spot markets, it is concerning that there is a gap in oversight and regulation of these markets, and it is that gap that we are particularly focused on.

The growth of the digital asset industry has centered on innovation, transparency, and security, and I believe in fostering that innovation here in the United States. In contrast to a traditional bank or financial institution, the most popular cryptocurrencies, Bitcoin and Ether, have entirely public ledgers. Anyone can view them and participate in recording and authenticating transactions on them.

As we will hear from our witnesses today, the digital asset economy presents opportunities to support financial inclusion, but without strong customer protections, education, and regulatory certainty, participants in the industry may be at increased risk of financial loss and exposure to fraud.

Digital assets are complicated, and retail participants may be tempted by the promise of quick returns without knowing how the digital asset functions, or without knowing who received early access to information. Regulation regarding disclosure to market participants may help retail investors understand the volatility of the assets and facilitate smart digital entrepreneurship, but how we do that matters, and it may require new ways of thinking.

Today's hearing will help this Committee understand how Congressional action, if done right, can give the CFTC the tools it needs to protect investors while fostering innovation here in the U.S. I am especially focused on whether such action could be done in a fully bipartisan manner.

Thank you again to the Members and witnesses joining us today as well as those who are following along online. I look forward to a productive conversation about the future of digital asset regulation.

[The prepared statement of Mr. Maloney follows:]

PREPARED STATEMENT OF HON. SEAN PATRICK MALONEY, A REPRESENTATIVE IN CONGRESS FROM NEW YORK

Again—Thank you all for joining me today in my inaugural hearing as Chairman of the Commodity Exchanges, Energy, and Credit Subcommittee, and welcome to today's hearing, *The Future of Digital Asset Regulation.*

Today's hearing is an excellent and timely opportunity to engage market experts at the CFTC, digital asset stakeholders, and academics in discussion on the effectiveness of current regulation of a continuously evolving digital asset markets and how to address regulatory concerns in any future regulatory framework.

Since the launch of Bitcoin in 2009 and the creation of the Ethereum blockchain in 2013, there has been rapid and expansive growth and innovation in both the diversity and volume of digital asset products available.

A digital asset can be a virtual currency, an investment opportunity, or traded on an exchange—and how investors and consumers use these products will say a lot about how they should be regulated.

As the Committee of jurisdiction over the CFTC, of primary importance to today's hearing is digital commodity products available for trade in the derivatives and underlying spot markets—a primary access point for investors to the digital asset market.

Digital assets are popular, but volatile. We see this reflected in the substantial decrease in combined digital asset market capitalization from its peak of approximately $3 trillion in November 2021, to current levels of approximately $1 trillion.

Polling also reveals that approximately 20% of American adults have invested in, traded, or used cryptocurrencies.

Providing Congressional direction to establish the rules of the road to ensure American retail investors are informed and protected is as important as ever.

While the CFTC has dutifully exercised its role as a regulator and enforcement authority in digital asset markets, its authority is limited. When you couple the recent volatility with high retail participation in digital asset spot markets, it is concerning that there is a gap in oversight and regulation of these markets.

The growth of the digital asset industry has centered on innovation, transparency, and security—and I believe in fostering that innovation here in the United States. In contrast to a traditional bank or financial institution, the most popular cryptocurrencies, Bitcoin and Ether, have entirely public ledgers. Anyone can view them and participate in recording and authenticating transactions on them.

As we will hear from our witnesses today, the digital asset economy presents opportunities to support financial inclusion, but, without strong customer protections and regulatory certainty, participants in the industry may be at increased risk of financial loss and exposure to fraud.

Digital assets are complicated, and retail participants may be tempted by the promise of quick returns without knowing how the digital asset functions, or without knowing who received early access to information.

Regulation regarding disclosure to market participants may help retail investors understand the volatility of the assets and facilitate smart digital entrepreneurship.

Today's hearing will help this Committee understand how Congressional action can give the CFTC the tools they need to protect investors while fostering innovation here in the United States.

Thank you again to the Members and witnesses joining us today as well as those who are following along online. I look forward to a productive conversation about the future of digital asset regulation.

With that, I'd now like to welcome the distinguished Ranking Member, Mrs. Fischbach from Minnesota, for any opening remarks she would like to give.

The CHAIRMAN. With that, I am pleased to welcome the distinguished Ranking Member, Mrs. Fischbach from Minnesota, for any opening remarks she would like to give.

OPENING STATEMENT OF HON. MICHELLE FISCHBACH, A REPRESENTATIVE IN CONGRESS FROM MINNESOTA

Mrs. FISCHBACH. Well, thank you, Mr. Chairman, and first of all, congratulations, and I am looking forward to working with you. But more immediately, thank you very much for holding this important hearing. I appreciate your comments on bipartisan work, so thank you so much for that.

And there is no better time than the present to discuss how and why we regulate financial markets and consider how to best balance the need to protect customers with the desire to protect innovation. According to a recent survey, roughly half of American adults today own or have owned some sort of cryptocurrency. This brings digital assets on par with the number of Americans that own traditional securities. Of those Americans who own cryptocurrency, more than 74 percent bought them for the first time within the last 2 years.

Since the creation of Bitcoin, thousands of cryptocurrency projects have been developed. Today, there are nearly 20,000 cryptocurrencies in existence spread across numerous blockchain platforms. Unfortunately, these tokens do not always fall neatly into our current financial regulatory framework. Traditionally, we protect investors through disclosure requirements and the segregation of their assets, and we promote market integrity through regulatory oversight and intermediaries and enforcement actions. But what rules apply depend on the nature of the asset and the specific types of risk market participants face.

Regulations have struggled to provide guidance to market participants on how and when their activities require registration and compliance. Market participants still do not know what rules apply and when. Real risk to market participants exist and we have an obligation to address them.

Over the past several years, Members of this Committee have proposed legislation that would lay down clear parameters for the roles of both the SEC and the CFTC in digital asset markets. In April Republican leader Thompson and Congressman Khanna introduced the bipartisan Digital Commodity Exchange Act of 2022 (H.R. 7614). The DCEA would give the CFTC—lots of initials today—expanded oversight of the trading of those digital assets which are commodities, and it would bring certainty to market participants by doing what the regulators cannot—providing legal clarity to market intermediaries and participants.

I appreciate the efforts of the CFTC and the SEC that they have made to try to fold digital assets into existing framework, but in some cases, particularly for spot digital commodity transactions, the existing laws simply lack the authorities necessary.

As the popularity of digital assets continues to grow, it is incumbent upon Congress to speak clearly about how best to regulate. I am glad we have the opportunity to explore these issues and the way Congress can better create an environment where digital assets can become not only a valuable financial product, but an important conduit of innovation in our financial system.

Thank you to each of our witnesses for their willingness to share their expertise with us, and I am looking forward to hearing your perspectives on how and why we regulate in financial markets, and

where and when we might apply those lessons to the crypto markets and to the market participants.

Thank you, Mr. Chairman, and I yield back.

The CHAIRMAN. I thank the Ranking Member, and also would like to take this opportunity to recognize the leadership of Chairman David Scott on these issues. I don't see him present today, but we will be happy to yield to him for any opening remarks should he join us. I do note the presence of the Ranking Member of the full Committee, Mr. Thompson, and I would invite him to share any opening comments he may wish to make.

OPENING STATEMENT OF HON. GLENN THOMPSON, A REPRESENTATIVE IN CONGRESS FROM PENNSYLVANIA

Mr. THOMPSON. Well, thank you, Mr. Chairman. Let me start by echoing the remarks of our Subcommittee Ranking Member, and congratulate you in your new role with leading the Subcommittee.

I look forward to working with you, and I know that digital assets have been an area of interest for you for several years now.

As you know, the House Agriculture Committee has a long history of fostering technology and innovation. Leading on digital assets is no exception. Given the Commodity Futures Trading Commission's role in regulated markets, the Agriculture Committee has an opportunity and responsibility to be at the table for these discussions. I appreciate you holding this hearing, and your commitment to continuing the Committee's education and examination of digital asset regulations and markets.

As some may recall, this Committee held one of the first Congressional hearings to examine digital assets in 2018, which led to subsequent roundtables and conversations focused on how to regulate these novel assets. While these events provided ample education on blockchain and cryptocurrency, we still find ourselves debating foundational questions about how to integrate these markets into our financial system.

Over the past month, the carnage in digital assets has filled our newsfeeds. Prices have fallen dramatically, projects have imploded, customer funds have been lost or frozen, and billions of dollars in value have been lost. For those who have lost significant sums of money, this sell-off has been a catastrophe. And yet, the promise of cryptocurrency remains. Despite losses, the public's interest in this technology has not diminished. Developers and investors continue to build new projects and refine the technology, and this is why this hearing on the regulation of digital assets is so timely.

Clearly defined guardrails can provide more certainty to developers, investors, and the public. To provide these guardrails, I introduced H.R. 7614, the Digital Commodity Exchange Act, with Congressman Khanna. The DCEA offers a framework to bring regulatory clarity to digital asset markets. This legislation protects market participants and builds on the successful system of principles-based regulation already in place at the CFTC. It establishes clear jurisdictional lines between financial regulators, helping to reduce regulatory complexity, and clarify existing regulatory roles. And perhaps, most importantly, it provides a clear pathway to compliance for those hoping to build the next great innovation with digital assets.

The DCEA will provide regulators with tools to hold bad actors accountable and help to protect market participants from fraud and market manipulation. Clearly defined core principles will also help establish a better understood and flexible framework to support the creation of new products and meet evolving market demands.

We don't yet know all the ways digital assets will be used, but that should excite us, not intimidate us. America has always been a leader in technological innovation and the spirit of entrepreneurship, and we should continue to embrace that spirit. Our Committee must continue to put forward innovative ideas and sound proposals in these novel policy areas facing Congress. I hope we can implement smart bipartisan solutions like the Digital Commodity Exchange Act together.

Again, thank you to our panelists for being here today, and thank you for taking the time to come and educate us. I look forward to today's discussion.

With that, Mr. Chairman, I yield back.

The CHAIRMAN. I thank the gentleman.

The chair would request that other Members submit their opening statements for the record so that we may proceed directly to witness testimony.

[The prepared statement of Ms. Kuster follows:]

PREPARED STATEMENT OF HON. ANN M. KUSTER, A REPRESENTATIVE IN CONGRESS FROM NEW HAMPSHIRE

Thank you, Mr. Chairman. And thanks to our panel for being with us.

We are in the midst of a brave new world of digital asset trading. Our Committee has given this issue worthwhile attention this Congress because of the role the Commodity Futures Trading Commission (CFTC) has and will continue to play in regulating this trade.

As more and more Americans invest in these assets, it is imperative for Congress to keep up as we regulate and oversee the digital realm just as we do the more established marketplaces.

As we all have seen recently, Bitcoin—the most popular cryptocurrency—has badly tumbled in the last few weeks and lost more than ½ its value in 2022 so far.

Clearly no marketplace is immune from severe vulnerability and uncertainty, be it Bitcoin or Wall Street. But we do need to assure digital markets are operating above-board and secure, and that investors have access to the information they need to fully understand the risks they are taking.

With that in mind, I'd like to focus my questions on consumer protection as it relates to digital assets.

The CHAIRMAN. Welcome, all of you. Our first witness today is Mr. Vincent McGonagle, the Director of the Division of Market Oversight at the Commodity Futures Trading Commission. Our second witness today is Dr. Christopher Brummer, Professor of Law at the Georgetown University Law Center. Our third witness is Mr. Jonathan Levin, the Co-Founder and Chief Strategy Officer of Chainalysis—am I saying that correctly? Okay, good. Let's get that right. Our fourth and—I mean, it is my first hearing. I don't want to screw it up.

Mrs. FISCHBACH. You are doing a great job.

The CHAIRMAN. Is it going all right? Okay, good. A lot of pressure up here. I have only been doing this for 10 years. I'm starting to get the swing of it.

Our fourth and final witness is Mr. Charles Hoskinson, the Chief Executive Officer and Founder of Input Output Global.

Thank you all for joining us today. We will now proceed to hearing your testimony. You will have 5 minutes. The timer should be visible to you all, so it will count down to zero, at which point there is no time left.

Mr. McGonagle, please begin when you are ready. Thank you, sir.

STATEMENT OF VINCENT "VINCE" MCGONAGLE, J.D., DIRECTOR, DIVISION OF MARKET OVERSIGHT, COMMODITY FUTURES TRADING COMMISSION, WASHINGTON, D.C.

Mr. MCGONAGLE. Thank you. Good morning, Chairman Maloney, Ranking Member Fischbach, Ranking Member Thompson, and Members of the Subcommittee. Thank you for the opportunity to appear before you today.

My views are mine alone, and do not reflect those of the Division of Market Oversight or the Commission.

The CFTC is the primary regulator of the futures and options markets, and since 2010, the swaps market as well. The agency's mission is to promote the integrity, resilience, and vibrancy of the U.S. derivatives markets through sound regulation. We do that through a regulatory framework that seeks to ensure market integrity and the protection of customer funds, avoid systemic risk, and police derivatives markets for abuses, while fostering innovation and fair competition.

A trading facility for market participants, including retail customers, interested in listing and trading futures must apply to the Commission to be designated as a contract market. That market must then comply with 23 statutory core principles. Those core principles require the market to ensure the protection of customer funds, protect market participants and the market from abusive practices, and promote fair and equitable trading in the contract market. The contract market must be able to detect and prevent manipulation, price distortion, and disruption of the contracts' cash settlement or delivery processes.

To comply with the system safeguards core principle, the market must establish and maintain a program to identify and minimize sources of operational risk, including cybersecurity and disaster recovery.

Designated contract markets are also self-regulatory organizations. That is, they must establish and maintain effective oversight programs, including monitoring and enforcing compliance with their rules. A market must submit to the Commission all new product terms and conditions, which must meet certain core principles, including the core principal that the designated contract market only lists contracts that are not readily susceptible to manipulation.

To ensure compliance with the core principles, CFTC staff conduct rule enforcement reviews and system safeguards examinations, and at any time, Commission staff may ask a designated contract market for a detailed justification of its continued compliance with core principles. And the CFTC also conducts direct surveillance on trading on those markets.

Digital assets are commodities, and the CFTC has broad regulatory oversight over any derivatives products listed by designated

contract markets. In December 2017, three designated contract markets self-certified that they would list Bitcoin derivatives contracts for trading. Today, five contract markets list for trading futures and options contracts on Bitcoin, Ether, or both of those products.

The CFTC does not have regulatory authority over cash markets. We do have anti-fraud, false reporting, and anti-manipulation enforcement authority over commodity cash markets and interstate commerce. Since 2014, the CFTC has brought more than 50 enforcement actions involving digital assets. We filed numerous cases charging retail fraud, as well as charging platforms with illegally offering off-exchange trading in digital assets. In all, the CFTC has filed 25 enforcement actions that have included digital asset-related allegations in the past 18 months.

Through the CFTC's extensive experience overseeing the trading of digital asset-based derivatives on CFTC regulated exchanges, as well as our vigilant exercise of our enforcement authority, the CFTC has developed a keen understanding of digital assets and will continue to deliver on its commitment to protect customers to the fullest extent of its statutory authority.

Thank you for the opportunity to appear before the Subcommittee. I look forward to answering any questions you may have.

[The prepared statement of Mr. McGonagle follows:]

PREPARED STATEMENT OF VINCENT "VINCE" MCGONAGLE, J.D., DIRECTOR, DIVISION OF MARKET OVERSIGHT, COMMODITY FUTURES TRADING COMMISSION, WASHINGTON, D.C.

Chairman Maloney, Ranking Member Fischbach, and Members of the Subcommittee, thank you for the opportunity to appear before you today to share my views on digital asset regulation as the Director of the Division of Market Oversight at the Commodity Futures Trading Commission (CFTC, Agency or Commission).

CFTC Mission

As you know, the CFTC is the primary regulator of the futures, options, and swaps markets. The Agency's mission is to promote the integrity, resilience, and vibrancy of the U.S. derivatives markets through sound regulation.

Our governing statute, the Commodity Exchange Act (CEA or Act), serves the public interest by mandating the establishment of a regulatory framework that allows the Agency to ensure market integrity, protect customer funds, avoid systemic risk, and police derivatives markets for manipulative activity, fraud and other abuses, while fostering innovation and fair competition.[1] As the transactions within our jurisdiction "are affected with a national public interest by providing a means for managing and assuming price risks, discovering prices, or disseminating pricing information through trading in liquid, fair and financially secure trading facilities,"[2] the CEA outlines "a system of effective self-regulation of trading facilities, clearing systems, market participants and market professionals under the oversight of the Commission."[3]

---

[1] CEA § 3(b) (7 U.S.C. § 5(b)).

[2] CEA § 3(a) (7 U.S.C. § 5(a)).

[3] CEA § 3(b) (7 U.S.C. § 5(b)). This system provides multi-tiered protections to market participants trading on our regulated exchanges, including the elimination of the risk of counterparty default or bankruptcy (because a regulated clearinghouse takes the opposite side of customers' transactions). Further, entities that broker futures trades (called futures commission merchants) are required to register with the CFTC, establish safeguards to prevent conflicts of interest, and segregate customer assets to protect the assets from the risk of the broker's bankruptcy. See CEA §§ 4d(a) and 4d(c) (7 U.S.C. §§ 6d(a) and 6d(c)).

Designated Contract Market Registration, Compliance Obligations, and Product Listing

Generally, in order for an entity to provide a trading facility for market participants (including retail customers) to trade futures, the market must apply to the Commission to be designated as a contract market.[4] To obtain and maintain designation, an entity must comply, on an initial and ongoing basis, with twenty-three Core Principles set forth in the CEA and CFTC regulations.[5] By design, the designated contract market Core Principles ensure customer protections, establish guardrails that provide clarity regarding the risks and protections involved in trading derivatives products, and enhance transparency, without hindering the trading facilities' ability to innovate and compete fairly. This firm but flexible approach has allowed the CFTC, with authority from Congress, to evolve along with the derivatives markets.

The CFTC oversees designated contract markets through various tools, including rule enforcement reviews and system safeguards examinations to ensure compliance with the Core Principles. The CFTC also conducts direct surveillance of trading on designated contract markets. Designated contract markets are separately required to serve as self-regulatory organizations,[6] and must establish and maintain effective oversight programs, including monitoring and enforcing compliance with their rules. As self-regulatory organizations and designated contract markets, they play a key role in safeguarding the integrity of the derivatives markets by, among other things, ensuring that their members understand and meet their regulatory responsibilities.

Among other things, the Core Principles require each designated contract market to establish and enforce rules to: ensure the protection of customer funds;[7] protect market participants and markets from abusive practices; and promote fair and equitable trading on the contract market.[8] The Core Principles also require each designated contract market to ensure that the contracts they list are not readily susceptible to manipulation, and require a designated contract market to have rules and resources in place to detect and prevent manipulation, price distortion, and disruptions of the cash-settlement or delivery process.[9] The Core Principle addressing system safeguards requires each designated contract market to: establish and maintain a program of risk analysis and oversight to identify and minimize sources of operational risk, through the development of appropriate controls and procedures and the development of automated systems that are reliable, secure and have adequate scalable capacity; establish and maintain emergency procedures, backup facilities, and a plan for disaster recovery; and periodically conduct tests to verify that backup resources are sufficient to ensure continued order processing and trade matching, price reporting, market surveillance, and maintenance of a comprehensive and accurate audit trail.[10]

Under the CEA and the Commission's contract review regulations, prior to listing any new product for trading, a designated contract market must submit to the Commission all new product terms and conditions, and subsequent associated amendments.[11] In all such submissions and amendments, a designated contract market is legally obligated to meet certain Core Principles—including Core Principle 3, which requires that a designated contract market only list contracts for trading that are not readily susceptible to manipulation.[12] Under the CEA, the designated contract

---

[4] Such designation is required absent an applicable exemption or exclusion. Criteria, procedures, and requirements for designation as a designated contract market are set forth in Section 5 of the CEA (7 U.S.C. § 7) and Part 38 of the CFTC's regulations. Appendix A and B to Part 38 provide specific information on these requirements and guidance to applicants seeking to become designated contract markets. Similarly, absent any applicable exemption or exclusion, in order for an entity to operate a trading facility for the trading or processing of swaps by and between eligible contract participants, the entity must seek and obtain registration with the CFTC as a swap execution facility (SEF) through CEA Section 5h and Part 37 of the CFTC's regulations. For a definition of eligible contract participants, see CEA § 1a(18) (7 U.S.C. § 1a(18)).

[5] *See* CEA § 5(d) (7 U.S.C. § 7(d)), with the implementing regulations under Part 38 of the CFTC's regulations.

[6] *See* CFTC Regulation 1.3.

[7] Core Principle (CP) 11 at CEA § 5(d)(11) (7 U.S.C. § 7(d)(11)).

[8] CP 12 at CEA § 5(d)(12) (7 U.S.C. § 7(d)(12)).

[9] CPs 3 and 4 at CEA § 5(d)(3)–(4) (7 U.S.C. § 7(d)(3)–(4)).

[10] CP 20 at CEA § 5(d)(20) (7 U.S.C. § 7(d)(20)).

[11] CEA § 5c(c) (7 U.S.C. § 7a–2(c)) and CFTC Regulations 40.2 and 40.3. These same processes also apply for products to be listed on SEFs, with compliance required with the corresponding SEF regulatory framework.

[12] The Commission has provided Guidance to designated contract markets and SEFs on meeting their Core Principle 3 obligations in Appendix C to Part 38 of the Commission's regulations.

Continued

market may file its new product submission under a process called "self-certification" by certifying that the product to be listed complies with the Act and CFTC regulations and providing a concise explanation and analysis of the product and its compliance.[13]

Similarly, under the CEA and the Commission's rule review regulations, prior to implementing a new or amended rule, a designated contract market must submit to the Commission the text of the rule and note any substantive opposing views to the rule that were not incorporated into the rule.[14] In all such submissions, a designated contract market is legally obligated to meet Core Principles. The designated contract market may file its new or amended rule submission through self-certification by certifying that the rule complies with the Act and CFTC regulations and providing a concise explanation and analysis of the operation, purpose and effect of the new or amended rule and its compliance.[15]

CFTC Regulatory Jurisdiction Involving Digital Assets

Digital assets have been broadly determined by the CFTC and Federal courts to be commodities under the CEA.[16] As discussed below, the CFTC has broad regulatory oversight over any futures, options, and swaps listed by designated contract markets.

The CFTC has regulated exchange listed futures contracts on digital assets since late 2017. By way of background, in 2017, three designated contract markets expressed interest to the CFTC in listing digital asset-based derivatives contracts for trading.[17] These designated contract markets voluntarily provided the CFTC with advance draft contract terms and conditions for their proposed contracts.[18] In December 2017, the three designated contract markets self-certified that they would list Bitcoin derivatives contracts for trading.[19] Though the Commission did not determine to stay the certifications or seek public comment at the time, the CFTC published two documents in connection with these self-certification submissions to provide the public with background information on the CFTC's oversight of, and approach to, virtual currency futures markets.[20]

See 17 CFR pt. 38, Appendix C. At any time, Commission staff may ask a designated contract market or SEF for a detailed justification of its continuing compliance with core principles, including information demonstrating that any contract listed for trading on the designated contract market or SEF meets the requirements of the Act and designated contract market or SEF Core Principle 3, as applicable. See CFTC Regulations 38.5 and 37.5. Failure of a designated contract market or SEF to adopt and maintain practices that adhere to these requirements may lead to the Commission's initiation of proceedings to secure compliance.

[13] CEA § 5c(c)(1)–(3) (7 U.S.C. § 7a–2(c)(1)–(3)) and CFTC Regulation 40.2. Alternatively, the designated contract market or SEF may voluntarily request that the CFTC review the exchange's analysis of the product and its compliance with the CEA and CFTC regulations and approve the new product for listing (through CEA 5c(c)(4)–(5) (7 U.S.C. § 7a–2(c)(4)–(5)) and CFTC Regulation 40.3).

[14] CEA § 5c(c) (7 U.S.C. § 7a–2(c)) and CFTC Regulations 40.5 and 40.6. These same processes also apply for products to be listed on SEFs, with compliance required with the corresponding SEF regulatory framework.

[15] CEA § 5c(c)(1)–(3) (7 U.S.C. § 7a–2(c)(1)–(3)) and CFTC Regulation 40.6. Alternatively, the designated contract market or SEF may voluntarily request that the CFTC review the exchange's analysis of the rule and its compliance with the CEA and CFTC regulations and approve the new rule (through CEA 5c(c)(4)–(5) (7 U.S.C. § 7a–2(c)(4)–(5)) and CFTC Regulation 40.5).

[16] The CFTC first found that Bitcoin and other virtual currencies are commodities in 2015. *See In re Coinflip, Inc., d/b/a Derivabit, and Francisco Riordan,* CFTC No. 15–29 (Sept. 17, 2015), *http://www.cftc.gov/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfcoinfliprorder09172015.pdf.* In 2017, the CFTC proposed guidance regarding its jurisdiction over certain types of retail transactions involving virtual currency. Following extensive industry engagement and public comment, the CFTC finalized this guidance in 2020. *Retail Commodity Transactions Involving Certain Digital Assets,* 85 FED. REG. 37734 (June 24, 2020). In 2018, Federal courts affirmed the CFTC's jurisdiction over digital assets in two cases, *CFTC* v. *McDonnell,* 332 F. Supp. 3d 641 (E.D.N.Y. 2018) and *CFTC* v. *My Big Coin Pay Inc.,* 334 F. Supp. 3d 492 (D. Mass. 2018). Certain digital assets may also be securities to which the securities laws apply. Whether or not a given digital asset is a security requires examination of the specific characteristics of that asset, as set forth in *SEC* v. *W.J. Howey Co.,* 328 U.S. 293 (1946).

[17] CFTC Backgrounder on Self-Certified Contracts for Bitcoin Products, Dec. 1, 2017, available at *https://www.cftc.gov/sites/default/files/idc/groups/public/@newsroom/documents/file/bitcoin_factsheet120117.pdf.* Two designated contract markets intended to list futures contracts on Bitcoin and a third designated contract market intended to list a new contract for Bitcoin binary options.

[18] *Id.*

[19] *Id.*

[20] CEA § 5c(c)(3) (7 U.S.C. § 7a–2(c)(3)). *See https://www.cftc.gov/sites/default/files/idc/groups/public/@newsroom/documents/file/bitcoin_factsheet120117.pdf* and *https://www.cftc.*

A few months later in 2018, staff issued an advisory to encourage innovation and growth of digital asset derivatives products to be traded on designated contract markets and cleared by derivatives clearing organizations within an appropriate oversight framework under the Core Principles.[21] Specifically, staff clarified their priorities and expectations when reviewing new virtual currency derivatives to be listed on a designated contract market or to be cleared by a derivatives clearing organization.[22]

Since then, the trading of futures contracts in digital assets has grown notably. Today, of the sixteen designated contract markets that the CFTC oversees, five list for trading futures and options contracts on Bitcoin, ether, or both. Market participants are actively trading over a dozen different futures and options contracts on digital assets across these five designated contract markets. When market participants trade digital asset-based futures contracts on a designated contract market, they are afforded the same customer protections and transparency as when they trade in futures contracts on any other asset class—including certainty over custody of their margin and clarity regarding bankruptcy protections.

CFTC Cash Market Enforcement Actions Involving Digital Assets

While the CFTC does not have direct statutory authority to regulate cash markets, the CFTC maintains anti-fraud, false reporting,[23] and anti-manipulation enforcement authority over commodity cash markets in interstate commerce (including digital asset cash markets). When the CFTC becomes aware of potential fraud or manipulation in an underlying market, we investigate and address misconduct through our enforcement authority. In the digital asset space, since 2014, the CFTC has aggressively exercised its enforcement authority bringing more than 50 enforcement actions.

Most recently, in FY 2021, the CFTC filed numerous cases charging retail fraud involving digital assets,[24] and cases charging platforms with illegally offering off-exchange trading in digital assets.[25] In all, the CFTC filed over 20 enforcement actions that included digital asset-related allegations of misconduct in FY 2021.

Thus far in FY 2022, the CFTC has filed several enforcement actions involving digital assets, including an action for making untrue or misleading statements and omissions of material fact in connection with the U.S. dollar tether token (USDT) stablecoin.[26] In addition, the Commission recently filed a complaint involving allegations for making false or misleading statements of material facts or omitting to state material facts to the CFTC in connection with the self-certification of a Bitcoin futures product.[27]

The Derivatives Markets the CFTC Oversees Work Well

The CEA and the CFTC's regulatory framework have worked well for our futures markets for many decades. The CFTC's focus on customer protections, market integrity, price discovery and transparency has proven to be effective, even in times of volatility. The strength of our futures markets is why in 2010, Congress tasked the CFTC with creating an oversight system for the over-the-counter swaps markets after the 2008 financial crisis.

Following enactment of the Dodd-Frank Act, the CFTC thoughtfully and quickly enacted regulations to register trading facilities for swaps as swap execution facilities and to regulate the trading of swaps on swaps execution facilities as well as customer protections for swaps traded bilaterally. Today, the swaps markets that the CFTC oversees exceed $300 trillion in gross notional outstanding. Of the swaps in the credit and interest rates markets (two of the largest swap asset classes in terms of volume and notional outstanding), a notable portion of the swaps positions are cleared at a derivatives clearing organization. By bringing the previously opaque over-the-counter swaps market under the CFTC's oversight, our extensive swaps markets now benefit from transparency, enhanced customer protections, and promoted competition.

---

gov/sites/default/files/idc/groups/public/%40customerprotection/documents/file/backgrounder_virtualcurrency01.pdf.

[21] *See* CFTC Staff Advisory No 18–14, *https://www.cftc.gov/LawRegulation/CFTCStaffLetters/index.htm*.

[22] *See Id.*

[23] *In re Coinbase Inc.,* CFTC No. 21–03 (Mar. 19, 2021).

[24] Press Releases 8366–21, 8374–21, 8381–21, 8441–21, 8434–21, 8434–21, and 8452–21.

[25] Press Releases 8374–21 and 8433–21.

[26] Press Release 8450–21.

[27] Press Release 8540–22.

Conclusion

Through the CFTC's extensive experience overseeing the trading of digital asset-based derivatives on CFTC-regulated exchanges as well as the CFTC's vigilant exercise of jurisdiction of its enforcement authority over commodity cash markets in interstate commerce, the CFTC has developed a keen understanding of digital assets, and will continue to deliver on its commitment to protect customers to the fullest extent of its statutory authority.

Thank you for the opportunity to appear before the Subcommittee. I look forward to answering any questions you may have.

The CHAIRMAN. I thank the gentleman.

Dr. Brummer, you may proceed when ready.

STATEMENT OF CHRIS BRUMMER, J.D., PH.D., AGNES N. WILLIAMS PROFESSOR OF LAW, GEORGETOWN UNIVERSITY LAW CENTER, WASHINGTON, D.C.

Dr. BRUMMER. Subcommittee Chairman Delgado and Chairman Maloney, Ranking Member Fischbach, and Members of the Subcommittee, it is a distinct pleasure to be here with you today. The Agriculture Committee is home to many of my favorite Members of Congress, which is saying something for a law professor.

If there is one thing I would like you to remember from my remarks today, it is that the future of digital asset regulation will require much more than just placing various digital asset products into varying digital—excuse me—governmental organizational charts. It will also have to involve revisiting longstanding assumptions about market infrastructures and adapting the regulatory system in creative ways that reflect the best of our collective values and experience.

As a securities law professor, I like to use disclosure as a simple example. All too often, carelessness, inaccuracies, and omissions of—social media posts, and blogs have plagued the retail investor experience and welfare. Something I noted in my testimony on ICOs with your colleagues in the House Financial Services Committee 4 years ago, and something that has only been highlighted in the last several weeks as investors and consumers have, too often, been caught unaware of the risks entailed when transacting with opaque intermediaries.

Yet, deeming a digital asset a *commodity* or a *security* will not magically cure the problem. Commodities like gold, corn, and oil are subject to grading and quality requirements, but spot commodity transactions are not automatically subject to any particular disclosure regime. Meanwhile, calling a digital asset a *security* won't solve the problem either. U.S. securities law is simultaneously under- and over-inclusive. It asks for disclosure on things like corporate board governance but not blockchain governance. Furthermore, securities regulations are premised on the idea of disclosures being filed and not read, a posture that does little to help consumers and investors desperate for information as they navigate digital asset markets.

So, irrespective of which regulator is in charge, that regulator will have to have a builders' mentality. Strong and rigorous enforcement is essential, but it is just one tool, and by definition, involves waiting for problems to arise instead of nipping them in the bud. You also need auditors of blockchain source code and better delivery systems for information and more.

Now, with that said, there is the question for this Subcommittee as to whether the CFTC in particular is up to the task of regulating the spot market for those digital assets which are commodities and not securities. Fortunately, the United States enjoys not one, but two world-class regulators, the SEC and the CFTC, and I do believe that both regulators could do the job. But each would bring to the table very different comparative advantages. The CFTC has a deep well of experience substantively regulating digital asset infrastructures, from approving the first Bitcoin swaps and options traded on exchanges in 2014, to overseeing the first U.S. listed Bitcoin futures contract.

Through its work, the CFTC has gained expertise overseeing the institutionalization of significant infrastructures intersecting directly with the digital asset commodities spot market, something the SEC has arguably only accomplished in attenuated fashion through Bitcoin futures ETS. The CFTC is also an important cop on the beat of Bitcoin spot markets.

So, in many ways, extending oversight of cash digital asset commodity markets could be interpreted as a natural evolution or extension of its existing oversight.

Where the CFTC is less developed than the SEC, however, is in the domain of disclosure, and the CFTC is well behind the SEC in terms of resources. The CFTC is but ¼ the size of the SEC, and enjoys a fraction of the SEC's budget.

Where, however, I think the builders' mentality will be most critical for either agency will be in the context of financial inclusion. To its credit, the digital assets debate has opened up a long overdue dialogue on how overlooked communities, and especially minority communities, build wealth. But critics and proponents alike tend to miss the forest for the trees, and almost entirely on the wisdom of a particular asset class. Is Bitcoin good or bad for Black Americans, for example. Without tackling the larger, thornier issue head-on, how do we ensure communities traditionally left out of our capital markets participate in a meaningful and diversified way over the long-term and earlier in a sector's life and economic cycle when value and wealth is created?

Moreover, focusing on digital assets as an investment also diverts attention from what is likely the far more relevant question, at least from the standpoint of financial inclusion. Namely, whether there are parts of the ecosystem's technology stack that can be leveraged to open opportunities for the underserved here in the United States, and in my testimony, I list some of those potential use cases.

So, thank you very, very much for your time. I am really looking forward to this conversation, and I am looking forward to your questions.

[The prepared statement of Dr. Brummer follows:]

PREPARED STATEMENT OF CHRIS BRUMMER, J.D., PH.D., AGNES N. WILLIAMS PROFESSOR OF LAW, GEORGETOWN UNIVERSITY LAW CENTER, WASHINGTON, D.C.

Chairman Maloney, Ranking Member Fischbach, and Members of the Subcommittee:

It is a distinct pleasure to be here with you today. The Agriculture Committee is home to many of my favorite Members of Congress—which is saying something

for a law professor—and I've long been impressed, and thankful for the bipartisanship this Committee has long embraced. Today's hearing is yet another example.

With financial markets experiencing enormous volatility, and global monetary practice reversing decades long trends in old and new markets alike, I've been asked to talk about how best to strategically think about the regulatory future of digital assets, and the implications of digital asset markets for financial inclusion.

Either issue could be the subject of its own hearing, but they are not altogether unrelated. I'll try my best to connect the dots where I can.

The Coming Work of Regulatory Agencies

If there is one thing I would like you to remember from my remarks today, it is that the future of digital asset regulation will require much more than just defining agency jurisdiction and placing digital asset products into varying governmental organizational charts. It will also, necessarily, involve revisiting longstanding assumptions about market infrastructures embedded in securities and derivatives law and adapting the regulatory system in creative ways that reflect the best of our experience and collective values.

Four years ago, near the height of the Initial Coin Offering (ICO) boom, I advised your colleagues in the Financial Services Committee that there would be significant work ahead for Congress and regulators seeking to tackle digital asset regulation, regardless as to how digital assets, ICOs or otherwise, were classified.[1] Time has proven those comments correct, and given the limited advances regulatorily since then, they are as true today as ever. Irrespective of which agency is ultimately given more authority over digital assets markets, regulators need to undertake significant work with regards to upgrading systems to be mission ready. The jurisdictional question is but the tip of a much larger iceberg of issues confronting regulators and Congress today.

As a securities law professor, I like to use disclosure as a simple example. As some of you may recall, disclosure was the focus of my testimony when I spoke on ICOs.[2] Today, the topic of disclosure has once again been highlighted as retail investors have been too often caught unaware of the risks entailed when engaging in digital asset transactions with lending firms, custodians and complex intermediaries and protocols.

Yet deeming a digital asset a "commodity" or "security" will not magically passport digital assets to regimes ready built to provide proper or even efficient oversight or clarity. Financial futures on "commodities" like corn, gold, and oil may face grading and quality requirements, but spot commodity transactions are not automatically subject to any particular disclosure regime. Instead, the identification of a product as a commodity subjects those that transact on the spot market to a range of anti-fraud protections—effectively 'negative' disclosure requirements prohibiting misleading statements and market manipulation—as opposed to any substantive, positive disclosure demands.[3]

Calling a digital asset a "security" won't solve the problem, either. This is because the SEC's disclosure obligations largely fail to anticipate the particularities of blockchain infrastructures. Indeed, as I have consistently noted for lawmakers, even if one were to make the counterfactual assumption that all digital assets were securities, Regulation S–K, the disclosure template for Initial Public Offerings, is simultaneously under- and over-inclusive. As such, it fails in some instances to account for critical aspects of the digital assets ecosystem, and in others imposes obligations with little to no relevance, creating both a lack of clarity and inefficiency in compliance.

Complicating things even further, the infrastructure supporting digital assets presents novel policy and strategic questions on the part of any regulator. Tradition-

---

[1] *See What Should Be Disclosed in an ICO White Paper?,* Hearing Before the Subcomm. on Cap. Mkts., Sec. and Inv of H.R. Comm. on Fin. Servs., 115th Cong. (2018) (written testimony of Chris Brummer, Fac. Dir., Geo. U. L. Ctr.); *See also* an expanded analysis by Chris Brummer, Jai Messari & Trevor Kiviat in *What Should be Disclosed in an* ICO?, DIGITAL ASSETS: LEGAL, REGULATORY AND MONETARY PERSPECTIVES 157–202 (2019).

[2] For an overview of shortcomings of white paper disclosures, *see* Shaanan Cohney, David A. Hoffman, Jeremy Sklaroff, & David Wishnick, *Coin-Operated Capitalism,* 119 COLUM. L. REV. 608 (2019). These shortcomings have particular salience given the complexity of some services; *See also* Hilary Allen, *DeFi 2.0?, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4038788* (noting how complexity inherently makes risks harder to anticipate, and to understand, especially for retail participants). The FTC has attempted to, at least indirectly, quantify the extent of the problem, suggesting that losses from digital assets scams topped $1 billion in 2021. Lesley Fair, *Reported digital assets scam losses since 2021 top $1 billion, says FTC Data Spotlight,* FTC (June 3, 2022) available at *https://www.ftc.gov/business-guidance/blog/2022/06/reported-crypto-scam-losses-2021-top-1-billion-says-ftc-data-spotlight*.

[3] *See* 17 CFR §§ 180.1.

ally, U.S. disclosure regimes have rested on the assumption that the issuer is in possession of nonpublic material information that needs to be made broadly accessible to investors. This transparency is intended to allow investors to better understand the risks they face and to then respond to these dangers by appropriately pricing that risk or avoiding altogether by investing elsewhere. But in most digital asset contexts, particularly those involving more decentralized actors operating on public blockchains, much (although not all) information relevant to an investor or consumer is already visible to the public on chain—but it is accessible and understandable only to technologically sophisticated actors.

This feature takes on special importance when contemplating the basic goals of a disclosure system for digital assets. With vast quantities of complex information already encoded on public blockchains for sophisticated actors, any disclosure regime for digital assets should be geared to speak to everyday retail customers and investors. Yet for those with even a passing familiarity with today's primary disclosure system, which applies to public companies, it is clear that disclosures are largely designed to be "filed and not read." Submissions are voluminous and dense. They are written in legalese and filed on the SEC's Edgar database, and often follow formats that respond to the demands of analysts at financial institutions, not retail investors.[4]

To truly protect participants in digital asset markets, another model is likely to be better suited for the diverse interests and backgrounds represented by retail investors. I have argued that we need to look much more carefully at consumer protection law's focus on targeted, retail-friendly disclosures that are meant to be engaged with and digested by everyday participants, and not ignored because they are too inaccessible or overwhelming.[5] Specifically, I've suggested building a better disclosure regime, one that could involve revamping Regulation S–K for the risks of digital asset applications and financial products—or a new regime that is developed from scratch employing the shorter, crisper disclosure approaches typically associated with consumer protection law. I've also drawn attention to the necessity of clarity and "Plain English" in disclosures for not just the business, but also the technology used to support different protocols.[6]

I've also made the case that serious regulation, irrespective of which regulator is in charge, requires courageous creativity and a *builder's mentality.* Strong and rigorous enforcement is essential—particularly where rules are reasonably clear and bad actors ignore them or exploit ambiguities. But it's still just one tool—and by definition involves waiting for problems to arise instead of nipping them in the bud and preventing them before they happen.

A safer, fairer, and more efficient system requires additional building blocks. Gatekeepers suited to the environment are an obvious starting point. Auditors of a blockchain or protocol's code will be as important in digital asset ecosystems as auditors of a public company's financial statements. Purpose-built operational systems will be critical as well. Just this month, an anonymous hacker was served with

---

[4] *See* Zohar Goshen & Gideon Parchomovsky, *The Essential Role of Securities Regulation,* 55 DUKE L. J. 711, 713 (2006) ("Any serious examination of the role and function of securities regulation must sidestep the widespread, yet misguided, belief that securities regulation aims at protecting the common investor. Securities regulation is not a consumer protection law."); *see also* Troy Paredes, *Blinded by the Light: Information Overload and Its Consequences for Securities Regulation* 2 (St. Louis U., Faculty Working Paper Series, Paper No. 03–02–02, 2003) available at *http://ssrn.com/abstract=413180* (noting that "[s]ecurities regulation is motivated, in large part, by the assumption that more information is better than less," but that it can create "information overload" for retail investors).

[5] Chris Brummer, *Disclosure, Dapps and DeFi,* STAN. J. OF BLOCKCHAIN LAW & POLICY (Mar. 27, 2022 forthcoming) available at *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4065143.*

[6] Notably, the SEC has implemented "Plain English" disclosure rules designed to reduce the jargon and difficulty often associated with reading registration statements. The most stringent requirements in Rule 421(d) articulate definitive prohibitions against "legal jargon" and "technical terms" in the summary, risk factors, and cover and back pages of a prospectus. Meanwhile, under Rule 421(b), the Commission has outlined a number of norms such as "short sentences whenever possible," "bullet points," and "descriptive headers" while advising that prospectus drafters avoid "legal and highly technical business terms," "legalistic, overly complex presentations," "vague boilerplate," "excerpts from legal documents," and "repetition." As such, the Plain English rules speak to the overly complex business narratives and communications that have traditionally made securities offerings indecipherable for everyday investors. Plain English disclosures apply, however, only to the front and back pages, and summary and risk factors, of prospectuses included in registration statements filed with the SEC. They do not relate to the disclosures consumers may need most, like the more in-depth descriptions of relevant tokens or supporting technologies that are often critical to understanding a dapp as an investment thesis. *Id.*

a restraining order via an NFT delivered to the perpetrator's wallet.[7] In a similar guise, I've written about using NFTs for disclosure delivery in some DeFi settings, incentivizing investors to read disclosures (through rewards or whitelisting) in ways that improve their disclosure experience in meaningful ways that advance consumer protection.[8] My point then, as now, is that a functioning system that safeguards consumers and investors will need more than just (re)drawing the regulatory perimeter, and punishing actors after the damage has been done. Proactive, creative steps will also be necessary to make the system work well for everyone—steps that acknowledge the strengths and weaknesses of not only emerging financial technologies, but also those of the legacy regulatory system.

CFTC as Crypto-Regulator

With that said, there is the obvious question for this Subcommittee as to whether the CFTC in particular is up to the task of regulating digital asset markets. It is in many ways a surprising question—even with the work ahead, few doubt that the United States enjoys not one, but two world class markets regulators. The SEC can and should regulate digital asset securities. The question is whether the CFTC could—or should—regulate the spot market for those digital assets which are "commodities" and not securities. I believe both agencies could do the job. But each would bring to the table different comparative advantages.

The CFTC's experience lies in effective and nimble deployment of its own limited authority, which has enabled it to be an important cop on the beat of Bitcoin spot markets. Although the agency does not have the power to set standards for digital asset commodity spot markets—or for that matter compel the registration of spot digital asset commodity exchanges—it does have the authority to police fraudulent and manipulative activities in digital asset commodity markets.[9] Additionally, CFTC jurisdiction covers digital asset commodity products, including products offered to retail investors and end-users, that provide for margin or leverage and is offered to retail customers.[10] Thus to the extent that spot digital asset commodity trading relies on margin or leverage to U.S. persons, it already falls under the CFTC's broader and more comprehensive registration jurisdiction—and the agency enjoys the authority to declare that those products be traded on an exchange and/or through a registered FCM.[11] Extending oversight of cash digital asset commodity markets, from this perspective, could be interpreted as a natural evolution of existing oversight.

The CFTC has also gained unique regulatory experience dealing with the risks entailed in substantively regulating digital asset infrastructures. As early as 2014, the CFTC granted under CFTC Chairman Timothy Massad approval for trading the first Bitcoin denominated swaps, options and NDFs on CFTC registered Swap Execution Facilities.[12] Several years later in 2017, the CFTC under CFTC Chairman Chris Giancarlo permitted the first Bitcoin futures contract to be listed on CBOE Futures and CME.[13] Similar to today's environment, critics panned the move, doubting both the asset and the CFTC's ability to oversee the market and arguing that the oversight would create a bubble. Subsequent studies by the San Francisco Fed would, however, confirm the opposite, that not only were the markets functioning properly—but that, if anything, the introduction of the futures market helped push Bitcoin's price down, not up. Through it all, the CFTC gained expertise in overseeing the institutionalization of significant infrastructures intersecting directly with the digital asset commodity spot market, something that the SEC, which has

---

[7] Sam Bourgi, *Anonymous hacker served with restraining order via NFT,* COINTELEGRAPH (June 9, 2022) available at *https://cointelegraph.com/news/anonymous-hacker-served-with-restraining-order-via-nft*.

[8] Brummer, *supra* note 5 at 35–37.

[9] Stephen M. Humenik, *et. al., CFTC and SEC Perspectives on Cryptocurrency*—Vol. 1: A Jurisdictional Overview, K&L Gates (May 6, 2022) available at *https://www.klgates.com/CFTC-and-SEC-Perspectives-on-Cryptocurrency-and-Digital-Assets-Volume-I-A-Jurisdictional-Overview-5-6-2022*. Notably, in the past fiscal year, the CFTC filed 23 digital asset-related enforcement actions, nearly half the total number of digital asset-related enforcement actions brought by the CFTC in the 2015–2021 period. James Rubin, *CFTC Chair Indicates Agency Will Increase Crypto Enforcement: Report,* COINDESK (May 19. 2022) *https://www.yahoo.com/video/cftc-chair-indicates-agency-increase-233028535.html*.

[10] See Commodity Exchange Act, 7 U.S.C. § 2(c)(2)(D).

[11] *Id.*

[12] Joon Ian Wong, *CFTC Chairman: We Have Oversight of Bitcoin Derivatives,* COINDESK (Dec. 11, 2014) *https://www.coindesk.com/markets/2014/12/11/cftc-chairman-we-have-oversight-of-bitcoin-derivatives/*.

[13] *Bitcoin makes debut on futures market,* AP (Dec. 10, 2017) *https://www.theguardian.com/technology/2017/dec/11/bitcoin-makes-debut-futures-market-cboe-chicago-board-options-exchange*.

yet to approve a spot Bitcoin or digital asset commodity ETF, has arguably only accomplished in attenuated fashion through multiple Bitcoin Futures ETFs.[14]

Where the CFTC's expertise *is* less developed than the SEC's is in the domain of disclosure. With nearly 90 years of history, the SEC has established itself as the nation's premier (but not sole) information regulator, with particular expertise where transactions involve an investment of money, in a common enterprise, with the expectation of profits, that is dependent on the efforts of others.[15] But where the target of regulation is fully decentralized assets, even disclosure principles would, as noted above, need a fundamental rethink by any regulator, including the SEC, and a revamp of existing legal infrastructure. And the SEC would have to pivot to doing things in ways that speak to the challenge and the times—and to *build* the infrastructure to do it properly. The SEC would have a head start in this particular area, but given the kind of conceptual agility needed, its already packed agenda, and the comparatively higher hurdle of establishing its jurisdiction (*e.g.,* the existence of a security), perhaps not as much as one would assume.

The CFTC is also well behind the SEC in terms of resources. The CFTC is but a quarter of the size of the SEC (700 *vs.* 4,000 full time employees), and enjoys a fraction of the SEC's budget ($350 Million *v.* $2.5 Billion). To build an architecture for regulating digital assets comprehensively will require considerably more resources than are currently available,[16] and unlike the SEC, which is able to move resources around the agency to meet staffing needs pertaining to digital asset regulation, the CFTC—an agency long under resourced—would presumably have little room to maneuver if proper resources were not allocated.[17]

Financial Inclusion

Where, however, I think the builder's mentality is most critical in the digital assets conversation is in the context of financial inclusion. Digital assets are, like most technologies, a tool whose benefits will depend on how the technology is used, and for whom. Skeptics have claimed that digital assets present no benefits for inclusion, or for that matter, anything else. Industry, meanwhile, has all too often touted inclusion without thinking seriously about what it means, or how to achieve it concretely.

To its enormous credit, the digital assets debate has opened up a long overdue dialogue on just how much the legacy financial system continues to fail many communities—and how overlooked communities, and especially minority communities, build wealth. But critics and proponents alike tend to miss the forest for the trees, and dwell almost entirely on the wisdom of a particular asset class ("Is Bitcoin a good or bad investment for Black Americans?") without tackling the larger, thornier issue head on: *how do we ensure communities traditionally left out of our capital markets participate in a meaningful and diversified way, over the longer term, and earlier in sectors' life and economic cycles, when value is created?* It's a question that digital assets prompt, but which is much larger than "crypto." And when digital assets are the avatar through which the conversation takes place, policy debates are invariably fixated on daily or weekly price movements instead of on basic principles of investing and on reforms needed to address a sprawling wealth gap.[18]

---

[14] *Pressure on SEC to Approve First Bitcoin ETF Ratchet Up,* PYMNTS (Apr. 25, 2022), *https://www.pymnts.com/blockchain/bitcoin/2022/pressure-on-sec-to-approve-first-bitcoin-etf-ratchets-up*.

[15] *SEC* v. *W.J. Howey Co.,* 328 U.S. 293 (1946); Securities Act 1933 § 2(a)(1) Pub. L. No. 112–106, 48 Stat. 74 (codified as amended at 15 U.S.C. §§ 77a et seq.)

[16] CFTC Chairman Rostin Benham has indicated that the CFTC would need about $100 Million in additional funding to handle regulating the spot Digital Asset commodities market, and varying proposals, and some Industry officials, have suggested a range of transaction taxes or fees to meet the challenge.

[17] What maneuverability the agency would have is hard to estimate. There is precedent suggesting that the CFTC's ability to make the most of the budget is considerable. Despite the staffing and funding differentials Congress ended up giving the CFTC, not the SEC, 95% of the swaps market jurisdiction under Dodd Frank. And despite largely missing out on commensurate increases in funding, even when compared with the SEC, the CFTC is widely viewed as a successful regulator of that market, despite its hamstrung resources. However, stacking additional responsibilities on top of an already resource poor agency, without the necessary funding, could end up not only hampering supervision of digital asset markets, but also disrupting other critical agency functions.

[18] Instead of focusing on whether people of color invest in any particular digital asset, the healthy policy discussion would center on the appropriate portfolio of low, medium and high-risk investments investors should have in order to build their economic lives—and ideally, overcome historic and growing wealth inequality. From this standpoint, basic principles of investing dictate that most investors should try to have some (modest) exposure to a diversified slice high

Continued

Focusing on digital assets as an *investment* also diverts attention from what is likely the far more relevant question, at least from the standpoint of financial inclusion—namely whether there are parts of the ecosystem's *technology stack* that can be leveraged to open opportunities for the underserved here in the United States.

I have been frank, at times painfully so, about the shortcomings in the digital assets and fintech ecosystem where I see them.[19] But for all of the challenges, the core attributes of immutability, programmability, transparency, and publicness are truly novel—and position it in ways, if done well, to supplement, and positively disrupt, a payments and financial system long tilted towards the wealthy. And it is these features that present a unique opportunity to experiment and think seriously about how to upgrade our financial system in ways that can uplift non-coastal, rural and minority populations.

Remittances have long been highlighted in Congressional hearings as obvious use cases, especially for immigrant communities facing predatory fees for cross border payments. (They also helpfully distinguish the interest many people have in using digital assets *vs.* investing in them.) But there are many other digital asset and blockchain-related projects currently under development that target financial inclusion and the democratization of opportunity even more directly for the U.S. context, and with obvious relevance to working class people and communities of color:

- Opportunities like decentralized identity, which can enable individuals to collect verifiable credentials with any constellation of actors—like banks, schools, employers, post offices, and more—that can be mixed and matched to prove not only who you are for any range of governmental purposes from voting eligibility, jury duty, "sophistication" for accredited investor status, *etc.*).
- Opportunities to build new kinds of reputation to open the credit box through decentralized credit scoring, or leverage decentralized credit scoring alongside decentralized IDs and credentials (*e.g.,* landlords and utility companies issuing credentials relating to a solid repayment history).
- Opportunities for using tokenized, real world assets as collateral for borrowing.
- Opportunities to not only reduce closing costs for home purchases and mortgage closing costs with portable credentials from mortgage agents, but to store title certificates as NFTs on blockchains.
- Opportunities to build a decentralized net for community banks and minority depositary institutions to process AML/KYC requirements associated with new bank accounts and in the process dramatically reduce their operational costs.
- Opportunities to escape predatory payments and banking fees, and access faster and cheaper financial rails via stablecoins (or CBDC) for quickly paying part time, remote and gig workers living check to check.

These kinds of innovations and projects are being explored, and in some instances built, with blockchains and digital asset technology, and could end up being massively profitable as well as socially useful. But in a world of sensational Twitter posts, big personalities and mega deals, they don't get the attention they deserve, from industry or national media. Meanwhile, regulatory agencies aren't in the business of financial inclusion, either—indeed, the Fed, SEC and CFTC all lack a financial inclusion mandate—and there is little incentive to take the time to ask what reforms are possible that could help direct energies towards positive social uses, or to ensure that the industry reaches its espoused potential of democratizing economic opportunities for everyone.

As I said 4 years ago, and at the outset of my remarks here today, the future of digital asset regulation will require much more than just defining agency jurisdiction and placing various digital assets into governmental organizational charts. More legal and regulatory brainpower will be needed, and lawmakers have a unique opportunity to step into the void, especially in periods of crisis or uncertainty, to make a real difference. But moving the dial, whether it be on consumer and investor

---

risk or alternative assets—whether it be digital assets, high end art, silver, private securities, *etc.*—alongside a much larger swath of medium and low risk assets, derisking the portfolio as a person nears retirement. Policy proposals should focus on whether or not the market, and regulatory policy, support enabling such longstanding, long proven, and nonpartisan insights. For communities of color that have long been under-invested in capital markets and have traditionally lacked access to the fastest growing parts of the economy and technology, this work is especially critical.

[19] *See 99 Problems,* Hearing Before the H.R. Comm. On Fin. Servs., (July 17, 2018) (written testimony of Chris Brummer, Prof. of Law Geo. U. L. Ctr.); See also Chris Brummer, *Fintech's Race Problem,* MEDIUM (June 9, 2020), *https://chrisbrummer.medium.com/fintechs-race-problem-856df6351695*.

protection, or financial inclusion, requires understanding the technology, its limitations, and opportunities. And having a builder's mentality.

Thanks so much to you all for the invitation to speak to you today. I look forward to your questions.

The CHAIRMAN. I thank the gentleman.

Mr. Levin, you may begin.

Mr. LEVIN. Thank you.

The CHAIRMAN. I will say, sir, you are joining us from Australia?

Mr. LEVIN. I am actually now in South Korea. I am in Seoul.

The CHAIRMAN. South Korea. Well, thank you for staying up late or getting up early. I appreciate it.

STATEMENT OF JONATHON LEVIN, CO-FOUNDER AND CHIEF STRATEGY OFFICER, CHAINALYSIS INC., NEW YORK, NY

Mr. LEVIN. Thank you, Mr. Chairman. Yes, I like doing things for the first time, since this is the first time that I am testifying from South Korea.

So, Chairman Maloney, Ranking Member Fischbach, Ranking Member Thompson, and distinguished Members of the Committee, thank you for inviting me here today on this important topic. I appreciate that this Committee is looking at how to approach market regulation for digital assets, and as has been said previously, this couldn't be more timely.

My name is Jonathan Levin, and I co-founded Chainalysis in 2014. I currently serve as our Chief Strategy Officer. I began studying cryptocurrencies 10 years ago through my research as an economist, but actually before that, my career started in commodities studying the impact that speculators have on the price of copper. Having visited the London Metal Exchange several times, I appreciate how an orderly and well-functioning market that sets reference prices of important commodities is critical to the functioning of our global economy. I think the stakes are as high in the regulation of digital assets.

While the internet brought citizens much closer together in terms of global connectivity, it hasn't given everyone the same economic opportunities that were promised. The cryptocurrency industry provides a new way to conduct global commerce, creating these economic opportunities for people across the world. The entrepreneurial dynamism present in cryptocurrencies allows for innovators and builders to create universal access to financial products that better serve consumers and their data. This technology has the potential to be significant in the U.S. competitiveness in the global economy over the coming decades.

An important point that I want to make to Members of this Committee is that the transparency of blockchains enhances the ability of policymakers and government agencies to detect, disrupt, and ultimately deter illicit activity and abuse in cryptocurrency markets. By examining a cryptocurrency payment made by a scammer, government agencies are actually able to look inside into the entire network that is behind this illicit activity, and the services that have relationship to that individual.

In contrast, in a traditional criminal financial investigation, a similar tip linking an illicit actor to a bank account is just the be-

ginning of a long, extensive process of legal requests and EMLA requests.

As with any new technology, cryptocurrency can be used by both good and bad actors. In my written testimony, I outline some of the evidence that we have at Chainalysis about the scams, thefts, and types of manipulation that we have seen. Preventing cryptocurrency from being abused in this way is intricately connected to our ability to unlock its profound potential for our economy. We are in a unique position to help this industry mitigate the risks, and in turn, increase the potential for a vibrant economy built on this new infrastructure.

The transparency provided by cryptocurrency enables unique insights into cryptocurrency markets, including an understanding of market risks that enables surveillance. There is a great deal of data and information available to government agencies looking to understand this space, whereas blockchain analytics companies like Chainalysis surveil and glean insights from transactions that are settled on the blockchain, there is also a lot of off chain data that can be used to understand market manipulation trends and market manipulation in order books, and allow typologies related to this type of abuse.

I make a number of recommendations in my written testimony, but a key recommendation I would like to highlight for this Committee is that we should aim to create a stable, regulated market whereby the world looks to the United States for established asset reference cryptocurrency prices just as they do for many other types of commodities. If America wants to lead in this sector, we must lead cryptocurrency market regulation. The clarification of cryptocurrency market regulator responsibilities would be a very important step for this market and would lend a great degree of order to the market functioning.

I appreciate your time and look forward to your questions.

[The prepared statement of Mr. Levin follows:]

PREPARED STATEMENT OF JONATHON LEVIN, CO-FOUNDER AND CHIEF STRATEGY OFFICER, CHAINALYSIS INC., NEW YORK, NY

Chairman Maloney, Ranking Member Fischbach, and distinguished Members of the Committee. Thank you for inviting me to testify before you today on this important topic. I appreciate that this Committee is looking at how to approach market regulation of digital assets. The topic of market regulation is important for safeguarding digital assets, but also the financial system more generally.

My name is Jonathan Levin and I co-founded Chainalysis Inc. with Michael Gronager, CEO of Chainalysis, in 2014. I currently serve as Chief Strategy Officer. I began studying cryptocurrencies 10 years ago through my research as an economist. I was interested in the way that the internet could create accessibility to markets and impact developing economies. While the internet brought citizens of the world closer together in terms of global connectivity, it did not give people the economic opportunities that were promised. The cryptocurrency industry provides a new way to conduct global commerce, creating economic opportunities for people across the world. The entrepreneurial dynamism that cryptocurrencies present allows for innovators and builders to create universal access to financial products that serve individuals and their data. This technology has the potential to be significant in global competition over coming decades.

An important point I want to make to the Members of this Committee, is that the transparency of blockchains enhances the ability of policymakers and government agencies to detect, disrupt and, ultimately, deter illicit activity in cryptocurrency markets. By examining a cryptocurrency payment made to a scammer, government agencies unlock immediate insight into the network of wallet

addresses and services (*e.g.,* exchanges, mixers, *etc.*) that have a relationship with this entity. In contrast, in a traditional criminal financial investigation, a similar tip, linking an illicit actor to a bank account, is just the beginning of a long, extensive process to request and subpoena records that are manually reviewed and reconciled to generate a comparable amount of insight. Despite the success of many of these investigations, the significant time investment that is required may create opportunities for illicit actors to evade justice *vs.* the real-time monitoring capabilities of blockchain intelligence.

As with any new technology, cryptocurrency can be used by both good and bad actors. As such, preventing cryptocurrency from being abused for illicit purposes is intricately connected to our ability to unlock its profound potential for the world. We are in a unique position to help this industry mitigate risks and, in turn, increase the potential for a vibrant economy to be built on this new infrastructure. The transparency provided by the blockchain enables unique insights into cryptocurrency markets, including an understanding of market risks, that can enable surveillance. There is a great deal of data and information available to government agencies looking to understand this space that is available for analysis. Whereas blockchain analytics companies like Chainalysis survey and glean insights from transactions settled on the blockchain, off-chain analytics companies offer trading insights into cryptocurrency firms' order books, and alert on typologies related to market price/volume manipulation. Off-chain analytics and market surveillance companies that we integrate with, provide alert capabilities to such typologies as pump and dumps, rugpulls, flash attack loans, spoofing, circular wash-trading as well as insider/employee trading. Where these datasets are found to be insufficient for market oversight, regulators may look to have a more complete understanding by combining on-chain data with off-chain data from other sources, or requiring additional reporting.

American markets are the world's largest, most developed, and most influential. Many of the world's most important agricultural, mineral, and energy commodities are priced in U.S. dollars in the U.S. derivatives markets. Dollar pricing of the world's commodities provides a tremendous advantage to American producers in global commerce, an advantage well-recognized by competing economies abroad. There is a key opportunity for the United States to have the regulator that establishes the world's prices for cryptocurrencies.

American markets are the best regulated in the world. The Commodity Futures Trading Commission (CFTC) has provided oversight of the U.S. exchange-traded derivatives markets for over 40 years. The CFTC is recognized for its principles-based regulatory framework and econometrically driven analysis. It also is recognized around the world for its level of expertise and breadth of capability. This combination of regulatory expertise and competency is one of the reasons why U.S. markets continue to serve participants' needs around the globe to hedge price and supply risk safely and efficiently. It is why well-regulated U.S. markets continue to serve a vital national interest—U.S. dollar pricing of important global commodities.

If America wants to lead in this sector, we must lead cryptocurrency market regulation. The clarification of cryptocurrency market regulator responsibilities would be a very important step for this market and would help to lend a greater degree of order. We should aim to create a stable, regulated market whereby the world looks to the United States for established asset-reference cryptocurrency prices, just as they do for many types of commodities.

I would also like to highlight that the cryptocurrency industry is working hard to ensure that there are the right protections for investors in this space. Two ways this is happening is through work conducted by trade associations made of cryptocurrency industry members, as well as initiatives like the *Crypto Market Integrity Coalition*,[1] a group of cryptocurrency industry members who have taken a pledge to focus on cultivating a fair digital asset marketplace to combat market abuse and manipulation and promote public and regulatory confidence in the new asset class. The cryptocurrency industry has made enormous strides to improve market integrity in the past few years. At the same time, cryptocurrency businesses are keenly aware of the concerns that still need to be addressed, and are committed to engaging with regulators to advance solutions to cryptocurrency's unique challenges.

In my testimony, I provide background on Chainalysis, outline how blockchain analysis can be leveraged by government agencies to provide greater insight into the cryptocurrency ecosystem, and describe risks we see to consumers, including contagion risks, scams, thefts, and manipulation in the cryptocurrency space and how they can be identified and mitigated using blockchain data. I also provide rec-

[1] *https://www.cryptomarketintegrity.com/*.

ommendations for how the government agencies, like the CFTC, can address potential risks in the market.

Background on Chainalysis

Chainalysis is the blockchain data platform. We provide data, software, services, and research to government agencies, exchanges, financial institutions, and insurance and cybersecurity companies. Chainalysis has over 750 customers in 70 countries. Our data platform powers investigations, compliance, and risk-management tools that have been used to solve many of the world's most high-profile cyber-crime cases and grow consumer access to cryptocurrency safely. We have worked closely with law enforcement and regulators as they have worked to disrupt and deter illicit uses of cryptocurrency.

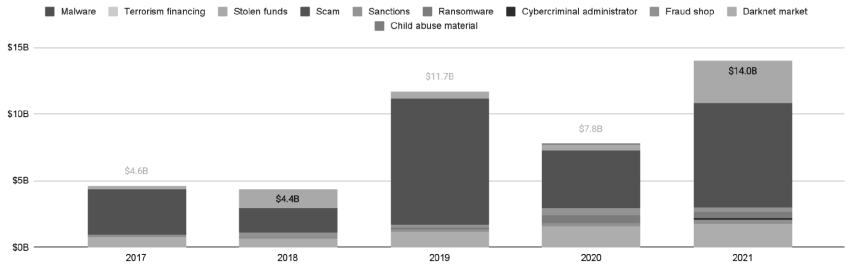
Chainalysis's partnerships with law enforcement and regulators are consistent with our corporate mission: to build trust in blockchains. Fundamentally, we believe in the potential of open, decentralized blockchain networks to drive new efficiencies, reduce barriers for innovators to create new financial and commercial products, encourage innovation, enhance financial inclusion, and unlock competitive forces across financial services and other markets. Our goal is to contribute our data, tools and expertise to drive illicit finance and other risks out of the cryptocurrency ecosystem, enabling the realization of the technology's potential.

Chainalysis's data powers both investigative and compliance tools. Our investigative tool, Reactor, enables government agencies and investigative teams to trace the illicit uses of cryptocurrency, including money laundering, theft, scams, and other criminal activities. Our compliance tool, KYT (Know Your Transaction), provides cryptocurrency businesses and financial institutions the ability to screen their clients transactions and ensure that they are not attempting to interact with illicit entities. This transaction monitoring tool provides ongoing insights for cryptocurrency businesses so that they can protect their businesses and clients and ensure regulatory compliance.

Another tool, Chainalysis Market Intel, provides the unique insights needed to conduct cryptocurrency research and make investment decisions. Chainalysis traces the funds flowing on the blockchain and tracks the cryptocurrency activity of over 3,300 businesses. This translates into intelligence on over 95% of the cryptocurrencies traded on the market. As all transfers are recorded on the blockchain in real-time, on-chain data, once mapped to real-world entities, this is a powerful dataset. It is a complete and real-time description of how cryptocurrency is being used and held. This means our metrics describe tangible, real-world activity rather than technical blockchain metrics. This offers new ways to value cryptocurrencies, and understand the market and the broader crypto-economy, as we can see how assets move in response, or to cause, events.

Chainalysis also leverages our data to conduct research into the cryptocurrency ecosystem, including the illicit use of cryptocurrency. We publish a number of reports, including our annual Crypto Crime Report. Based on this research, we reported in our *2022 Crypto Crime Report* [2] that cryptocurrency-based crime hit a new all-time high in 2021, with illicit addresses receiving $14 billion over the course of the year, up from $7.8 billion in 2020. Top categories include scams, stolen funds, darknet markets, and—pertinent to this hearing—ransomware.

Total cryptocurrency value received by illicit addresses, 2017–2021



Despite this large increase in illicit transaction volume, illicit activity as a percentage of total volume has actually fallen dramatically since 2019. In 2019, the illicit share was about 3%, in 2020 it was just over 0.5%, and in 2021 it was 0.15%. The reason for this is that cryptocurrency usage is growing faster than ever before,

[2] *https://go.chainalysis.com/2022-Crypto-Crime-Report.html*.

so while cryptocurrency-related crime is definitely increasing, the legitimate use of cryptocurrency is far outpacing its use by illicit actors. This is good news for the cryptocurrency ecosystem, but the government and industry are still faced with putting in place and implementing the appropriate controls to mitigate risks in the system.

How Blockchain Data Can be Leveraged to Gain Insights into the Cryptocurrency Ecosystem

It is a common misconception that cryptocurrency is completely anonymous and untraceable. In fact, the transparency provided by many cryptocurrencies' public ledgers is much greater than that of other traditional forms of value transfer. Cryptocurrencies like Bitcoin operate on public, immutable ledgers known as blockchains. Anyone with an internet connection can look up the entire history of transactions on these blockchains. The ledger shows a string of numbers and letters that transact with another string of numbers and letters. Chainalysis maps these numbers and letters—or cryptocurrency addresses—to their real-world entities. For example, in Chainalysis products, we are able to see that a given transaction was between a customer at a specific exchange, with a customer at another exchange, between a customer at an exchange and a sanctioned entity, or any other illicit or legitimate service using cryptocurrency. Our data set and investigative tools are invaluable in empowering government and private sector investigators to trace cryptocurrency transactions, identify patterns, and, crucially, see where cryptocurrency users are exchanging cryptocurrency for fiat currency.

Using blockchain analysis tools, law enforcement can trace cryptocurrency addresses to identify the origination and/or cash-out points at cryptocurrency exchanges. Law enforcement can serve subpoenas to these cryptocurrency exchanges, which are required to register as money services businesses (MSBs) here in the United States and collect know-your-customer (KYC) information from their customers. In response to a subpoena, the exchange will provide law enforcement with any identifying information that it has related to the cryptocurrency transaction(s) in question, such as name, address, and government identification documentation, allowing the authorities to further their investigation.

Blockchain analytics and market surveillance are two pillars for effective crypto risk monitoring and compliance programs. Chainalysis KYT addresses the need for insights across blockchain-based transactions and anti-money laundering (AML) compliance, while market surveillance tools detect manipulative trading behavior across order books and venues. Combined, these capabilities give exchanges, brokerages, regulators and other market participants a powerful view across both the external and internal risk landscapes of crypto trading. This takes market integrity to the next level, bringing us closer to addressing regulatory concerns associated with consumer and investor protections, for example.

There are many private sector tools that enable oversight of the cryptocurrency markets and detecting market abuse and manipulation in cryptocurrency trading. Our tools can be paired with these tools, including those focused on analysis of orderbook data, to enable broader insight into the ecosystem. We are working with regulatory agencies to incorporate our on-chain data alongside off-chain data from other sources in order to allow for better market surveillance. This will better enable agencies to identify market manipulation and malicious activity on the blockchain, including front and back running, rug pulls, and initial coin offering (ICO) scams, among other things.

The amount of transparency that exists in the market enables an understanding of the systemic risks that can be used to provide appropriate oversight of this space. There is a great deal of data and information that are readily available for analysis. Agencies can identify where there may be information gaps and implement additional reporting requirements or additional data sources to gain a more complete picture.

Risks in the Digital Asset Space

While Chainalysis tracks the illicit use of cryptocurrency in a number of different categories, for the purposes of this Committee and the agencies over which they have jurisdiction, I will focus on scams, thefts, and manipulation in this testimony. Here I will explain what we see in each of these categories.

Contagion Risks

One risk that has been highlighted by recent cryptocurrency news is the potential broader contagion of risks in this market. We are currently in a bear market across financial assets, including cryptocurrency. In fact, cryptocurrency prices are now more correlated to tech stocks than ever before. This means, when the broader financial markets slump, cryptocurrency prices do as well.

But there's one important difference between cryptocurrency and traditional finance: transparency. Due to the open nature of decentralized finance (DeFi) protocols, the market can often see where large, well-known players placed their bets and if those positions are facing liquidation. Furthermore, market participants can use this transparency to assess the stability of the core protocols that power the DeFi ecosystem. However, this transparency has not stopped large, centralized companies from making bets on the price of various cryptocurrencies, both using open DeFi protocols and by lending funds to one another. This creates potential contagion risks, as various centralized market participants are financially exposed to one another. While the transparent DeFi protocols continue to function as designed because they are simply code running on the blockchain, some highly leveraged businesses have struggled to unwind complex financial positions in a hostile macroeconomic environment.

This transparency and the fall in cryptocurrency prices is also exposing projects with fundamental design flaws or unsustainable economic models. Some projects that were hastily built or didn't properly manage risk will fail, and that's a natural process for any new technology or industry. This is an opportunity for the industry to leverage blockchains' transparency to analyze systemic risk and build better systems and design better rules for the next bull market.

It is important for regulators to understand both the decentralized and centralized parts of the cryptocurrency market and how they may impact each other. For example, centralized players investing in decentralized finance may find themselves overleveraged if they have not appropriately calculated the risks, in particular in a bear market. The decentralized projects in which centralized entities have invested may also fall victim to code exploits or hacks and lose their value precipitously. Being able to adequately oversee centralized players will require understanding the entire ecosystem.

Scams

There has been an evolution of scamming activity in the cryptocurrency space over the past few years. Several years ago, scams mostly presented themselves as centralized platforms where you could invest in new cryptocurrencies. *OneCoin* [3] is an example of this type of scam. As law enforcement has become better at identifying and investigating these sorts of scams, and as consumers have become wise to them, we are seeing a new trend in this space, where scammers will impersonate *high-profile people* [4] and make claims such as offering to double any cryptocurrency sent to them. Others will impersonate legitimate cryptocurrency projects on *social media* [5] platforms like Telegram, Discord, or Twitter in order to trick would-be investors into sending the scammers their funds, rather than sending them to the real platform. We also see an increase in romance scams, where the scammer develops a relationship with a victim over time and convinces them to invest in a scam website, or send them funds directly. This type of scam is also conducted using other financial assets, but it's becoming *prevalent* [6] in the cryptocurrency space, with a focus on elderly individuals. Another type of scam we now increasingly see are rug pulls. As is the case with much of the emerging terminology in cryptocurrency, the definition of "rug pull" isn't set in stone, but we generally use it to refer to cases in which developers build out what appear to be legitimate cryptocurrency projects, for example create "legitimate" ERC–20 tokens or non-fungible tokens (NFTs) that work technically on-chain. However, the real intention of the project is to accumulate as much funds as possible and disappear abruptly. Usually they try to drum up as much hype as possible (potentially hiring celebrities to endorse the product) before taking investors' money and disappearing.

In 2021, scams were once again the largest form of cryptocurrency-based crime by transaction volume, with over $7.7 billion worth of cryptocurrency taken from victims worldwide.

---

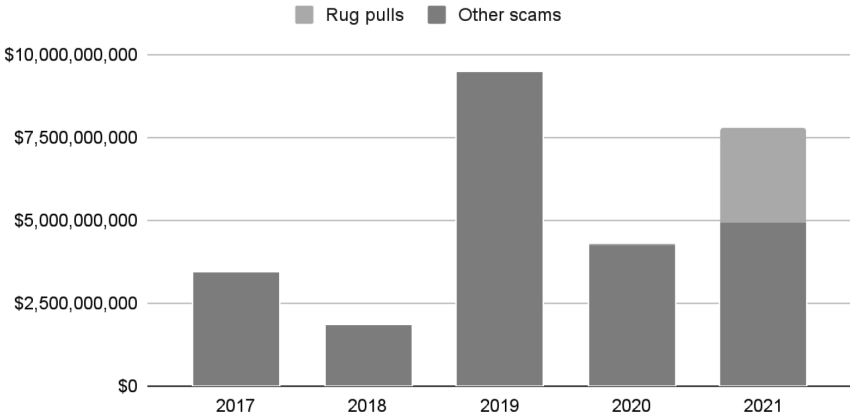
[3] *https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-charges-against-leaders-onecoin-multibillion-dollar*.

[4] *https://www.cnbc.com/2020/07/15/hackers-appear-to-target-twitter-accounts-of-elon-musk-bill-gates-others-in-digital-currency-scam.html*.

[5] *https://coinmarketcap.com/alexandria/article/3-minute-tips-avoiding-common-crypto-scams-on-telegram*.

[6] *https://www.cftc.gov/PressRoom/PressReleases/8545-22*.

Total yearly cryptocurrency value received by scammers, 2017–2021



That represents a rise of 81% compared to 2020, a year in which scamming activity dropped significantly compared to 2019, in large part due to the absence of any large-scale Ponzi schemes. That changed in 2021 with Finiko, a Ponzi scheme primarily targeting Russian speakers throughout Eastern Europe, netting more than $1.1 billion from victims.

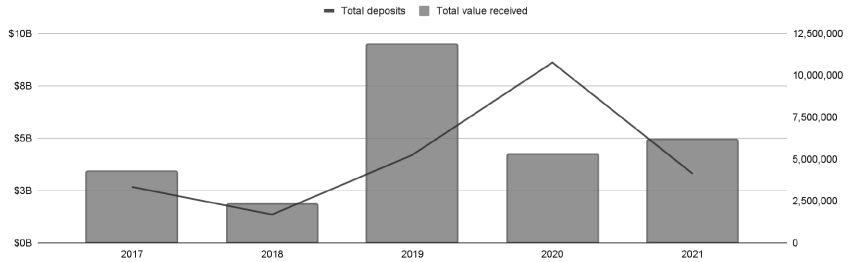
Another change that contributed to 2021's increase in scam revenue: the emergence of rug pulls, a relatively new scam type particularly common in the DeFi [1] ecosystem, in which the developers of a cryptocurrency project—typically a new token—abandon it unexpectedly, taking users' funds with them. We'll look at both rug pulls and the Finiko Ponzi scheme in more detail later in this testimony.

As the largest form of cryptocurrency-based crime and one uniquely targeted toward new users, scamming poses one of the biggest threats to cryptocurrency's continued adoption. However, cryptocurrency businesses are taking innovative steps to leverage blockchain data to protect their users and nip scams in the bud before potential victims make deposits.

Investment scams in 2021: More scams, shorter lifespans

While total scam revenue increased significantly in 2021, it stayed flat if we remove rug pulls and limit our analysis to financial scams—even with the emergence of Finiko. At the same time though, the number of deposits to scam addresses fell from just under 10.7 million to 4.1 million, which we can assume means there were fewer individual scam victims.

Total yearly cryptocurrency value received by investment scams, 2017–2021



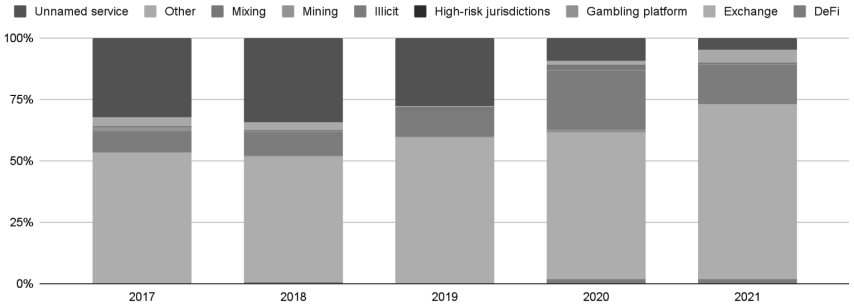
This also tells us that the average amount taken from each victim increased.

Scammers' money laundering strategies haven't changed all that much. As was the case in previous years, most cryptocurrency sent from scam wallets ended up at mainstream exchanges.

---

[1] Also known as decentralized finance, "DeFi" offers peer-to-peer financial services without the need of intermediaries such as banks, exchanges, or brokerages (who typically charge for their services). DeFi services are built and run on a blockchain through the use of smart contracts which defines the logic and rules for the service being used.

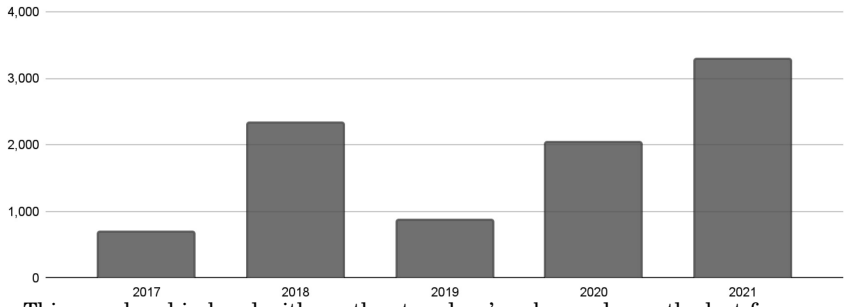
Destination of funds leaving investment scam addresses by year, 2017–2021



Exchanges using Chainalysis KYT for transaction monitoring and other transaction monitoring solutions can see this activity in real time, and take action to prevent scammers from cashing out.

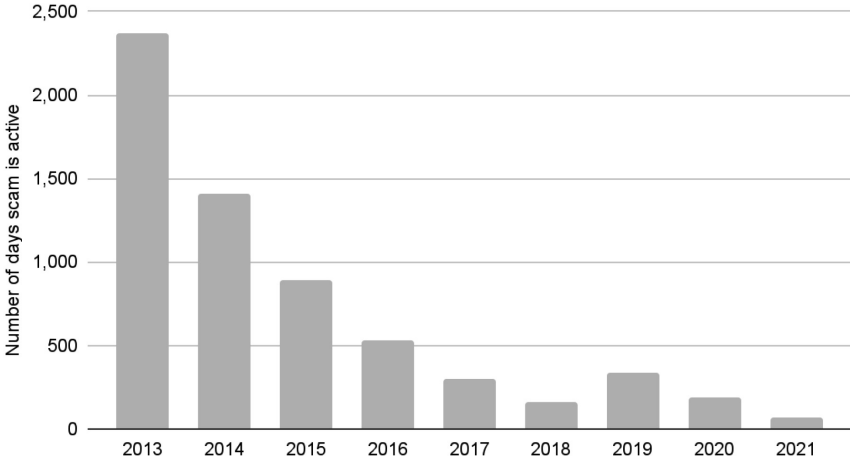
The number of financial scams active at any point in the year—active meaning their addresses were receiving funds—also rose significantly in 2021, from 2,052 in 2020 to 3,300.

Total number of unique active investment scams by year, 2017–2021



This goes hand in hand with another trend we've observed over the last few years: The average lifespan of a financial scam is getting shorter and shorter.

Lifespan of average scam by year, 2013–2021



The average financial scam was active for just 70 days in 2021, down from 192 in 2020. Looking back further, the average cryptocurrency scam was active for 2,369 days, and the figure has trended steadily downwards since then.

One reason for this could be that investigators are getting better at investigating and prosecuting scams. For instance, in September 2021, the CFTC *filed charges* [7] against 14 investment scams touting themselves as providing compliant cryptocurrency derivative trading services—a common scam typology in the space—whereas in reality they had failed to register with the CFTC as futures commission merchants. In October 2021, the CFTC *charged* [8] an El Paso resident and his firm in ongoing $3.9 million forex and cryptocurrency fraud and misappropriation scheme. In March 2022, the CFTC *charged* [9] four people with fraud for operating Ponzi schemes involving Bitcoin. In April 2022, the CFTC *settled a case* [10] against Florida-based companies and their owner for fraudulently soliciting customers to purchase a digital asset they falsely promised would allow customers to gain access to a proprietary foreign currency (forex) trading algorithm.

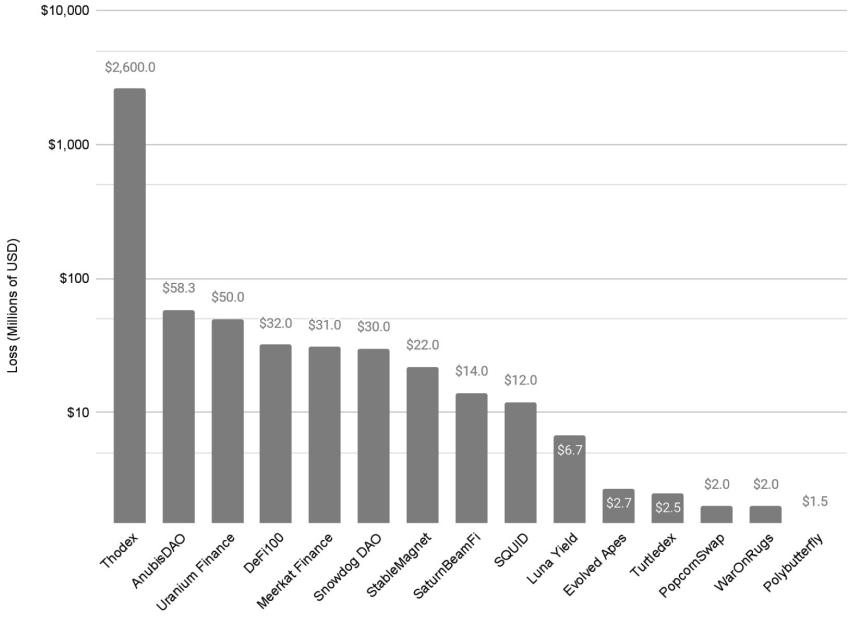
Previously, these scams may have been able to continue operating for longer. As scammers become aware of these actions, they may feel more pressure to close up shop before drawing the attention of regulators and law enforcement.

Rug pulls have emerged as the go-to scam of the DeFi ecosystem, accounting for 37% of all cryptocurrency scam revenue in 2021, *versus* just 1% in 2020. All in all, rug pulls took in more than $2.8 billion worth of cryptocurrency from victims in 2021.

Most DeFi projects entail developers creating new tokens and promoting them to investors, who purchase the new token in order to access the utility that the cryptocurrency network provides, or with the hope it will rise in value. These actions also provide liquidity to the project. In rug pulls, however, the developers eventually drain the funds from the liquidity pool, sending the token's value to zero, and disappear. Rug pulls are prevalent in DeFi because, with the right technical know-how, it's cheap and easy to create new tokens on the Ethereum blockchain or others and get them listed on decentralized exchanges (DEXes).

The chart below shows 2021's top 15 rug pulls in order of value stolen.

2021 top 15 rug pulls by cryptocurrency value stolen



[7] *https://www.cftc.gov/PressRoom/PressReleases/8434-21.*
[8] *https://www.cftc.gov/PressRoom/PressReleases/8452-21.*
[9] *https://www.cftc.gov/PressRoom/PressReleases/8498-22.*
[10] *https://www.cftc.gov/PressRoom/PressReleases/8510-22.*

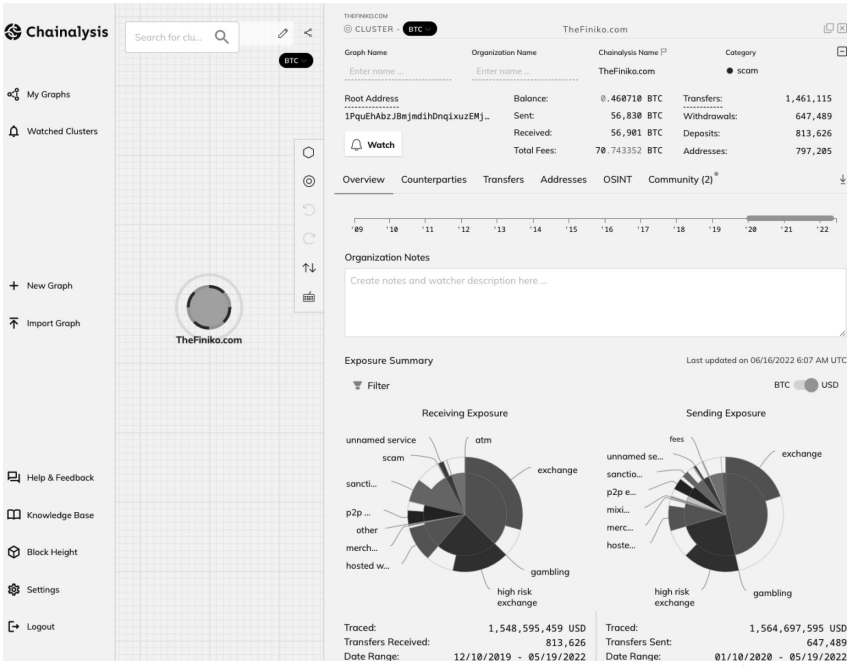
It's important to remember that not all rug pulls start as DeFi projects. In fact, the biggest rug pull of the year centered on *Thodex*,[11] a large Turkish centralized exchange whose CEO disappeared soon after the exchange halted users' ability to withdraw funds. In all, users lost over $2 billion worth of cryptocurrency, which represents nearly 90% of all value stolen in rug pulls. However, all the other rug pulls in 2021 began as DeFi projects.

Finiko: 2021's billion dollar Ponzi scheme

Finiko was a Russia-based Ponzi scheme that operated from December 2019 until July 2021, at which point it collapsed after users found they could no longer withdraw funds from their accounts with the company. Finiko invited users to invest with either Bitcoin or Tether, promising monthly returns of up to 30%, and eventually launched its own token that traded on several exchanges.

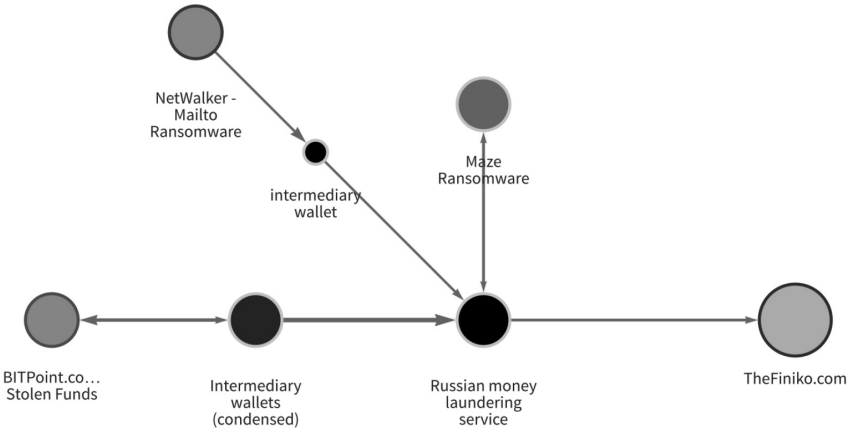
According to the *Moscow Times*,[12] Finiko was headed up by Kirill Doronin, a popular Instagram influencer who has been associated with other Ponzi schemes. The article notes that Finiko was able to take advantage of difficult economic conditions in Russia exacerbated by the [COVID] pandemic, attracting users desperate to make extra money. *Chainalysis Reactor* [13] shows us how prolific the scam was.

[11] *https://decrypt.co/68894/thodex-ceo-denies-rug-pull-discloses-cyberattacks-says-funds-are-safe*.
[12] *https://www.themoscowtimes.com/2021/07/30/as-incomes-fall-russians-are-once-again-falling-for-pyramid-schemes-a74654*.
[13] *https://www.chainalysis.com/chainalysis-reactor/*.



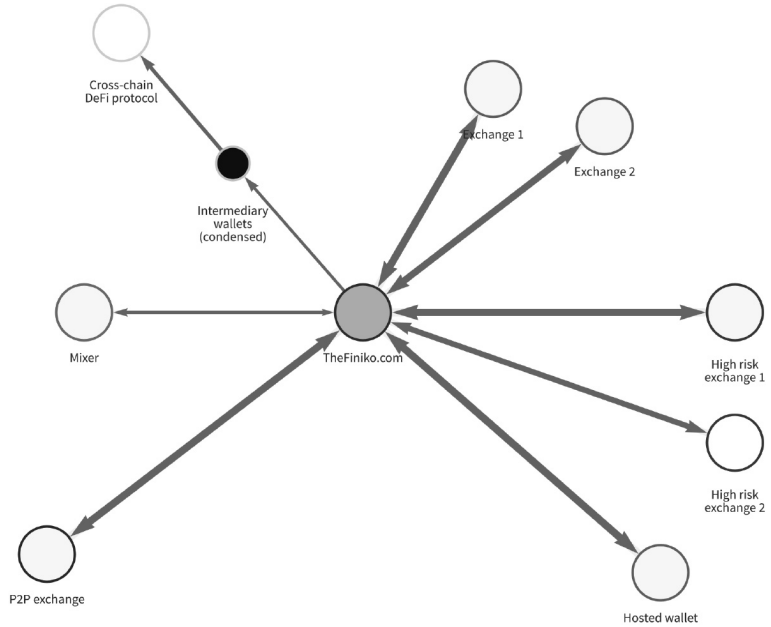
During the roughly 19 months it remained active, Finiko received over $1.5 billion worth of Bitcoin in over 800,000 separate deposits. While it's unclear how many individual victims were responsible for those deposits or how much of that $1.5 billion was paid out to investors to keep the Ponzi scheme going, it's clear that Finiko represents a massive fraud perpetrated against Eastern European cryptocurrency users, predominantly in Russia and Ukraine.

As is the case with most scams, Finiko primarily received funds from victims' addresses at mainstream exchanges. However, we can also see that Finiko received funds from what we've identified as a Russia-based money launderer.



This launderer received millions of dollars' worth of cryptocurrency from addresses associated with ransomware, exchange hacks, and other forms of cryptocurrency-based crime. While the amount the service has sent to Finiko is quite small—under 1 Bitcoin (BTC) total—it serves as an example of how a scam can also be used to launder funds derived from other criminal schemes. It's also possible that Finiko received funds from other laundering services we've yet to identify.

Finiko sent most of its more than $1.5 billion worth of cryptocurrency to mainstream exchanges, high-risk exchanges, a hosted wallet service, and a peer-to-peer (P2P) exchange. However, we don't know what share of those transfers represent payments to victims in order to give the appearance of successful investments.



Finiko also sent $34 million to a DeFi protocol designed for cross-chain transactions via a series of intermediary wallets, where it was likely converted into ERC–20 tokens and sent elsewhere. It also sent roughly $3.9 million worth of cryptocurrency to a few popular mixing services. Most interesting of all, perhaps, is Finiko's transaction history with Suex, an over-the-counter (OTC) broker that was *sanctioned* [14] by U.S. Department of Treasury's Office of Foreign Assets Control (OFAC) for its role in laundering funds associated with scams, ransomware attacks, and other forms of cryptocurrency-based crime.

Between March and July of 2020, Finiko sent over $9 million worth of Bitcoin to an address that now appears as an identifier on Suex's entry into the Specially Designated Nationals (SDN) List. This connection underlines the prolificness of Suex as a money laundering service, as well as the crucial role of such services generally in allowing large-scale cybercriminal operations, like Finiko, to victimize cryptocurrency users.

Soon after Finiko's collapse in July 2021, Russian authorities *arrested Doronin*,[15] and later also nabbed Ilgiz Shakirov, one of his key partners in running the Ponzi scheme. Both men remain in custody, and arrest warrants have reportedly been issued for the rest of Finiko's founding team.

How one cryptocurrency platform is saving users from scams

Mainstream cryptocurrency platforms, like exchanges, are in the perfect position to fight back against scams and instill more trust in cryptocurrency by warning users or even preventing them from executing those transactions. One popular platform did just that in 2021, and the results were extremely promising.

---

[14] *https://blog.chainalysis.com/reports/ofac-sanction-suex-september-2021/*.

[15] *https://news.bitcoin.com/court-extends-detention-of-finiko-pyramid-founder-doronin-and-his-right-hand-man/*.

Luno is a leading cryptocurrency platform operating in over 40 countries, with an especially heavy presence in South Africa. In 2020, a major scam was targeting South African cryptocurrency users, promising outlandishly large investment returns. Knowing that its users were at risk, Luno decided to take action, in part by leveraging Chainalysis tools and services.

The first step was a warning and education campaign. Using in-app messages, help center articles, emails, webinars, social media posts, YouTube videos, and even one-on-one conversations, Luno showed users how to spot the red flags that indicate an investment opportunity is likely a scam, and taught them to avoid pitches that appear too good to be true.

Luno then went a step further and began preventing users from sending funds to addresses it knew belonged to scammers. That's where Chainalysis came in. As the leading blockchain data platform, we have an entire team dedicated to unearthing cryptocurrency scams and tagging their addresses in our compliance products. With that data, Luno was able to halt users' transfers to scams before they were processed. It was a drastic strategy in many ways—cryptocurrency has historically been built on an ethos of financial freedom, and some users were likely to chafe at a perceived limitation on their ability to transact. But thanks to Chainalysis' best in class cryptocurrency address attributions, Luno was able to establish the trust necessary to sell customers on the strategy.

Luno first began blocking scam payments for South African users only in November 2020, and then rolled the feature out worldwide in January 2021. The plan worked, and transfers from Luno wallets to scams fell drastically over the course of 2021.

Daily value received by scams from Luno, 30 day moving average

Orig Sheets *link* [16]

The moving 30 day average daily transaction volume of transfers to scams fell 88% from $730,000 at its peak in September 2020, to just $90,000 by November. One customer summed up the results perfectly, saying, "Thank you, Luno. I was about to lose my pension and savings."

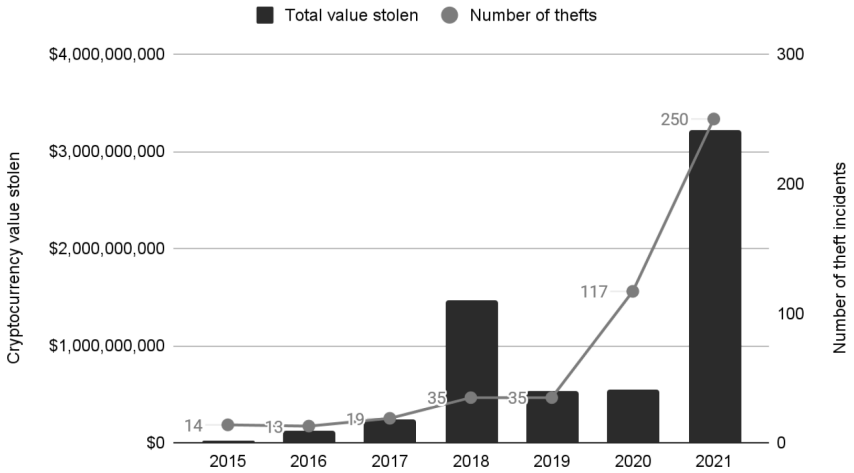
Scams represent a huge barrier to successful cryptocurrency adoption, and fighting them can't be left only to law enforcement and regulators. Cryptocurrency businesses, financial institutions, and, of course, Chainalysis have an important role to play as well. With this strategy, Luno took an important step towards establishing greater trust and safety in cryptocurrency, which we hope to continue to see grow in the industry.

Theft

Throughout 2021, $3.2 billion in cryptocurrency was stolen from individuals and services—almost 6x the amount stolen in 2020. Approximately $2.3 billion of those funds were stolen from DeFi platforms in particular, and the value stolen from these protocols catapulted 1,330%.

[16] *https://docs.google.com/spreadsheets/d/16qcyOn8EBz8KLQ6aRGmE1WObaBy0tRO8v1gMCGUBNTg/edit#gid=1289181670&range=E8.*

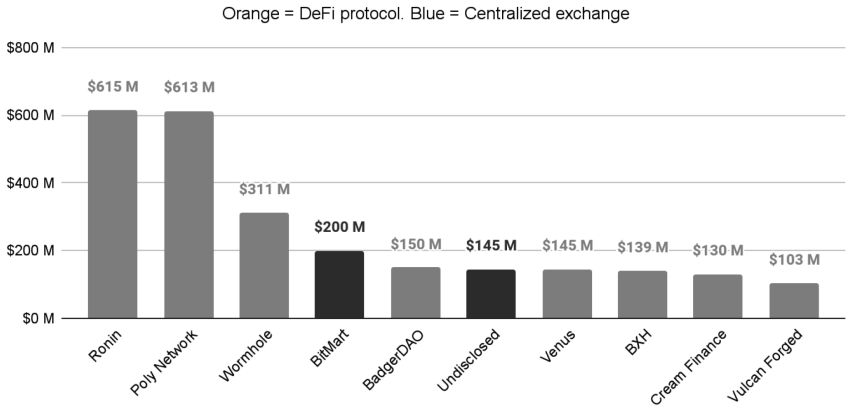
Total value stolen and total number of thefts, 2015–2021



This shift toward DeFi-centric attacks doesn't just sound pronounced—it looks like it, too. In every year prior to 2021, centralized exchanges lost the most cryptocurrency to theft by a large margin. But this year, DeFi platform thefts dwarfed exchange thefts.

The biggest cryptocurrency thefts of 2021

Top ten cryptocurrency theft incidents by amount stolen, 2021–2022 Q1



As is the case most years, the ten largest hacks of 2021 and Q1 2022 accounted for a majority of the funds stolen at $2.2 billion. Eight of these ten attacks targeted DeFi platforms in particular.

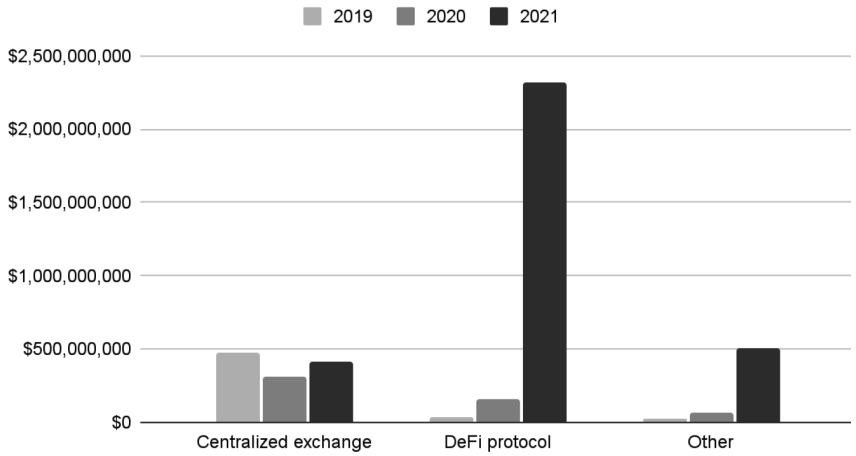
Code exploits are a prominent feature in 2021's cryptocurrency theft landscape

Historically, cryptocurrency thefts have largely been the result of security breaches in which hackers gain access to victims' private keys—the crypto-equivalent of pickpocketing. These keys could be acquired through phishing, keylogging, social engineering, or other techniques. From 2019 to 2021, almost 30% of all value was stolen from just this type of hack.

With the rise of DeFi and the extensive smart contract capabilities that power those platforms, deeper vulnerabilities have begun to emerge around the software underpinning these services. While these services are decentralized, these sorts of exploits can lead to contagion in the centralized parts of the cryptocurrency market, so it is important for regulators to understand these exploits and their broader impacts.

In 2021, code exploits and flash loan attacks—a type of exploit involving price manipulation—accounted for a near-majority of total value stolen across all services, weighing in at 49.8%. And when examining only hacks on DeFi platforms, that figure increases to 69.3%.

Annual total cryptocurrency stolen by victim type, 2019–2021



These exploits occur for a variety of reasons. For one, in keeping with DeFi's faith in decentralization and transparency, open-source development is a staple of DeFi applications. This is an important and broadly positive trend: since many DeFi protocols move funds without human intervention, users need to be able to audit the underlying code in order to trust the platform. But this also stands to benefit cybercriminals, who can analyze the scripts for vulnerabilities and plan exploits in advance.

Another potential point of failure is DeFi platforms' reliance on *price oracles*.[17] Price oracles are tasked with maintaining accurate asset pricing data for all cryptocurrencies on a platform, and the job isn't easy. Secure but slow oracles are vulnerable to arbitrage; fast but insecure oracles are vulnerable to price manipulation. The latter type often leads to flash loan attacks, which extracted a massive $364 million from DeFi platforms in 2021. In the hack of Cream Finance, for example, a series of flash loans exploiting a *vulnerability*[18] in the way Cream calculated yUSD's "pricePerShare" variable enabled attackers to inflate yUSD price to double its true value, sell their shares, and make off with $130 million in just one night.

These two dangers—inaccurate oracles and exploitable code—underscore the need for the security of both. Fortunately, there are solutions. To ensure pricing accuracy, decentralized price oracles like *Chainlink*[19] can protect platforms against price manipulation attacks. To ensure the security of smart contracts, code audits can steel programs against *common hacks*[20] like reentrancy, unhandled exceptions, and transaction order dependency.

But code audits aren't infallible. Nearly 30% of code exploits occurred on platforms audited within the last year, as well as a surprising 73% of flash loan attacks. This highlights two potential shortfalls of code audits:

1. They may patch smart contract vulnerabilities in some cases, but not all;
2. They seldom guarantee that platforms' price oracles are *tamper-proof*.[21]

So while code audits can certainly help, DeFi protocols managing millions of users and billions of dollars must adopt a more robust approach to platform security.

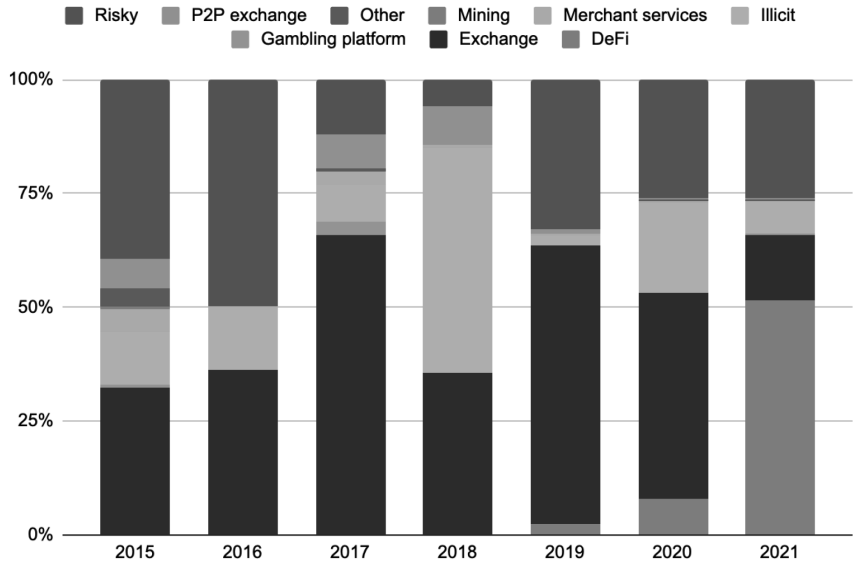
Following the money: the final destinations of stolen cryptocurrencies

In the aftermath of cryptocurrency thefts, more stolen funds flowed to DeFi platforms (51%) and risky services (25%) this year than ever before. Centralized ex-

[17] *https://cointelegraph.com/explained/defi-oracles-explained*.
[18] *https://medium.com/cream-finance/post-mortem-exploit-oct-27-507b12bb6f8e*.
[19] *https://chain.link/*.
[20] *https://www.usenix.org/system/files/sec21summer_perez.pdf*.
[21] *https://blog.chain.link/flash-loans-and-the-importance-of-tamper-proof-oracles/*.

changes, once a top destination for stolen funds, fell out of favor in 2021, receiving less than 15% of the funds. This is likely due to the embrace of *AML and KYC*[22] procedures among major exchanges—an existential threat to the anonymity of cybercriminals.

Destination of stolen funds, 2015–2021



Note: "Risky" refers to services like mixers, high-risk exchanges,[2] and services based in high-risk jurisdictions.[3]

Manipulation

In 2021 and the first half of 2022, *Chainalysis tracked*[23] a minimum $83 billion worth of cryptocurrency sent to ERC–721 and ERC–1155 contracts—the two types of Ethereum smart contracts associated with NFT marketplaces and collections—up from just $106 million in 2020.

[22] *https://blog.chainalysis.com/reports/what-is-aml-and-kyc-for-crypto/*.

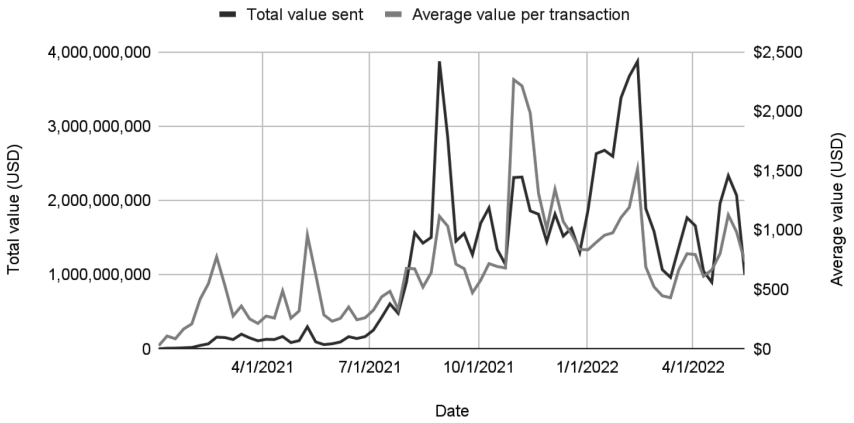
[2] A high risk exchange is an exchange that meets one of the following criteria:

- No KYC: The exchange requires absolutely no customer information before allowing any level of deposit or withdrawal. Or they require a name, phone number, or email address but make no attempt to verify this information.
- Criminal ties: The exchange has criminal convictions of the corporate entity in relation to AML/Combating the Financing of Terrorism (CFT) violations.
- High risky exposure: The exchange has high amounts of exposure to risky services such as darknet markets, other high risk exchanges, or mixing. We examine if the exchange's exposure to illicit activity is an outlier compared to other exchanges. A service with direct high risk exposure one standard deviation away from the average across all exchanges identified by Chainalysis over a 12 month period is considered a high risk exchange.

[3] High-risk jurisdictions consist of jurisdictions subject to OFAC comprehensive sanctions, which includes Iran, Cuba, Syria, North Korea, the Crimea, Donetsk, and Luhansk regions of Ukraine, as well as Venezuela due to broad government-based sanctions.

[23] *https://go.chainalysis.com/nft-market-report.html*.

Weekly total cryptocurrency value and average value per transaction sent to NFT platforms, 2021–2022 YTD

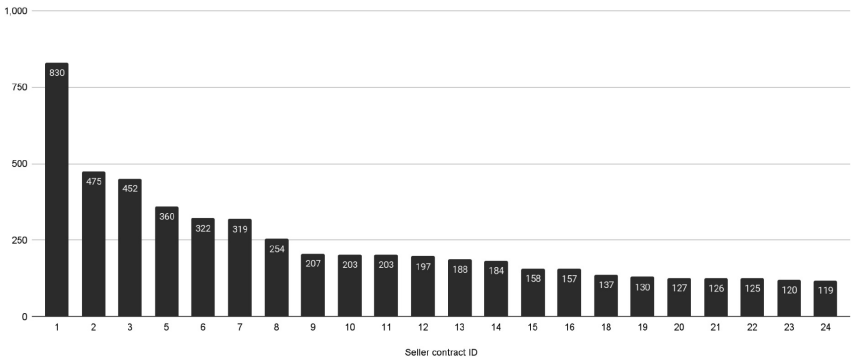


However, as is the case with any new technology, NFTs offer potential for abuse. It's important that, as our industry considers all the ways this new asset class can change how we link the blockchain to the physical world, we also build products that make NFT investment as safe and secure as possible. There have been several forms of illicit activity in NFTs: wash trading to artificially increase the value of NFTs, money laundering through the purchase of NFTs, and *insider trading*[24] on NFT marketplaces. Here I will outline what we have seen in relation to wash trading.

Wash trading, meaning executing a transaction in which the seller is on both sides of the trade in order to paint a misleading picture of an asset's value and liquidity, is another area of concern for NFTs. Wash trading has been a concern in the past with cryptocurrency exchanges attempting to make their trading volumes appear greater than they are. In the case of NFT wash trading, the goal would be to make one's NFT appear more valuable than it really is by "selling it" to a new wallet the original owner also controls. In theory, this would be relatively easy with NFTs, as many NFT trading platforms allow users to trade by simply connecting their wallet to the platform, with no need to identify themselves.

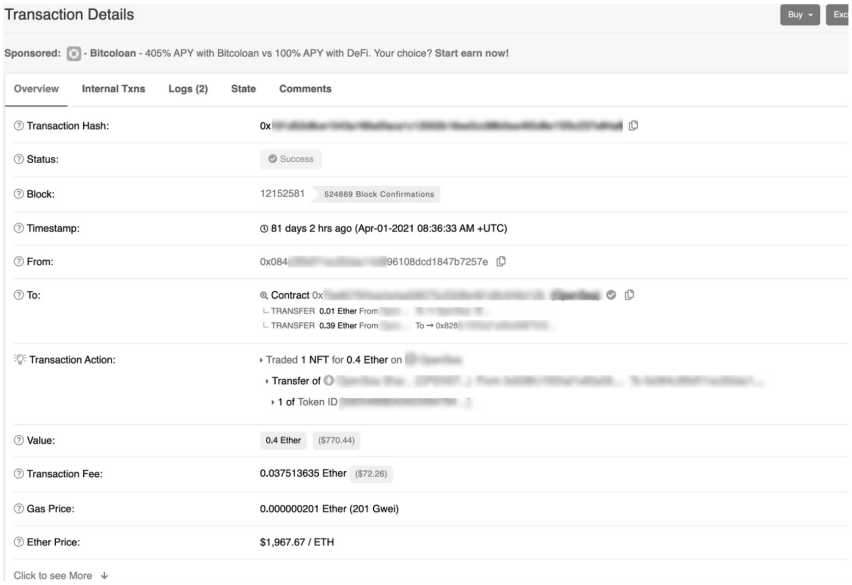
With blockchain analysis, however, we can track NFT wash trading by analyzing sales of NFTs to addresses that were self-financed, meaning they were funded either by the selling address or by the address that initially funded the selling address. Analysis of NFT sales to self-financed addresses shows that some NFT sellers have conducted hundreds of wash trades.

NFT sellers by number of sales to self-financed addresses, 2021

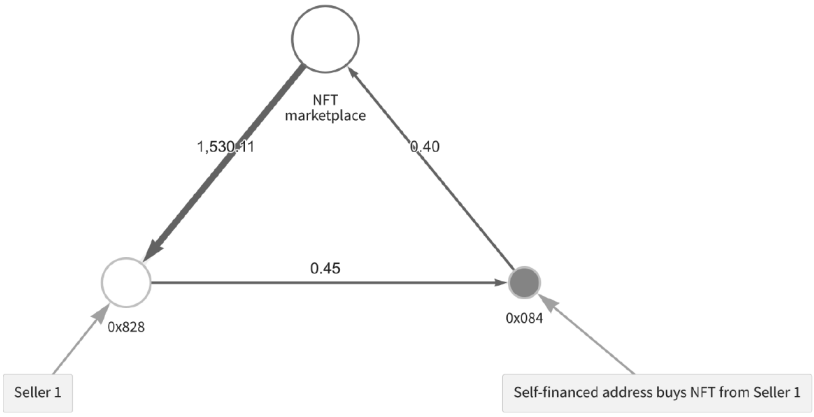


[24] *https://www.justice.gov/usao-sdny/pr/former-employee-nft-marketplace-charged-first-ever-digital-asset-insider-trading-scheme*.

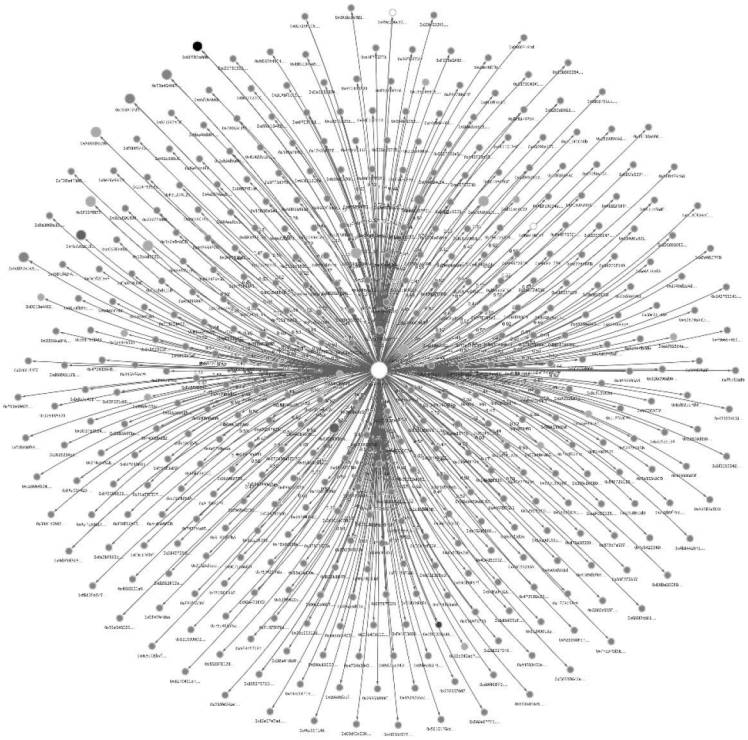
Let's look more closely at Seller 1, the most prolific NFT wash trader on the chart above, who has made 830 sales to addresses they've self-financed. The Etherscan screenshot below shows a transaction in which that seller, using the address beginning 0x828, sold an NFT to the address beginning 0x084 for 0.4 Ethereum via an NFT marketplace.



Everything looks normal at first glance. However, the Chainalysis Reactor graph below shows that address 0x828 sent 0.45 Ethereum to that address 0x084 shortly before that sale.



This activity fits a pattern for Seller 1. The Reactor graph below shows similar relationships between Seller 1 and hundreds of other addresses to which they've sold NFTs.



Seller 1 is the address in the middle. All other addresses on this graph received funds from Seller 1's main address prior to buying an NFT from that address. So far though, Seller 1 doesn't seem to have profited from their prolific wash trading. If we calculate the amount Seller 1 has made from NFT sales to addresses they themselves did not fund—whom we can assume are victims unaware that the NFTs they're buying have been wash traded—it doesn't make up for the amount they've had to spend on gas fees during wash trading transactions.

Address	Spent on gas fees in wash trading transactions	Revenue from sales of wash traded NFTs to victims	Profits
0x828	−$35,642	$27,258	−$8,383

While wash trading is prohibited in conventional securities, futures, and other derivatives, wash trading involving NFTs has yet to be the subject of an enforcement action. Wash trading in NFTs can create an unfair marketplace for those who purchase artificially inflated tokens, and its existence can undermine trust in the NFT ecosystem, inhibiting future growth. Blockchain data and analysis makes it easy to spot users who sell NFTs to addresses they've self-financed, so marketplaces may want to consider bans or other penalties for the worst offenders.

Recommendations

Provide regulatory clarity to market participants.

While cryptocurrency businesses have been subject to anti-money laundering laws since at least 2013, there are other aspects of the market that still require additional clarification, including direction from Congress. One of these areas is the cryptocurrency spot market, over and above fraud and manipulation. While the CFTC oversees derivatives markets such as Bitcoin and ether futures, and the Securities and Exchange Commission provides oversight over those tokens that are securities, cryptocurrency spot markets are largely regulated at the state-level. Clarifying these responsibilities at the Federal level, likely through legislation, would

bolster anti-fraud and manipulation protections. It is also important to provide clarity about different tokens—for example, which tokens fall under the securities framework and which fall under the commodities framework. Having this guidance will help to make the perimeters very clear and will also make clear what falls outside of an agency's specific jurisdiction.

Providing market clarity will also support the goals of economic growth and leadership in the U.S. If America wants to lead in the cryptocurrency sector, we must lead cryptocurrency market regulation. Clarifying roles around cryptocurrency market regulation at the Federal level would be a very important step for this market and would help to lend a greater degree of order. We should aim to create a market in which the world looks to the United States for established asset-reference cryptocurrency prices, just as they do for many types of commodities.

Ensure adequate funding, resources, and training for government agencies charged with investigating fraud, manipulation, and abusive practices in this space.

As this asset class grows and is increasingly adopted, the U.S. government must do their best to root out fraud, manipulation, and abusive practices. Governments that have already embraced blockchain analysis have seized millions of dollars in cryptocurrency and stopped a number of illicit actors exploiting cryptocurrency. Many government agencies, including the CFTC, have limited or inconsistent personnel dedicated to investigating the illicit use of cryptocurrency because of a lack of training resources and a lack of funding for new personnel, tools, and training. Allocating appropriate financial and personnel resources to these efforts would ensure that agencies can address illicit activity in this space.

Leverage the unique and transparent nature of cryptocurrency in market surveillance and in the development of policies and regulations.

The information that is available to government agencies due to the transparent nature of blockchain technology provides an opportunity for policy makers and regulators to think differently about regulatory requirements in this space. For example, regulators can leverage this data to gain insights into the ecosystem and inform where the greatest risks are as they build their capacity to provide market surveillance. This will allow them to prioritize regulatory requirements that fill in information gaps. For example, reporting requirements may be different in this space given the on-chain data made available to regulators because of the transparent nature of the technology. It may not be necessary to require the same level of reporting because of the ease of availability of that on-chain data. Instead, regulators can focus reporting requirements on the parts of the market where there may be incomplete data or other gaps.

Understand and monitor systemic risks in the cryptocurrency ecosystem.

Regulators need to understand and monitor systemic risks in the whole cryptocurrency ecosystem—not just those market participants they have oversight of—to better understand the contagion risks that may be present. For example, it is important that regulators understand DeFi and DeFi products to understand the potential contagion risks. Understanding the broader market structures will better enable market surveillance and inform regulatory decisions.

Prioritize public education to ensure consumers understand cryptocurrencies and have the information they need to make educated decisions.

As with any new asset class, there is sometimes confusion among the general public about what cryptocurrencies are and how they work. It is important that the U.S. government engage in educational efforts related to cryptocurrency to better enable consumers to understand this asset class and avoid scams and fraudulent activity in the cryptocurrency ecosystem. The CFTC and others should consider partnering with the private-sector in addition to conducting agency—lead initiatives to broaden the access, breadth, and depth of public education and ensure its impact.

Leverage public-private partnerships.

It is important that the U.S. Government work together with private industry to address issues related to fraud, abuse, and manipulation in the cryptocurrency ecosystem. Establishing and improving upon coordination and collaboration mechanisms between countries can help to streamline investigations and improve oversight of the markets. These partnerships can provide additional insights into what is happening in the market to better inform policy decisions and guide discussions about how best to improve regulation.

Conclusion

Cryptocurrency has a variety of applications which contribute to the public good. Of particular interest to this Committee these contributions include job creation, fast cross-border payments, global leadership opportunities, and technological innovation. The U.S. is well-positioned to bring to bear our decades of innovation in cutting-edge technologies to this fast growing industry and be a key player in regulating the industry. As regulators approach this new asset class, they can leverage its technology and transparency to glean important insights and assess risks. Congress must do its part to ensure that the government agencies charged with oversight of this space are equipped to understand and address fraud, abuse, and manipulation in cryptocurrency markets. By providing the resources necessary, the U.S. government as a whole will be better equipped to mitigate risks and investigate and disrupt illicit activity when it does occur in the cryptocurrency markets. Thank you for your time, and attention to this very important issue.

The CHAIRMAN. I thank the gentleman.

Chainalysis rolls right off the tongue. Thank you, sir.

Mr. Hoskinson, you may proceed.

STATEMENT OF CHARLES HOSKINSON, CHIEF EXECUTIVE OFFICER, INPUT OUTPUT GLOBAL, INC., SINGAPORE, SG

Mr. HOSKINSON. Hi, everybody. Chairman Maloney, Ranking Member Fischbach, Members of the Subcommittee, and Congressional staffers who work so hard, thank you for inviting me to testify at this hearing. I applaud the work of this Subcommittee, and I appreciate you all taking the time to provide a forum for the blockchain industry.

The blockchain industry has grown over the past decade from a small group of uncommercialized volunteer developers—and it was very small, believe me—to a trillion dollar global economy encapsulating sophisticated engineering, scientific research, publicly traded companies, and millions of users.

While our remarkable growth yields significant opportunities ranging from infrastructure security to entirely new economies like metaverses and NFTs, it also has presented new challenges and amplified the existing problems. Our legacy systems cannot handle the rapid movement of value without counterparty risk and require centralized middlemen. Our regulatory tools, risk management systems, and oversight processes were never designed for such speed, scale, and rapid evolution. For example, in just 4 years, our industry has touched concepts ranging from IPOs to intellectual property to completely new business structures called DOWs that are effectively leaderless and jurisdiction free.

Reflecting upon the 20th century, the dominance of the United States has rested upon three pillars: our financial services, our technology companies, and our manufacturing capabilities. These industries are rapidly transforming under the demands of globalization, increased competition, new technologies, and our desire to define ESG rules to ensure a sustainable, values driven global economy. At our core, our industries technology is about creating distributive ledgers to store information that needs to be transparent, auditable, time-stamped, and immutable. This process enables records of social and economic concerns to be reliable and programmable.

For example, as a rancher, I have to deal with water rights, grazing leases, BLM land, and numerous other agreements, contracts, and economic events. Many of these are not digitized, nor are they

shared in ways to provide emergent value to policymakers, regulators, and researchers. The consequences of this fragmentation and lack of digitization are a large amount of inefficiency, replication of work, and a lack of access for entrepreneurs and innovators who could build new products and services that would dramatically reduce costs and improve efficiency for all stakeholders. The power of blockchain technology is its universality and permissionless model for innovation. Our company, Input Output, has never had to pay a royalty, file a patent application, or acquire a license to pursue business in countries as diverse as Ethiopia to Mongolia. Thus, we have to understand that categories-based regulation that is segregated to the borders of a particular jurisdiction and relies upon centralized actors for reporting a disclosure is unlikely to be effective, and frankly, will inhibit regulation.

Furthermore, the internet's governance, evolution, and innovation are not controlled by the ITU or some other transnational body, but rather, by thousands of interconnected and interdependent agencies and private companies working towards the self-emerging common goals of increased connectivity, capacity, and utility.

If we are to discuss how to regulate our industry, protect consumers, and align growth with the realities of modern society, then we ought to have the humility to admit innovation makes specifics difficult. We should focus on principles instead.

Blockchains enable the liquidity of value, thought and commerce at a scale and speed society has never enjoyed before. Instead of predicting the outcome of these new capabilities, we ought to decide on what risks we must guard against, what fundamental rights consumers should have, and how to use new tools for the greatest possible good. It seems prudent to focus on concepts like measuring decentralization, information asymmetries, accessibility of data, and access rather than arguing about jurisdictional bodies or asset categorization. Cryptocurrencies are financial stem cells at their core. They can be nearly any asset and can change over time. Principles don't change.

For example, the notion of measuring consolidation and its risks has been an endeavor the United States has pursued and is, frankly, good at since the Sherman Anti-trust Act of 1890.* While none of us are personally familiar with life in the 1890s, we would certainly be comfortable with the intent and concepts behind the Sherman Antitrust Act. Centralization of markets and power seldom leads to good outcomes. I hope we can engage in a fruitful and ongoing dialogue throughout the coming months as the United States debates the regulatory future of the American blockchain and cryptocurrency industry. Like the prior Congresses in the 1990s discussing the regulatory framework for the internet that led to the rise of trillion dollar companies, I believe this Congress can achieve great results by working with our industry at a principles-based legislative approach, and leveraging our capabilities to innovate and adapt.

Thank you all for your time, and I look forward to your questions.

---

*__Editor's note:__ Enacted July 2, 1890; 26 Stat. 209, Public Law No. 51–109.

[The prepared statement of Mr. Hoskinson follows:]

PREPARED STATEMENT OF CHARLES HOSKINSON, CHIEF EXECUTIVE OFFICER, INPUT OUTPUT GLOBAL, INC., SINGAPORE, SG

I. Introduction

Chairman Maloney, Ranking Member [Fischbach], Members of the Subcommittee and distinguished guests, thank you for inviting me to testify at this hearing. My name is Charles Hoskinson and I sincerely applaud the work of this Subcommittee and appreciate you all taking the time to provide a forum for the blockchain industry. I am pleased to provide you with as much information as you need in order to ensure a fully informed and robust conversation on the future of digital asset regulation.

II. Background on Input Output Global

I am one of the founders of the Ethereum blockchain, founder of the Cardano blockchain and CEO of Input Output Global (IOG), which is a research and engineering company focused on the development of blockchain and other cutting-edge technologies. IOG is an American company that has helped to build the Cardano blockchain as well as other products on top of the blockchain such as Atala Prism,[1] a blockchain-based self-sovereign identity solution that provides digital identity to individuals and Lace light wallet,[2] a digital portal that provides individuals access to a variety of financial services. IOG's research team has published more than 140 academic research papers relating to blockchain technology and has relationships with academic institutions such as the University of Wyoming, Carnegie Mellon University, Stanford University and the University of Edinburgh. Beyond the United States, the company is working across Africa (particularly in Ethiopia, Tanzania, Kenya and Burundi) to help expand broadband service in rural areas, increase financial inclusion through microfinance and lending marketplaces and provide students and teachers with digital identities and verifiable credentials—all on the Cardano blockchain.

III. Using Blockchain Technology to Solve Real-World Problems

Distributed ledgers (*i.e.,* blockchains) store information that needs to be transparent, auditable, timestamped, and immutable. This process enables records of social and economic concerns to be reliable and programmable.

Public blockchains, just like many commodities, are intrinsically decentralized and permissionless. For example, I grow hay on my farm in Colorado. I did not ask for permission to plant and harvest my hay, and now I am a member of a global, dynamic marketplace. There are regulations and controls in all of these markets, but we do not assume there is a centralized hay agency to ensure somehow this market works. Such absurdities were reserved for the Soviet central planners of old, not modern economies. Blockchain projects operate and embody this decentralized ethos and would fail under the weight of a heavy-handed and outdated regulatory structure.

As a rancher, I have to deal with water rights, grazing leases, public land authorities, and numerous other agreements, covenants, and economic events. The management and oversight of much of these activities are not digitized, nor are they shared in ways to provide emergent value to policymakers, regulators, and researchers. When these activities are conducted and managed, and the resulting information is shared, on a blockchain they are transparent and auditable.

Looking, for example, at the beef industry, blockchain technology can be used in many ways including creating significant value for the industry's end-to-end supply chain and more over sustainability and safety, such as grass-fed assurance, trade finance, consumer engagement, consumer feedback, certification and end-to-end traceability. With regards to traceability, BeefChain is a blockchain startup that allows consumers to trace their beef product. BeefChain is built on the Cardano blockchain and utilizes IOG's Atala Trace solution. In 2019 the company achieved USDA Certification with the Process Verified Program.[3] This means that certain characteristics, such as being hormone free, are treated as audited and certified in line with U.S. food safety regulations. By enabling unique animal identification and ensuring origin, BeefChain allows the rancher to receive premium pricing for premium beef and provides consumers with greater confidence in the meat they consume. Digitizing animal branding rules and procedures, such as those in Wyoming,

[1] *https://atalaprism.io/*.
[2] *https://www.lace.io/*.
[3] *https://www.ledgerinsights.com/proof-of-steak-blockchain-food-beef-traceability/*.

could save thousands of hours waiting for inspectors, speed up livestock sales, and enable more data collection for supply chain management scored against environmental and conservation goals. Livestock branding takes on a new meaning when a record of the event is immutably fixed in a blockchain.

As for some of the work that my company is doing, IOG is working with Ethiopia's Ministry of Education to create a blockchain-based digital identity and verifiable academic credentials for five million students and teachers in the country. The goal of this vital project is to enable data-driven policy-making and simultaneously allow students to prove their educational achievements internally and across borders to universities and the job market by reducing the risk of fraud. IOG's partnership with World Mobile [4] will lay the foundations for a totally connected Africa by utilizing the Cardano blockchain to help empower remote and hard to reach areas across the continent so that everyone gets an equal chance to access services and opportunities. World Mobile's mesh network model leveraging the Cardano blockchain enables scalable, shared infrastructure, security, transparency and self-sovereignty, which can lower the costs and barrier for people to access connectivity. The sharing economy gives every participant of the network a mutual stake in its success.

In Kenya and Ghana, in order to tackle the financing gap through an ecosystem of products that remove the frictions between crypto liquidity and real-world economic activities to offer cheaper financial products, IOG has partnered with Pezesha Africa Limited to facilitate loans to small and medium sized businesses looking for short term loans for working capital. The goal is to build simple friction-free tools that enable seamless lending.

Another use case here in America that I would like to highlight is a loyalty program powered by blockchain technology, which is currently being developed through a strategic collaboration between IOG and DISH Network Corporation.[5] The two companies are working to create a backend token-based loyalty system supported by the Cardano blockchain. Cardano tracks the balance of loyalty coins or Boostcoins™ accrued by customers, and mints or burns the loyalty tokens based on customer rewards and reward redemptions. The loyalty token balance is adjusted in a nightly batch operation, using a DISH-controlled digital wallet. IOG's Atala Prism is leveraged to ensure no personally identifiable customer information is included in the process. This first step of the collaboration enables blockchain capabilities in DISH's infrastructure through Atala PRISM's identity services and Cardano's native asset features allowing DISH to better serve and securely connect with its customers.

These use cases and projects exemplify the kind of economic development and growth that blockchain technology can bring to America, especially to rural and remote regions of the country.

IV. Principles for the Blockchain Industry

If we are to discuss how to regulate digital assets, protect consumers, and align growth with the realities of modern society, then we ought to have the humility to admit that innovation makes specifics difficult and thus focus on principles instead. Although the concept of freedom of speech is ever challenged by new technology, we can recognize that the constitutional notions of free speech remain the same. We have a desire to express ourselves in a free society without fear of government interference or retribution. What are the principles that should guide thinking coming out of the blockchain industry in its interaction with the U.S. Government?

Looking at another American creation, the internet, the governance, evolution, and innovation of the internet are not controlled by the International Telecommunication Union (ITU) or some other transnational body, but rather by thousands of interconnected and interdependent agencies and private companies working together towards the self-emerging common goals of increased connectivity, capacity, and utility. The United States embraced the public-private partnership that allowed the internet to flourish and for the United States to play and maintain a primary role in internet technology. Similarly, it will take many different agencies working together with the private sector to ensure the American blockchain industry flourishes and reaches its full potential.

Like the prior Congresses in the 1990s discussing the regulatory framework for the internet that led to the rise of trillion dollar companies, I believe this Congress can achieve great results by working with the blockchain industry towards a principles-based approach that leverages our countries' remarkable capabilities to innovate and adapt.

---

[4] *https://worldmobile.io/*.
[5] *https://www.dish.com/*.

It is of the utmost importance to acknowledge that category-based regulation, which is segregated to the borders of a particular jurisdiction and relies solely upon centralized actors for reporting and disclosure, is unlikely to be effective in a blockchain-based decentralized ecosystem and will inhibit innovation. Whereas, principles-based regulation, which is more flexible, can adapt and evolve alongside the nascent technology without strangling an industry that has only started and forcing companies abroad.

V. Values in Support of American Industry

Reflecting upon the 20th century, the dominance of the United States has rested upon three pillars: financial services, technology companies, and manufacturing capabilities. These industries are rapidly transforming under the demands of globalization, increased competition, new technologies, and the desire to define environmental, social governance (ESG) rules to ensure a sustainable, values-driven global economy. I believe that the blockchain industry is building the foundational technology that will enable trust, compliance, and competitiveness for these industries throughout the 21st century, thereby ensuring another American century.

Transparent, immutable, always objective ledgers—provided by blockchain technology—are phenomenal tools for record-keeping, reporting, and oversight. In other words, blockchain technology itself provides many of the tools that can be deployed for safeguarding consumers and protecting market integrity. The same concepts that protect a decentralized exchange from front running or security breaches can also be used by regtech companies like Chainalysis to provide unprecedented information to government agencies, regulators, economists, and financial engineers about an exchange. The collection of this data is permissionless and royalty-free. No more dark pools. No more centralized brokers.

The power of blockchain technology is its universality and permissionless model for innovation. True competition exists when everyone has equal access to markets. My company, Input Output Global, has never had to pay a royalty, file a patent application, or acquire a license to pursue blockchain-related business development in countries as diverse as Ethiopia to Mongolia. The same tools that would enable a rancher to register a brand could be reused for land deeds, a credit score, or issuing a non-fungible token (NFT) to represent a musical composition, assuring its artist of receiving fair compensation.

Blockchains enable the liquidity of value, thought, and commerce at a scale and speed society has never experienced before. Instead of predicting the outcome of these new capabilities, we ought to decide on what consumer and market risks we need to guard against, what fundamental rights consumers should have, and how to use these new tools for the greatest possible good. Compliance with regulation and legislation coming out of the United States must be a guiding value for the blockchain industry, nation and world, as speed of development without any control whatsoever will lead to rampant fraud, waste, and abuse.

VI. The Importance of Appropriate & Responsible Regulation

IOG, myself and many others in the industry are in favor of and support appropriate and responsible regulation of digital assets and blockchain technology. However, this is a new technology and a radically new asset class that can not readily fit within the confines of the laws and tests created almost a century ago.

Cryptocurrencies are financial stem cells—programmable software that can be nearly any asset and can change over time. In fact, no two cryptocurrencies are alike and the uses, functions and features of cryptocurrencies can vary depending on who is holding the cryptocurrency, why and where. Cryptocurrency can be used to verify data, transfer information or value, purchase goods, provide access to services, serve as a reward or membership program, act as a store of value or as an investment, all at the same time or at different times over the life of the cryptocurrency.

The United States legislature has never tried to regulate something that could be so many different things at the same time. Yes, some cryptocurrencies may be securities, some may be commodities, some may be both, but many may not be either. Regardless of how a cryptocurrency is labeled, three things should be kept in mind: (i) the existing U.S. regulatory regimes never contemplated such an asset, (ii) without cryptocurrencies, most blockchain technologies simply will not function and (iii) any regulatory goals should be to promote appropriate consumer protections and assure market integrity. The last can be achieved through regulatory approaches that do not necessarily require labeling a cryptocurrency as either a security or commodity.

U.S. securities laws achieve investor and market protections based on the assumption that there is and will always be a centralized entity (*e.g.,* a corporation

who is identifiable and can permanently assume the role of providing financial and other data to the holders of its equity). Some blockchain technologies, and thus cryptocurrencies may initially be created or backed by a somewhat centralized entity similar to a corporation but many times that is not the case and over time, virtually all cryptocurrencies and blockchains exist without any centralized entity that can be identified as the party supporting such technology. The existing laws and regulations that assume the existence of such centralized and responsible parties simply and logically cannot work in the case of blockchain technology and the cryptocurrencies that drive such technologies.

Responsible regulation should start with an understanding as to the critical role blockchain technologies can play for assuring American competitiveness, America's security, particularly digital infrastructure, financial inclusion for Americans and promotion of economic development and growth.

VII. Conclusion

Cryptocurrencies and the broader blockchain industry, which relies on cryptocurrencies to operate and function, have grown over the past decade from a small group of uncommercialized, volunteer developers to a trillion dollar, global ecosystem encapsulating sophisticated engineering, scientific research, publicly traded companies and tens of millions of people using these technologies throughout the world.

The great growth of blockchain technology rivals only the internet and arguably yields more significant opportunities ranging from cheaper and more efficient payment systems, cryptographically enhanced infrastructure security, new forms of governance, self-sovereign identity and so much more. However, this new technology has also presented new challenges and amplified the existing problems of many legacy systems. The instantaneous movement of information and value without counterpart risk nor the need for centralized middlemen combined with reducing complex business processes and structures to open source software that can be rapidly upgraded means that commercial activity can now proceed at the speed of thought on a global scale.

I am grateful to have the opportunity to present these real-world use cases, my opinions on the guiding values of the industry and thoughts regarding the promise of the blockchain industry. My knowledge and network are always available to this Subcommittee to aid and assist in the legislative process. In conclusion, I hope we can engage in a fruitful and ongoing dialogue throughout the coming months as the United States debates the regulatory future of the American Blockchain and Cryptocurrency industry. I sincerely appreciate your time and look forward to your questions.

ATTACHMENT 1

SoK: Blockchain Governance

Aggelos Kiayias
University of Edinburgh, IOHK
United Kingdom
aggelos.kiayias@ed.ac.uk

Philip Lazos
IOHK
United Kingdom
philip.lazos@iohk.io

ABSTRACT

Blockchain systems come with a promise of decentralization that, more often than not, stumbles on a roadblock when key decisions about modifying the software codebase need to be made. In a setting where "code-is-law," modifying the code can be a controversial process, frustrating to system stakeholders, and, most crucially, highly disruptive for the underlying systems. This is attested by the fact that both of the two major cryptocurrencies, Bitcoin and Ethereum, have undergone "hard forks" that resulted in the creation of alternative systems which divided engineering teams, computational resources, and duplicated digital assets creating confusion for the wider community and opportunities for fraudulent activities. The above events, and numerous other similar ones, underscore the importance of Blockchain governance, namely the set of processes that blockchain platforms utilize in order to perform decision-making and converge to a widely accepted direction for the system to evolve. While a rich topic of study in other areas, including social choice theory and electronic voting for public office elections, governance of blockchain platforms is lacking a well established set of methods and practices that are adopted industry wide. Instead, different systems adopt approaches of a variable level of sophistication and degree of integration within the platform and its functionality. This makes the topic of blockchain governance a fertile domain for a thorough systematization that we undertake in this work.

Our methodology starts by distilling a comprehensive array of properties for sound governance systems drawn from academic sources as well as grey literature of election systems and blockchain white papers. These are divided into seven categories, suffrage, Pareto efficiency, confidentiality, verifiability, accountability, sustainability and liveness that capture the whole spectrum of desiderata of governance systems. We interpret these properties in the context of blockchain platforms and proceed to classify ten blockchain systems whose governance processes are sufficiently well documented in system white papers, or it can be inferred by publicly available information and software. While all the identified properties are satisfied, even partially, by at least one system, we observe that there exists no system that satisfies most properties. Our work lays out a common foundation for assessing governance processes in blockchain systems and while it highlights shortcomings and deficiencies in currently deployed systems, it can also be a catalyst for improving these processes to the highest possible standard with appropriate trade-offs, something direly needed for blockchain platforms to operate effectively in the long term.

1 INTRODUCTION

Following the founding of Bitcoin [1] in 2009, cryptocurrencies and other blockchain platforms have tremendously risen in popularity. Unlike centralised organisations, which are governed by a select few, blockchain platforms operate in a decentralised fashion by the different actors in these platforms. The decentralised nature of blockchains has been essential to their appeal; however, it has also introduced new challenges. Blockchain platforms, like other organisations, try to adapt and adjust to their stakeholders' needs and preferences. With different actors present whose preferences might not always align, governance problems arise and the risk of division between their community members increases.

Different governing mechanisms exist, depending on the platform. Off-chain governance is the most centralised of such mechanisms with the core developers or the most trusted contributors making most of the decisions. On-chain governance is achieved via on-chain voting mechanisms, which can be more transparent and inclusive than off-chain governance. In both of these mechanisms, community division can take place when a backward-incompatible update is adopted, where some stakeholders choose to stay on the original chain and others choose to upgrade to the updated chain, dividing the community into two. Alternatively, two or more competing updates may be proposed dividing the community about their potential merits. Eventually, consensus can fail and different segments of the community adopt the update that they believe to be the most beneficial.

In the most general sense, such deviations are known as hard forks and numerous examples of them have been observed in popular cryptocurrencies. Two notable examples are the split of the Ethereum chain to Etheurem and Ethereum Classic due to the the DAO debacle [2] and the split of the Bitcoin system into Bitcoin and Bitcoin Cash over the debate around block size and the SegWit upgrade. Such divisions can fragment the community and its resources, and as a result reduce the overall value of the platform as well as its security. The latter consideration can be quite tangible as the reduced number of resources supporting a fork can lead to attacks. Such attacks are referred to as 51% attacks and have occurred on a number of occasions, e.g., see the case of Ethereum Classic [3] for a notable such instance.

The above issues highlight the importance of sound blockchain governance, the ability of a blockchain platform community members to express their will effectively regarding the future evolution of the platform as well as the best possible utilization of its resources. So this brings forth the question what characterizes proper governance in blockchain systems? This fundamental question motivates the systematization effort we undertake in this paper.

Our methodology is first to derive a set of properties, that are drawn from general governance principles and election theory and then interpret them to the blockchain governance setting. We use a variety of sources to ensure the comprehensiveness of our property list that include the Council of Europe technical standards for e-voting [4], the Federal Election Commission's Voting Systems Standards [5], but also blockchain specific ones such as [6–8]. Given the set of properties, we then evaluate a wide array of blockchain

platforms against those properties revealing each platform's unique strengths and weaknesses.

We distill seven fundamental properties for blockchain governance. The properties capture different aspects of important requirements for governance. The first property deals with participation eligibility; Decision making systems can produce legitimate outcomes provided they are inclusive — a property that we capture by different aspects of *Suffrage* suitably adapted to the blockchain setting. Suffrage determines a set of "decision-makers" who are a subset of the community of a blockchain project. The second property has to do with the *Confidentiality* of the decision-makers' inputs; it further specializes to Privacy, which asks for maintaining the input private while Coercion Resistance asks for the input to be free of any external influences. The third property —*Verifiability*— asks for decision-makers to be able to verify their input has been taken into account in the output and that such output is correctly computed. These last two properties are in a sense "classical" security properties. Next we move to two properties that have to do with the incentives of the decision-makers. *Accountability* asks for decision-makers to be held accountable for the input they provide to the system, while *Sustainability* asks whether appropriate incentives are provided for the system to evolve constructively and to the decision-makers for providing meaningful input. We then move to a social choice consideration. *Pareto efficiency* asks that, given all decision-makers' preferences, the outcome of the governance process cannot be strictly improved vis-à-vis these preferences. Finally, the crucial ability of the system to produce outputs expediently is captured by *Liveness*.

Armed with the above comprehensive list of governance properties we investigate a number of popular blockchain platforms which provide some sort of governance functionality and we detail the way they satisfy (or fail to satisfy) each of the given properties. Our results dictate that while each of the properties is considered in the context of at least one system, there exists no platform that satisfies most of the properties.

1.1 Related Work

As of the time of writing, there is yet to be a formal or rigorous coverage of good blockchain governance properties. However, the topic of blockchain governance has received coverage in multiple disciplines. Given their diversity, additional related work is also presented in context within each subsection of Section 2, where each governance property is defined. Pelt et al. [9] adapt the definition of OSS (open-source software) governance to blockchain governance; they then go on to derive six dimensions and three layers of blockchain governance from the literature to build a framework, which can be used as a starting point for discussion in new blockchain projects. Similarily Beck et al. [10] derive three key dimensions of blockchain governance to define an IT governance definition. De Filippi and McMullen [11] investigate the social and technical governance of Bitcoin, making a distinction between two coordination mechanisms: governance by the infrastructure (via the protocol) and governance of the infrastructure (by the community of developers and other stakeholders). Corporate governance has been drawn from in the literature to examine the governance of public blockchains. The work done by Hsieh et al. [12] and Allen and Berg [13] are such examples, where the authors of the latter work derive a definition of blockchain governance and make a distinction between endogenous and exogenous governance. Given the variety of actors and strategies in the decision-making processes in blockchain platforms, Khan et al. [14] view blockchain governance from the lens of IT governance and then analyse decision-making processes in the form of voting on a new blockchain improvement proposal, by using Nash equilibria to predict optimal governance strategies. Certain forms of blockchain governance, like traditional forms of governance, have the short-coming of participants not able to change their vote between two consecutive elections or votes. Venugopalan and Homoliak [15] address this shortcoming, among others, by introducing an always-on-voting (AoV): a repetitive blockchain-based voting framework that allows participants to continuously vote and change elected candidates or policies without having to wait for the next election. More specific analysis on certain aspects of blockchain decision-making processes also exist in the literature (e.g. Gersbach et al. [16] where the authors analyse delegated voting and conclude caution should be exercised when implementing such mechanisms).

2 BLOCKCHAIN GOVERNANCE PROPERTIES

One of the main contributions of our work is systematizing the properties pertinent to blockchain governance systems. We would like to stress that there is no *single set* that optimally captures every aspect. There are trade-offs between satisfying some properties to a high degree and others to a lesser degree. In addition, many current implementations do not have rigorously defined governance mechanisms for every use case and usually contain a mixture of formal on-chain features as well as informal off-chain ones. This is almost inevitable, as different blockchains are built for specific purposes and not all decision-making processes can be sufficiently captured by a smart contract or special purpose protocol logic. Others might still be centralized or transitioning to full decentralization. Irrespective of this, our property systematization focuses on *first principles* and is meaningful across the board, independently of the underlying set of mechanisms that are set in place to facilitate decision-making in each blockchain platform.

We can categorize the properties into four broad classes pictorially shown in Figure 1. The first class contains properties about the *voting system* that is used for decision-making. It will touch the issues of who is eligible to participate and what is the process that combines the inputs provided. The voting system enables us to argue about the governance process in an ideal, philosophical sense; questions such as who has the right to vote are relevant here. The remaining three classes deal with the way an ideal voting system can be implemented and touch three important domains: *security* which deals with cryptographic and cyber-security aspects, *incentives* which deals with game-theoretic and economics aspects, and *timeliness* which deals with issues of time and expediency. Failures in the properties of these classes can have important repercussions for the legitimacy of the governance process. Even though the voting system might be acceptable in a 'Platonic' ideal sense, failures in the remaining properties can suggest that certain community members are disenfranchised because it is harder for them to participate, or they cannot express their will freely or even that they

have no ability to properly form an opinion due to lack of proper incentivization. It is also worth adding that *usability* permeates these three implementation related classes, but it will be outside of scope of our systematization.

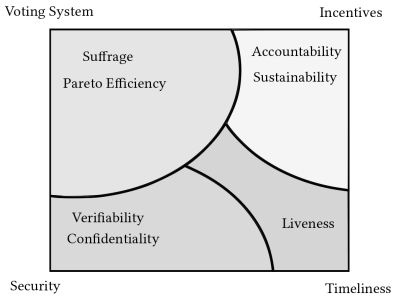


Figure 1: The partition map of governance properties.

An important aspect of our property systematization is that we emphasize fundamental properties entirely decoupling them from any specific techniques, algorithms or mechanisms that facilitate them. To illustrate the point, a simple example is the distinction between the property of having privacy (or secrecy) and the cryptographic protocol techniques that may be used to achieve it. Another example is quadratic voting, which is a technique where additional votes can be 'bought' (using actual money, voting credit, etc.) but the cost scales quadratically with the number of votes. Even though it has received renewed interest in blockchain governance, particularly for participatory budgeting applications,[1] it should be clear it is still just a *mechanism*, not a fundamental property per se; we revisit it in some more detail when we discuss Suffrage below as it is one of our basic properties that is most related.

Further to this point, whether a particular governance mechanism is on-chain, off-chain, uses a foundation etc. is a *mechanism*, **not** a property. These inner workings will not be part of our classification explicitly, unless they affect some fundamental property.

We want to stress that satisfying all properties to some higher or lower degree, as feasible, would not make a blockchain governance system perfect. There are many blockchains applications and each of them has different needs and use cases that would require community involvement. Some properties might be incompatible with each other. Our thesis though is that any design would have to *consider* how each property is addressed and ensure that the the choices made are deliberate. As such, during the evaluation of different governance systems we will make sure that each property is judged *in context*, taking the goals of each system into account.

[1] Such as Gitcoin quadratic funding, https://gitcoin.co/blog/gitcoin-grants-quadratic-funding-for-the-world/

2.1 Suffrage

One of the first considerations of any governance system is determining who is granted *suffrage*, which is the right to participate in decision making procedures. This can be distinguished in *active* suffrage, the right to vote, and *passive* suffrage, which is the right to stand for election and become an elected representative. Suffrage, an already a complicated and nuanced property, is even more so when applied to blockchain systems.

In national or regional elections, it is often the case that the voting mechanism implements a 'one person, one vote' rule. Different jurisdictions use different criteria in guaranteeing the right to vote to individuals, but the bottom line is that one person can only submit one vote. Although research is currently underway on proof-of-personhood systems [17], which verify that accounts correspond to unique individuals, the 'one person, one vote' rule is not applicable to most, if not any, current blockchain platforms. Instead, we often see that a minimum amount of stake or hashing power is required to guarantee a vote. We also see platforms where only the founders or core developers are guaranteed a vote. In any case, these are attempts to define and reconcile two groups of people: the set of community-members C and decision-makers D.

Definition 1. *The community-members C of a blockchain system are people that have* direct *interaction with it. This may be by providing resources in service of its security or consensus protocol, owning tokens, develop software etc.*

Definition 2. *The decision-makers $D \subseteq C$ of a blockchain system are the people that participate in (any way) its governance.*

Given these definitions, we establish the basic ways that community-members are granted voting rights in the blockchain space. The voting rights should more accurately be called voting *weights*, as it is very common to allocate a different number of votes across all community-members.

Definition 3 (Type 1: Identity-Based Suffrage). *A blockchain governance system satisfies this property if it guarantees decision-making rights to participants who are able to prove their identities such that the votes correspond to unique individual humans.*

Contrary to the usual notion of community-membership, identity alone is not (so far) a robust enough connection between users and blockchains. Also, there is no restriction against switching to different blockchains or having direct interactions with many of them. The following notions of suffrage are based on a more 'quantifiable' approach and typically assign voting power accordingly.

Definition 4 (Type 2: Token-Based Suffrage). *A blockchain governance system satisfies this property if it guarantees decision-making rights to participants who have certain tokens in the platform or a minimum amount of tokens in the platform.*

Definition 5 (Type 3: Mining-Based Suffrage). *A blockchain governance system satisfies this property if it guarantees decision-making rights to participants who have a certain amount of hashing power in the platform (or other physical resource relevant to the platform, e.g., disk storage).*

In the PoS setting, voting weight is often measured by an operator's stake (or wealth). This can result in the following undesirable

situations: **(i)** participants who may be more enthusiastic about the platform have lower voting weight than those who are less enthusiastic about the platform, and **(ii)** participants who may have contributed more to the platform may have lower voting weight than those who contributed less. Methods like quadratic voting [18] can help dampen the effects of stake-based voting weight (see below for an explanation), but it does not address the root of the problem: voting weight is ultimately based on wealth owned or even managed (e.g., centralized cryptocurrency exchanges may control a significant amount of stake that does not belong to them). Similar issues exist in the PoW setting, where hashing power may not proportionately reflect stakeholder contributions to the platform. Analysis in quantifying decentralisation [19] on blockchain platforms, in terms of stake and hashing power, can provide insights into resultant power concentrations.

Remark (Governance Tokens). *Often, tokens used to determine suffrage can have more than one use (e.g., native currency of a proof-of-stake system). However, particularly for the governance of smart contract based protocols, specific* governance *tokens can be used, who have no other direct functionality or value (such as paying for transaction fees or appearing as block rewards) other than enabling participation. Especially when these tokens are transferable, special care is needed to ensure that their supply, distribution and price accurately represents the community members who are more invested in the project. This was observed in the recent Beanstalk exploit, where an attacker used a flash loan to obtain a majority of governance tokens, passing his own malicious proposal and quickly implementing it. The voting mechanism worked well: but clearly, the voting weights did not accurately reflect the community. To avoid such attacks, other platforms such as Compound employ more fail-safes, such as a mandatory waiting period before enacting the election result.*

Instead of assuming that community-members would have an implied incentive to positively contribute to their respective blockchain's governance, sometimes a more direct approach is taken. Participants are granted a decision-making right based on whether they have positively contributed to the platform. What defines a 'positive' contribution is not always clear cut and its definition is left to the platform's community.

Definition 6 (Type 4: Meritocratic Suffrage). *A blockchain governance system satisfies this property if it only guarantees decision-making rights to participants who have positively contributed to the platform.*

Definition 7 (Type 5: Universal Suffrage). *A blockchain governance system satisfies this property if it guarantees decision-making rights to participants who have mining power or tokens in the platform as well as participants with positive contributions to the platform.*

We reiterate that it is not our objective to outline specific mechanisms for translating community-membership to voting power. For example, we are not suggesting that an actor's voting weight should be more influenced by previous contributions than by an actor's stake in the platform. Instead, we are suggesting that it is important that all forms of investments and contributions of a community-member (which can be very different across different blockchains) should be considered when formulating voting weight.

In this context, a mechanism that has gained traction recently in the blockchain context is quadratic voting. In this mechanism, 1 vote would cost 1, but 2 votes would cost 4 and so on. Such a mechanism could achieve a better balance between what *Token-Based Suffrage* and *Identity-Based Suffrage*: having additional currency within the system does entail enhanced voting rights, but some balancing effect vis-à-vis the one-person one-vote rule seems appropriate. It also provides a more flexible way of expressing voter preferences. To see this, suppose that, in a governance system where votes can be exchanged for tokens, two voters believe that one vote in favour of some proposal is worth 5 and 10 respectively. By this, we mean that the voters believe investing 1 coin for a vote, would yield a return on investment of 4 and 9 respectively. In the final election, if the first voter is richer they could purchase 100 votes, while the second only buys 3. This would signal that the first voter is particularly in favour of this proposal, but in fact they bought more votes just because they had a higher budget to spare. With quadratic voting, the first voter would acquire 2 votes: the next vote would cost 4, which is not seen as a profitable investment.

2.2 Pareto Efficiency

Any blockchain governance system will necessarily depend on a number of decision-making procedures: individual, competing preferences have to be collected and combined into specific actions. In this section we try to formalize how well the tools provided by blockchain allow the *decision-makers* (recall Definition 2) to reach their most favourable outcome. Ideally, the result would the same as one chosen by an omniscient algorithm that has collected all their private thoughts and magically chose the 'perfect' outcome. As we will see, even the notion of a 'perfect' outcome is hard to define (and under most definitions, does not always exist). We stress that this might be *terrible* for the community-members of the blockchain; in this section we only focus on how well the intentions of the decision-makers can be turned into actions. Aligning the intentions of the community-members and decision-makers is a question of suffrage (as well as *Accountability*, which we define in Section 2.5).

The investigation of such decion-making processes is the focus of Social Choice Theory [20], which is an entire field of study dedicated to them. One of its crowning early achievements is the famous Arrow's Impossibility Theorem (Arrow [21]), on voting systems where participants *rank* the possible candidates. Specifically, given a set of alternatives $A = \{a_1, a_2, \ldots, a_n\}$, each voter i submits an ordered vector of the form $a_{i_1} \succ a_{i_2} \succ \ldots \succ a_{i_n}$. Combining the votes should lead to an outcome preference ordering $a_{j_1} \succ a_{j_2} \succ \ldots \succ a_{j_n}$ of the candidates that best represents the voters. Unfortunately Arrow's Theorem states that the following natural properties cannot be satisfied at the same time:

- If every voter prefers candidate X over Y, then X is ranked higher than Y in the final outcome. This property is often called *unanimity*.
- The order of X and Y in the final outcome depends only on the ordering of X and Y in each voters preference, irrespective of how all other candidates are ordered. This is called *independence of irrelevant alternatives*.
- There is no voter who has dictatorial control over the final outcome.

Variations of this result have been adapted in many voting settings, even in cases where the voting process does not have to reveal an entire ordering of outcomes (but only to select the 'best' one) or when voters have *cardinal* preferences (i.e. they can assign numerical preference values to each candidate). Note that almost all popular voting schemes (such as *approval voting*, where each voter selects a set of acceptable candidates) fall under these definitions. Perhaps the most famous of those impossibility results is the Gibbard-Satterthwaite Theorem (Gibbard [22], Satterthwaite [23]), roughly stating that any voting scenario with more than two candidates is either dictatorial, or subject to *strategic voting* (i.e., voters swaying the outcome by misreporting their actual preferences.

To deal with these impossibilities, the voting procedures used in practice are not required to be optimal in every scenario, but to satisfy certain weaker properties depending on the setting. One such mild property is *Pareto efficiency* (e.g., [24, 25]). These properties are tested assuming every voter truthfully reports their preferences.

Definition 8. *A blockchain governance system is Pareto efficient if whenever a decision-making process is held, alternative X cannot win if there exists another alternative Y that is preferred by at least one participant and no participant prefers X over Y.*

A Pareto efficient governance system would never lead to an outcome that is *clearly* worse than another possible outcome. This property should typically be satisfied (at least when interpreted loosely, as some blockchain systems do not have an entirely rigorous governance model), unless there is good reason not to. Evaluating whether this property is satisfied can be tricky because a blockchain governance system contains many interacting components, with the final result seldom depending on a single vote. We make our best effort to fairly evaluate how *likely* it is that a Pareto efficient outcome is not selected and *how* much worse is the selected alternative.

Approval voting is of particular importance, as it is the most common voting mechanism used by the blockchains we evaluate. Given n candidates, each voter can 'approve' as many as they want. The winner is the candidate which was approved by most voters, often combined with a threshold, such as also requiring approval from at least 20% of them. Notice that even though the voters might have ordinal or cardinal preferences, they can only submit a binary signal for each candidate. Starting with a simple example, suppose that 2 possible *incompatible* blockchain updates a and b are up for election. Furthermore, suppose that *every* voter prefers $a \succ b$. The outcome will be dictated by the threshold they chose when *converting* their ordinal preferences to an approval vote. Typically we would expect a to win, but b could win as well! Clearly, any truthful voter who approved b would also approve a, since $a \succ b$ for every voter. However, some voters might chose *not* to approve either of them. In this case b could win because of a tie. In fact, this is the only way an outcome of approval voting might not be Pareto efficient: if the winner is tied with the Pareto optimal candidate. This happened because the voters where completely uniformed about the preferences of each other and set their 'approval threshold' too high. The more information they have the less likely such an outcome becomes. A group of perfectly rational and informed voters would always produce a Pareto efficient outcome. In addition, it is important to keep in mind that there are two more 'secret' (implicit) options always available: to do *nothing* or to *fork*, which is to be avoided. When combined with a minimum approval threshold and some awareness on the part of the voters, the winner is most likely either Pareto efficient, a suboptimal yet highly popular alternative or a deadlock. Finally, strategic voting involves setting the threshold very high, which decreases the total number of votes and could lead to a deadlock, but is unlikely to result in a fork.

We briefly discuss an alternative voting system that uses the complete *ordinal* preference profile called *instant-runoff* (IRV) voting. It proceeds in turns:

- From every ballot, only the top preference is counted.
- If one candidate obtains a majority, they win.
- Otherwise, the least popular top preference is deleted from all ballots and the process repeats.

IRV is also not Pareto efficient as a good candidate might be deleted early, if they fail to win many first choice votes. It is however remarkably resistant to strategic voting [26] while retaining some properties that approval voting lacks, such as selecting the majority winner if one exists. This makes IRV particularly appealing when the community is asked to choose between alternatives in a non-binding way. The result can be further ratified by a referendum.

In some cases, IRV (and any voting system using ordinal preferences) might force the voters to inadvertently submit misleading information. For example, IRV assumes that the first and second place candidate on every ballot are separated by an equal amount, whereas some voters might be indifferent while others strongly in favour of their first choice only. Approval voting sometimes gets around this issue by asking for even less information. Ordinal preferences can be easily elicited by an *auction* which is undesirable for an election. A better alternative is to use an ordinal voting mechanism such as majority judgment [27] or combine approval voting with *token locking*: voters who feel strongly about some candidate may lock their vote tokens for longer, indicating that this election is particularly important to them.

2.3 Confidentiality

One of the initial goals of Bitcoin, as well as arguably the first design consideration when implementing a voting system on which the governance system will be based, is the approach to *privacy*. While its definition is fairly intuitive, we make a distinction between *secrecy* and *pseudonymity*.

Definition 9 (Type 1: Secrecy). *A blockchain governance system satisfies secrecy if whenever a decision-making process is held, an adversary cannot guess the input of any participant better than an adversarial algorithm whose only inputs are the overall tally and, if the adversary is a participant, the adversary's input.*

This definition follows from the early work of Benaloh, cf. [28] and has been formally modeled in numerous subsequent works, e.g., see the model of Juels et al. [29]. This is the strongest of the two notions and typically what would be required of an offline voting system (e.g., traditional elections in most countries). Often, true secrecy is difficult to accomplish in a decentralised setting or might be undesirable. For example, many blockchain combine on-chain governance with *off-chain* elements, such as discussions on forums. These discussions may be part of the formal governance model and

could be combined with an off-chain poll, based on the on-chain distribution of voting power. In these cases there could be a benefit in using *pseudonyms*, keeping the real life identity safe but tying their public discourse with their actual vote. This is particularly relevant when the distribution of voting power distribution. Even though not explicitly mentioned by name, the Bitcoin whitepaper provides an explanation about why *pseudonymity* [1] might be a good enough alternative.

Definition 10 (Type 2: Pseudonymity). *A blockchain governance system satisfies pseudonymity if no participant is required to reveal their real-life identity to participate in the decision-making processes.*

The reason for the development of this notion is that blockchain systems are usually designed with the assumption that consensus is achieved *only* with regards to the shared ledger; it is impossible to keep track of any information outside of it. Therefore, the same techniques used to keep track of the distribution of wealth (e.g., publicly announcing and linking transactions together), can be used to provide voting rights to the people actually involved in the blockchain without requiring much additional work. This is further related to the notion of *suffrage*, which is defined in Section 2.1. For example, in Proof-of-Stake based cryptocurrencies like Cardano, voting rights for some applications are distributed based on the amount of *stake* held by each user, as outlined in the paper by Zhang et al. [30] describing the voting system used by the treasury system of that platform. In practical terms, as long as the cryptographic information required when first producing one's online identity cannot be traced back to any real-life information, pseudonymity is satisfied. Privacy can be further strengthened, considering the notion of *coercion-resistance* [29, 31].

Definition 11. *A blockchain governance system satisfies coercion-resistance if whenever a decision-making process is held, a participant can deceive the adversary into thinking that they have behaved as instructed, when the participant has in fact made an input according to their own intentions.*

In a strict sense, this definition is arguably stronger than the guarantee provided by traditional elections: the voter should be able to deceive the adversary even about his participation, not just his vote. By definition, this exceeds the notion of privacy and requires at least one *anonymous* channel of communication. Such a scheme is described in [29], but tallying requires an amount of communication which is quadratic in the number of votes. As such, this property is typically too demanding to be fulfilled in a blockchain setting, for most applications. However, it can be partially satisfied (e.g., if a ballot is encrypted in a way such that the voter can verify its inclusion when it is cast, but it is impossible for him to reclaim it later, if asked to prove that they voted in some way — the fact that this only provides partial fulfillment of the property stems from the fact that if the participant's device leaks the random coins, then the ciphertext can be demonstrated to encode the participant's input).

2.4 Verifiability

To complement confidentiality, we now need a property that goes in the opposite direction, namely *verifiability*. This is a crucial property of every voting system, as it legitimises the election result. The widely accepted "golden standard" of verifiability is expressed below in the form of end-to-end verifiability.

Definition 12 (End-to-End Verifiability). *A blockchain governance system is verifiable if whenever a decision-making process takes place, participants are to able to verify their inputs were properly tallied and independent observers are able to verify that inputs from eligible participants were properly tallied.*

Furthermore, Gharadaghy and Volkamer [32] split the definition of verifiability into two separate notions.

- **Individual Verifiability:** It is possible for the voter to audit that his/her vote has been properly created (in general encrypted), stored, and tallied.
- **Universal Verifiability:** Everyone can audit the fact that only votes from eligible voters are stored in a ballot box, and that all stored votes are properly tallied.

At a high level, a system satisfying both properties would be called end-to-end verifiable – but we refer to [33] for more details on the notion of verifiability as well as the subtleties that arise in defining the concept formally.

Intuitively, satisfying privacy (and Definition 9 in particular) as well as coercion-resistance definition 11 should make verifiability more difficult to achieve. After all, these two limit the amount of information that a third-party could elicit by observing the blockchain. Despite this, it is indeed possible to achieve both to a certain adequate level. As exemplary schemes we can point to the work of [29] mentioned earlier, but also schemes such as the early work of Benaloh and Tuinstra [34], the Benaloh-challenge approach [35] that has influenced a lot of practical e-voting systems, see e.g., [36], or the hardware token based approach of [37]. This latter work also provides a comprehensive modeling of the concept of incoercibility that extends well beyond the setting of e-voting per se and can be immediately applicable to the blockchain setting as well.

2.5 Accountability

The quest for accountability in governance is not a recent pursuit, as it was clearly recognised by the ancient Egyptians and the ancient Greeks [38]. Since then, accountability as a concept has been split into multiple types and dimensions. For example, Grant and Keohane [39] outlines that accountability can take two general forms: vertical (where a party is accountable to other parties that are higher in a given hierarchy) and horizontal (where a party is accountable to other parties that are not higher or lower in a given hierarchy). Although *collective* accountability is often implicitly implied in coin-based voting, *individual* accountability is not. That is, if enough voters vote for a bad decision, the coin value of every voter declines whether or not they supported the decision. Individual accountability can take various forms, the most prominent of which is often referred to as 'skin in the game', where participants have an individual investment that will be directly affected by their individual actions.

Even though only the decision-makers take part in governance, accountability should capture the possible harm incurred to the community-members as well. This is an added layer of security required to align the incentives of these two types of participants, particularly in governance designs where the two groups could be

disjoint (e.g., voting rights based on a governance token that has no other function or direct relation to any on-chain activity).

Definition 13. *A blockchain governance system satisfies the property of accountability if whenever participants bring in a change, they are held individually responsible for it in a clearly defined way by the platform.*

Examples outside the blockchain space include the work done in Sacco et al. [40], where participants review publications and those having more 'skin in the game' (evaluating publications in which they will be marked as co-authors) have an increased individual interest in ensuring that a study's ambiguously reported methods and analyses are clarified prior to submission. Examples in the blockchain space include Polkadot's governance system [41], where voters who vote in favour of a proposal will have their stake locked until the proposal is 'enacted' or deployed.

2.6 Sustainability

Changes in blockchain governance rely on two main actors: those who develop and propose the changes, and those who decide on whether or not to adopt these changes. Contributions from both actors help the platform to adapt and evolve and need to be rewarded.

Definition 14 (Sustainable Development). *A blockchain governance system sustains development if it incentivises, via monetary rewards or otherwise, participants who develop successful improvement proposals for the platform.*

Definition 15 (Sustainable Participation). *A blockchain governance system sustains participation if it incentivises, via monetary rewards or otherwise, participants who participate in the decision-making process of the platform.*

Remark. *Sustainability is different from accountability in both moral and practical terms. Contrary to the definition of Accountability, Sustainability rewards development or participation with no regard to its outcome (ideally, before the respective agents have to perform the work or incur any costs). Accountability relates to possible penalties applied afterwards, once the effects of a particular change are apparent. For example, rewarding users just for voting would somewhat enable sustainable participation, but would not qualify for accountability. On the contrary, penalizing voters who approved a malicious proposal, without ever rewarding anyone, would only meet the definition of accountability.*

The idea behind having participation and development incentives in place is to *help* justify the cost of engagement, which can lead to higher voter participation or more contributions to the platform. These incentives can take various forms, from monetary incentives to reputation- or merit-based incentives [42]. However, Sustainable Participation could be a double edged sword if applied carelessly (e.g., [43, 44]. A monetary reward that is too small might convert a moral decision into a financial one, paradoxically decreasing participation. While in general increased participation also leads to an increase in information acquisition from the voters, it is certainly more beneficial to have a smaller set of participants that have done their due diligence and vote as honestly as possible, than a larger group of disinterested individuals who cast votes at random just to collect rewards.

2.7 Liveness

In formal, on-chain governed platforms, the process for proposing and adopting changes is often constrained by fixed-length time periods. An example of this is Tezos's Granada protocol [45], where a proposal has to go through five governance cycles (each lasting roughly two weeks) in order to be adopted. In such platforms, an unforeseen event that requires urgent action will not be resolved promptly through the platform's governance process. Therefore, a blockchain governance system must not only be able to process regular changes, but also urgent ones.

Definition 16. *A blockchain governance system satisfies liveness if it is capable of incorporating an input of urgency from the stakeholders and then being capable of acting on it in the sense that if an issue is deemed to be urgent according to some function, then the decision making procedure is capable of terminating within a reasonable amount of time, as a function of the urgency of the matter.*

This definition includes having some protection against *denial of service* attacks, that would prohibit governance mechanisms from terminating in time. All systems evaluated in this work are safe, at least from a high level standpoint, ignoring implementation details.

Events like the DAO hack [2] have shown the need for blockchain governance systems to be able to accommodate inputs of urgency and act on them within a suitable amount of time. An example of blockchain governance system with liveness measures is Polkadot [41], which allows for emergency referenda to be initiated by an assigned technical committee. Others, such as MakerDAO, implement an emergency shutdown functionality: since it is running on Ethereum, in an emergency the smart contact can suspend its normal operation and return the invested assets to their owners.

3 EVALUATIONS

In this section, we evaluate a number of popular platforms with respect to the properties outlined in Section 2. The platforms below were chosen such that they present an overview of current approaches. An overall view of the evaluations can be found in Table 1. We start with Bitcoin and Ethereum, two of the oldest and most influential blockchains. These two use proof-of-work for consensus and rely mostly on their developers for governance, who maintain a connection with the community but ultimately have control over the direction of the platform. Continuing, we consider Tezos, Polkadot and Decred. The first two use proof-of-stake, while Decred takes a hybrid approach. In particular, whereas Tezos and Decred favour "direct" democracy, Polkadot uses a *council* as well, representing two fundamentally different approaches to managing how voters express their preferences and interact with the governance process. Next, we study Project Catalyst and Dash, which incorporate a treasury in their decision making, meaning that the result of the voting process needs to respect a budget. Finally we consider Compound, Uniswap and MakerDAO that use a governance token approach. In the case of Compound and Uniswap this token is purely used for voting, while for MakerDAO it also supports the normal operation of the Maker protocol.

Gathering all the necessary information about every governance system is not always easy: typically, the platform's white paper

would contain a very high level overview. Moore details can sometimes be found on the websites of the respective blockchains, but often the complete picture can only be acquired by interacting with a wallet, voting app or forum. Keeping that in mind, we have made our best efforts to cite the relevant sources.

Remark. *In the main text we only include a high-level description and evaluation of the governance protocols. A more in-depth study, along with a point-to-point comparison with respect to each property can be found in the appendix.*

3.1 Bitcoin

Bitcoin [1] is the most prominent blockchain platform and it is a proof-of-work, mostly off-chain governed blockchain. The Bitcoin Improvement Proposal (BIP) process [46] is Bitcoin's primary mechanism for 'proposing new features, for collecting community input on an issue, and for documenting design decisions'. An individual or a group who wishes to submit a BIP is responsible for collecting community feedback on both the initial idea and the BIP before submitting it to the Bitcoin mailing list for review. Following discussions, the proposal is submitted to the BIP repository as a pull request, where a BIP editor will appropriately label it. BIP editors fulfil administrative and editorial responsibilities. There are repository 'maintainers' who are responsible for merging pull requests, as well as a 'lead maintainer' who is responsible for the release cycle as well as overall merging, moderation and appointment of maintainers [47]. Maintainers and editors are often contributors who earnt the community's trust over time. A peer review process takes place, which is expressed by comments in the pull request. Whether a pull request is merged into Bitcoin Core rests with the project merge maintainers and ultimately the project lead. Maintainers will take into consideration if a patch is in line with the general principles of the project; meets the minimum standards for inclusion; and will judge the general consensus of contributors [47].

There are stages through which a BIP can progress, including 'Rejected' and 'Final'. In progressing to a status of 'Final', there are two paths:

- *Soft-fork BIP.* A soft-fork upgrade often requires a 95% miner super-majority. This is done via an on-chain signalling mechanism introduced in [48].
- *Hard-fork BIP.* A hard-fork upgrade requires adoption from the entire 'Bitcoin economy', which has to be expressed by the usage of the upgraded software.

Evaluation. It is important to note here that the Bitcoin decision-making mechanism is informal, at least with respect to other platforms. Clearly, the on-chain aspects of Bitcoin's governance satisfy pseudonymity, but not secrecy or coercion resistance as no 'votes' are even encrypted. The same is true for its off-chain component. This has the advantage that the system is mostly verifiable, even though having part of the deliberation take place in public forums is harder to track and could be an impermanent storage solution. Since the decision-making process is informal, without clearly defined structure or voting rules, Pareto Efficiency (to any degree) cannot be guaranteed. Sustainability and Accountability fail for the same reason, as there are no defined rules for either. Liveness is arguably partially satisfied, given the informality and flexibility of the BIP system. Since miners are guaranteed to explicitly signal their approval or disapproval of soft-fork upgrades [48], mining-based suffrage is satisfied. Although those with previous positive contributions and relevant expertise are able to provide substantial inputs in the decision-making process, there is no explicit guarantee of their decision-making rights due to the informality of the process. Despite this, we conclude that meritocratic suffrage is *likely* satisfied.

3.2 Ethereum

Ethereum [49] is one of the most significant second-generation blockchain platforms. It is proof-of-work and governed off-chain, using the Ethereum Improvement Proposal (EIP) process [50] as a mechanism for proposing and integration changes. It is almost identical to that of Bitcoin, without giving miners the option to signal their preferences on-chain.

3.3 Tezos

Tezos [51] is a proof-of-stake, on-chain governed blockchain platform, which defines its governance process as 'self-ammending". Contrary to Bitcoin or Ethereum, participating in governance is based on *stake*. Specifically, Bakers (also known as *delegates*) need to have at least 8,000 XTZ (called a *roll*) and the infrastructure to run a Tezos node in order to gain *both* block producing and voting priviledges. Community members who have fewer than 8,000 XTZ or are unwilling to spend the computational resources can *delegate* their stake to bakers, who produce blocks and vote on their behalf. The voting process is currently divided in five governance periods, each period spanning roughly two weeks: Proposal, Testing-vote, Testing, Promotion-vote and Adoption. During the proposal period, *approval voting* is used to select the winning proposal, which must also be accepted by at least 5% of the total vote. In testing-vote and promotion-vote the possible options are 'Yea', 'Nay' or 'Pass'. A quorum between 0.2 and 0.7 of the total stake need to be reached, and the proposal is implemented if an 80% supermajority of 'Yea' is reached.

Evaluation. As with Bitcoin, Tezos only satisfies Pseydonymity, but is completely verifiable. Pareto Efficiency is more nuanced. If a proposal receives less than 5% of the upvotes or is tied with another proposal, no proposal will pass, even though operators could have voted for some proposals. However, given the properties of approval voting outlined in Section 2.2, this effect is mild. In addition, the selected outcome is checked once again at the last step. Pareto efficiency could be further hampered under the assumption that the proposals appearing in a single voting period are *too many* or *too technical* to evaluate in the allotted time, before the vote. This could make voters inadvertently split their votes and abstain on many proposals, either leading to a deadlock if no proposal reaches 5% or favoring *whales* (i.e. users with many tokens). To see this, consider that between 3 proposals A, B and C one whale with 40% of the tokens favours A while every other user equally likes B and C, but dislikes A. If the whale votes in favour of A and the other voters evenly split their votes between B and C, A could win the election. A possible solution to this would be to separate *vote* from *stake* delegation. Voters could transfer their

Platform	*Suffrage*				*Pareto Efficiency*	*Confidentiality*		*Verifiability*	*Accountability*	*Sustainability*		*Liveness*
	Identity-based	*Token-based*	*Mining-based*	*Meritocratic*		*Secrecy*	*Coercion Resistance*			*Development*	*Participation*	
Bitcoin	○	○	●	◓	○	◔	○	◓	○	○	○	◓
Ethereum	○	○	○	◓	○	◔	○	◓	○	○	○	◓
Catalyst	○	○	●	N	◓	◓	◔	◓	◔	●	●	○
Dash	○	●	○	○	◓	◔	○	●	○	●	●	○
Tezos	○	●	N	○	◓	◔	○	●	○	○	○	○
Polkadot	○	●	N	◔	●	◔	○	●	●	◓	○	●
Decred	○	●	○	○	◓	◔	○	●	○	●	○	○
Compound	○	●	○	◔	◓	◔	○	●	○	○	○	●
Uniswap	○	●	○	◔	◓	◔	○	●	○	○	○	◓
Maker DAO	○	●	○	○	◓	◔	○	●	○	○	○	●

Table 1: Overview of the evaluations of each property against each of the chosen platforms.
Every platfom might satisfy each property to a different degree. This is shown by a filled circle for robustly meeting the definition down to an empty circle if clear improvements are needed. The letter *N* is used if a property does not apply.

voting rights to more knowledgeable individuals that they trust which could consolidate their votes, while retaining their block production capabilities. Accountability or Sustainability are not satisfied. Given the lack of flexibility of the on-chain governance model, the Tezos governance system is incapable of taking inputs of urgency. Although a Gitlab issue or a pull request could be initiated without going through the formal on-chain route, it is still not the officially documented, and certainly not the 'self-amending', way by which the system processes inputs.

3.4 Polkadot

Polkadot [41] is a proof-of-stake, *mostly-on-chain* governed blockchain platform with a number interesting additions, including an elected council and a technical council. Voters require at least 5 DOT to participate in governance and their voting power is based on stake. At a glance, the voters elect councillors, directly vote on referenda and submit proposals. The councilors then have the power to *veto* dangerous proposals, elect the technical committee, submit proposal of their own for approval by the voters and also control the *treasury*. The technical council can submit *emergency* referenda, that are implemented immediately if approved.

More specifically, the council consists of 13 members with 7 day tenures. They are elected using an approval voting based method, the weighted Phragmén election algorithm (e.g. [52]. An in-house refinement of Phragmén called Phragmms [53] could be used in the future. During a referendum election, an *adaptive* quorum is used, requiring a different majority and turnout based on how the referendum was created (e.g, by the community or a weak council majority). A successful referendum enters a 28 day waiting period before enactment, unless it is an emergency. Typically, the votes cast are *locked* for these 28 days. However, the voters can increase their voting power by voluntarily locking them for longer (or decrease it by not locking at all). The treasury is controlled by the council, which decides whether to allocate funds to proposals that ask for them based on current supply.

Evaluation. As usual, only pseudonymity and verifiability are satisfied. Council elections and referenda voting functions are Pareto efficient. In addition, the voters have the ability to lock their votes for an extended time, to signal the strength of their preferences. Arguably, a veto might not be Pareto efficient if there is 100% consensus in a referendum. However, this is an extremely contrived case. Voting in favour of a proposal requires funds to be locked in until the proposal is enacted. The documented rationale behind this is to hold voters responsible for a proposal that they vote for, satisfying accountability and further reinforcing Pareto Efficiency. There are no explicit or direct rewards given for participation or contribution to satisfy sustainability. However, Polkadot have deliberately chosen *against* monetary rewards for voters, for justified reasons. Often the rewards for voters are too low for a significant effect, as detailed in Section 2.6. However, council members should probably receive some direct compensation. Even though their tenure is short, they hold a lot of power and should have the ability to devote themselves full time. The Polkadot governance mechanism is capable of taking in inputs of urgency (i.e. emergency referenda) and acting on it if deemed urgent by the council, all whilst being able to terminate within an amount of time proportional to the urgency. Token-based suffrage *is* satisfied since only token holders are allowed to vote. The council adds teams to the technical committee (which is able to propose emergency referenda) based on their positive technical contributions and expertise. However, those teams are chosen by council members only and a positive contribution does not equate to a guarantee of an input in a decision-making process.

3.5 Decred

Decred is a hybrid proof-of-work and proof-of-stake system that is mostly on-chain governed [54]. Voters can participate in governance by locking enough DCR, which is the native token of Decred. This provides them with *tickets* which supplement the consensus protocol and can also be used for voting. High level issues that require funds from the Decred Treasury are handled off-chain, in Politeia. This deliberation results in an election which is cryptographically coupled to a snapshot of the chain. A 20% quorum is needed, with over 60% of the votes being in favour. The on-chain component is the Decred Change Proposal (DCP) [55], through which the consensus mechanism is updated. This requires a 10% quorum and 75% majority of approval. Failing to meet the quorum, the election will be repeated in the next cycle. If it is successful, a 'lock-in' period begins, after which all nodes should update their software.

Evaluation The votes are not encrypted, therefore only pseudonymity and verifiability are satisfied. Pareto efficiency is somewhat satisfied: there are similar issues as Tezos, but the added role of Politeia could improve the outcome. Sustainable development is satisfied (somewhat informally) but there are no specific rewards for participating in governance. Voters receive rewards, but these have to do with their role in the hybrid consensus protocol. Accountability could be improved, as the token locking required for voting is shorter than the timelock for successful proposals.

3.6 Compound

Compound [56] is a protocol running *on* the Ethereum blockchain that establishes money markets. Governance in Compound is fuelled by an ERC-20 compatible token called COMP [57]. These *governance* tokens are distributed to the community through various channels: some are allocated to users based on their invested assets, others to Compound Labs Inc. shareholders and employees, etc. Holding COMP allows users to vote, delegate to others and create proposals, which are executable pieces of code. Once submitted, these proposals enter a two day review period, following a three day election. A proposal is successful if a majority is in favour and a quorum is reached. After that, the proposal is *locked* for two days before implementation, for security reasons. In addition, the *Pause Guardian* (controlled by a community appointed multi-signature) can suspend most functionalities of Compound at any time.

Evaluation Every step of the governance process is performed by interacting with smart contracts on Ethereum, without any further cryptographic techniques, satisfying pseudonymity and verifiability. Once a proposal enters the voting phase, the voters only have two options: yes or no, which is clearly Pareto Efficient. If there are multiple incompatible options (e.g., values of a specific parameter), these proposals would have to be dealt with sequentially: the actual order could bias voters, which complicates their decisions and leaks information. Therefore, Pareto Efficiency is somewhat satisfied (e.g., between two highly popular proposal, the slightly less popular one might win if it is up for election first and then the users might be less eager to implement another change). Once a proposal is executed, its creator and voters are completely independent from its future and there are no rewards associated with the process. Therefore, neither availability or sustainability are satisfied. The total time between creating a government proposal and voting for it takes 7 days, 2 of which are hard-coded into the Timelock. This window for immediate action is only open right after a vote, but adding the Pause Guardian, liveness is satisfied. Since voting eligibility depends only on having COMP tokens, which can be exchanged and are initially distributed to addresses with assets on Compound, token-based suffrage is satisfied. Some COMP tokens are distributed or reserved for members of the Compound team. Therefore, meritocratic suffrage is slightly satisfied.

3.7 Uniswap

We briefly sketch Uniswap [58] governance, which combines off and on-chain components. The on-chain part of its governance system is almost identical to Compound appendix A.4, using the UNI token instead. However, UNI can also be used to empower off-chain processes. The off-chain discourse takes place on the Uniswap governance forum, where 2 types of posts have particular significance. The first is the Temperature Check, whose goal is to gauge interest in changing the status quo. After 3 days there is a poll, where users have vote according to the amount of UNI they hold on-chain. If a majority is reached and quorum are reached, a Consensus Check is created on the same forum. During the 5 day duration of the Consensus Check, a proposal needs to be fleshed out. In the end, a second poll is brought before the users, this time possibly containing many alternatives. As long as the highest ranked alternative receives more than 50,000 UNI, an on-chain Governance Proposal is created and handled like in Compound.

3.8 Maker DAO

Maker DAO [59] is a decentralized organization running on Ethereum and based on the Maker Protocol. One of its novel features is using a two-token system, with DAI, which is a stablecoin pegged to the U.S. dollar, and MKR which the governance token. MKR serves an additional purpose however: to support DAI's peg. The governance system employs both on and off-chain elements. The off-chain component takes place at the Maker DAO forum, where users can create Forum Signal Threads, which are followed by a poll. Each forum user has a single vote, irrespective of MKR. These are further ratified on-chain by Governance Polls, which employ *instant-runoff voting*, weighted by the MKR of each voter. Finally, changes to the protocol (which are pieces of executable code) are enacted by Executive Votes. These follow a *continuous* approval vote system, with the most approved Vote at any given time being the actual implementation. For security reasons, these changes happen after a 24 hour waiting period and there is also an emergency shutdown functionality, triggered if the community locks enough MKR.

Evaluation. As there is no vote encryption, only pseudonymity and verifiability are satisfied. Pareto Efficiency is improved compared to other designs by using instant-runoff voting to handle competing proposals, thus giving voter a richer action space to declare their preferences accurately (without requiring multiple rounds or additional strategic behaviour). Suffrage is also improved, as there is a clear connection between MKR tokens and the overall functionality of Maker DAO, further coupling its value to some actual generated utility.

Remark. *Project Catalyst and Dash also include a* treasury, *which complicates the voting process. Funds are periodically collected by the normal blockchain operation and allocated to fund its development and undertake projects* whose results may take months to materialize. *In addition, at every funding round more than one proposal may be selected, as long as their total cost does not exceed a budget. Voters need additional flexibility to signal their preferences. Specifically, they need to compare a proposals perceived value with it with its budget and think about the opportunity cost of funding it. This is closely related to the field of* Participatory Budgeting *(e.g., [60–62]). Decred also includes a treasury. The salient difference (e.g., with Project Catalyst) is that competing proposals are first debated off-chain, rather than set to compete on-chain for some portion the budget available in one round of funding. The final vote is on-chain, but only as a referendum on proposals that already acquired off-chain support.*

3.9 Project Catalyst

Project Catalyst [63] is the on-chain treasury governance system used by the Cardano blockchain, which is proof-of-stake. Governance takes place in twelve week periods called funds and involves a number of additional agents, on top of the usual voters, whose voting power and eligibility is dependent on stake ownership. At the beginning of the fund, community generated proposals (which include a corresponding budget) are submitted. These are then reviewed by Community Advisors (CA's) and these reviews are further checked for their quality by veteran Community Advisors (vCA's), both of which are rewarded for their efforts. Given these evaluations, an approval voting based mechanism [30] is used. The proposal whose 'Yes' votes minus the 'No' votes are more than 5% of the total votes received is eligible for funding. These eligible proposals are then sorted according to their approval. If the available funds are not enough to cover some proposal, it is skipped and a less popular (but cheaper one) could take its place. In addition, there is the Catalyst Circle [64], an elected group of representatives that oversees Catalyst and a delegated voting system is proposed for future iterations.

Evaluation. Everyone participates in Project Catalyst using their wallet address. Voters submit *encrypted* ballots (padded with some randomness), using the public key issued by a committee, which tallies the votes and decrypts the result. If the voter address is linked to a real identity, the only information available is that this particular person voted, keeping the contents secret. The ballot itself cannot be decrypted by the voter and if the random padding is not kept, it is impossible even for the voter to convince anyone of the way they voted. The result of the vote can be independently verified and long as the voter saved the random padding, they can verify that their particular vote was counted. Therefore, there is a (somewhat contrived) sequence of events after which a voter would be unable to check that their ballot has been added.

In some cases, proposals with fewer votes will be prioritised for their lower budgets. For example, if the total fund is 100 and the three winning proposals have budget 1, 50 and 50 (in order of popularity) the last proposal will not receive funding, even though every voter might prefer funding the two 50 proposals. Additionally, each voter could submit an uninformative 'no' vote to many proposals, in order to maximize the winning chance of their favourite. A potential mitigation would be to use techniques from Participatory Budgeting [61] and Distortion [65], which use a small amount of *ordinal information* (e.g., asking voters to compare between 2 proposals or to list their most favourite one) to improve the quality of the outcome. Overall, Pareto Efficiency is only *somewhat* satisfied.

There are no explicit, on or off-chain, penalties. Proposers need to submit progress reports about their projects to keep receiving funding and community advisors can be penalized for poor reviews or absence. As these are either centralized or community-driven without clearly described mechanisms, accountability is mostly *not* satisfied. Although there is no explicit reward given to the proposer, it is her responsibility to request the amount which cover the cost of her work. All other parties are rewarded for participating in the governance process and to an extent receive larger rewards for additional effort. Each Project Catalyst Fund follows a 12 week timeline. Liveness is not satisfied: even though the funds can be released in accordance with each proposal's progress, there is no mechanism to take urgent action. Voting rights depend only on having at least 500 ADA. There are no guaranteed voting rights based on previous positive contributions, however, community advisors can affect the outcome of the votes through their reviews.

3.10 Dash

Dash [66] uses proof-of-work for the underlying consensus mechanism, but includes an additional layer of functionality enabled by *masternodes*, including governance and treasury fund allocation. These masternodes are users that have locked at least 1,000 DASH (called collateral, which is part of their stake) and also operate a server. The treasury operates in similar fashion to Project Catalyst, but requires a 10% difference between 'Yes' and 'No' votes for eligible proposals. Proposals can be submitted by anyone, but require spending 5 DASH to ensure that only serious enough issues are raised. Only masternodes may vote and there are no designated roles for reviewers or elected representatives. Additionally masternode do not collect rewards specifically for voting, but are rewarded for the entirety of their duties.

Evaluation. The system only satisfies pseudonymity and verifiability, as votes are public. Pareto Efficiency is similar to Project Catalyst. Although masternodes have collateral, this is not directly tied to governance and could be withdrawn immediately after enacting some controversial proposal. Sustainable development is satisfied through the treasury, but sustainable participation could be improved as the masternode rewards are not specific to voting, but conensus as well. Additionally, there is an issue of Suffrage since *only* token holders (having at least 1,000 DASH, or about 54,000$) who are also willing to run a server can participate, leaving other token holders without representation.

4 CHALLENGES & RESEARCH DIRECTIONS

It should be clear from our exposition so far that the blockchain governance space is still rife with challenges and open questions. We summarize in this section a number of them to motivate future research in the area.

I. Tradeoffs between Privacy vs. Verifiability and Suffrage. The tension between verifiability and privacy stems from requirements

such as universal verifiability which mandates tracing each decision back to the inputs of decision-makers as determined by suffrage. The higher degree of privacy that is required, the more difficult it is to ensure verifiability; as a simple example from classical elections, if the electoral roll remains private, then it is difficult for an external observer to verify whether the correct set of decision-makers has participated. This also creates a tension with suffrage as types of suffrage that maximize inclusion, for the sake of verifiability, might have to expose a larger set of community-members that otherwise would have remained private. Technically reconciling these properties is highly non-trivial, especially if privacy aspects such as coercion resilience are desired.

II. Proofs of Personhood, Identity-based suffrage and tradeoffs with Privacy. While there is wide agreement that individual users should have equal weight in decision-making (something advocated in the context of election reform for centuries, cf. [67]), achieving this type of suffrage is particularly challenging in the context of decentralized systems. Even though some initial work is undertaken in this direction e.g., [17], and there are also connections with other concepts in cyber-security such as CAPTCHAs [68], nevertheless the problem of achieving a satisfactory level of identity-based suffrage in the context of blockchain governance is still wide open. This challenge should be also considered from the lens of privacy, since in many cases of such proofs, community-members would have to reveal personally identifiable information to other actors something that comes inevitably with privacy implications.

III. Meritocratic suffrage and tradeoffs with privacy. The challenge in the context of meritocratic suffrage is in two levels, first, in quantifying what type of merit itself should warrant participation to decision-making. The second level is recording reliably the relevant actions of community-members in the system so that it can be acted upon during the decision-making process. Finally, as in the case of proofs of personhood, there can be privacy implications. Some early works in this direction show that privacy and merit may be reconciled, see e.g., the signatures of reputation primitive [69] but still, significantly more work is required to fully tackle the full spectrum of possible ways to express and act on merit.

IV. Exchanges, venture capital investors and token-based suffrage. In the setting of token-based suffrage, an important consideration is the fact that token-holders may choose custody solutions for their tokens for a variety of reasons (reducing risks regarding loss of keys, or the ability to access services or rewards provided by custody operators). While among some cryptocurrency users this is frowned upon (the tenet "not your keys, not your coins" is frequently repeated in social media) there is a large number of users that prefer to keep their digital assets in third party providers' systems.[2] This state of affairs, results in entities with inflated leverage in a token-based system that in some cases can control a very significant portion of the token supply. A related issue is the presence of venture capital firms that are early investors in some platforms and receive a large amount of tokens at preferential prices in exchange for funding initial development efforts. This similarly may result in increased leverage which can be perceived as unfair by other community-members.

[2]Indicatively, statistics from the web-site https://cryptoquant.com/, at the time of writing (May 2022), suggest that about 13.3% of the Bitcoin supply is held on exchanges. The figure for Ethereum is higher at slightly above 20%.

V. Rational ignorance and inaction. Rational ignorance [70] is when decision-makers refrain from acquiring the knowledge required of meaningful input when voting, or when delegating their vote, due to the fact that the cost of acquiring that knowledge exceeds any expected potential benefits. A similar argument can be applied to developing improvement proposals, where inaction can be more rational than action if the cost of development (or even the act of preparing a proposal) exceeds any potential benefits. These issues pertain to the property of sustainability which so far lacks a comprehensive theoretical framework in the context of blockchain governance. For some recent work that can be helpful in this direction see [71, 72].

VI. Tradeoffs between accountability and utility. Recall that making decision-makers accountable suggests some degree of "skin-in-the game" on their side and the natural way to achieve this suggests some form of restriction of the functionality that is offered to them by the platform. As a result, the immediate utility that decision makers can extract from the platform is reduced — recall the example of "token lockup" for the duration of a certain decision making process. The main challenge in this setting is to model and quantify the relevant aspect of this utility reduction and mapping the spectrum of possible options so that the the right balance between accountability and utility can be determined on a case by case basis.

VII. Tradeoffs between Liveness vs. Pareto Efficiency and Suffrage. As we discussed in the context of liveness, expedient decision-making is highly desirable. Unfortunately high expediency can come at odds with Pareto efficiency: if decision-makers have preferences which are not recorded due to the system not giving them enough opportunity to them for reacting, then it is easy to see that this can violate Pareto efficiency (observe here that abstaining can be also a preference - however there is a distinction between having an actual preference and missing the deadline to provide it to the system and preferring to abstain altogether). Liveness can also exhibit a similar tradeoff with suffrage: the more exclusive the suffrage mapping from community-members to decision-makers is, the higher the expediency of the system may become - but this of course comes at the expense of the system being less inclusive. Striking the right balance between liveness and these properties is another question on which future research should focus.

5 CONCLUSION

In this systematization work we focused on documenting a comprehensive list of properties of blockchain governance. We took a first principles approach and derived seven fundamental properties using which we analyzed a number of widely used blockchain platforms. It is worth saying that there are also other platforms that we have attempted to cover, but these were either too poorly documented or were yet to implement governance mechanisms, thus we consider the list a comprehensive coverage of popular blockchain systems at the time of writing.

The main outcome of the systematization effort, as illustrated in Table 1, is that in many ways all current blockchain platforms either have deficiencies in their governance processes or allow significant room for improvement. It is worth also reiterating that achieving all stated properties to the highest possible degree is impossible due to their conflicting nature and as a result it is inevitable that platforms

must decide on appropriate tradeoffs between the various properties that are the most suitable for each particular setting. Arguably, without effective governance processes, blockchain technology will fail to reach its full potential. For one thing, software engineering practice has shown that software updates, extensions and patches are a necessity in the lifecycle of computer systems and as a result, without proper governance, blockchain systems will fail to adapt to unanticipated use cases and mitigate software bug vulnerabilities that are inevitably discovered in any system.

6 ACKNOWLEDGMENTS

We would like to thank Yussef Soudan for his extensive research and participation in many meetings during the earlier stages of this work. Additionally, we thank Roman Oliynykov for providing many details and insights regarding the evaluation of Project Catalyst.

REFERENCES

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[2] Divisions of Corporation Finance and Enforcemen. Statement by the Divisions of Corporation Finance and Enforcement on the Report of Investigation on the DAO. Investigation report. July 2017. URL: https://www.sec.gov/litigation/investreport/34-81207.pdf.

[3] Almost $500,000 in Ethereum Classic coin stolen by forking its blockchain, Dan Goodin, 1/8/2019, Arstechnica.

[4] Legal operational and technical standards for e-voting, Recommendation Rec(2004)11 adopted by the Committee of Ministers of the Council of Europe on 30 September 2004 and explanatory memorandum, Council of Europe publishing, 2004, http://www.eods.eu/library/CoE_Recommentaion%20on%20Legal,%20Operational%20and%20Technical%20Standards%20for%20E-voting_2004_EN.pdf.

[5] Voting System Standards Volume I, Federal Election Commission, USA. April 2002. https://www.eac.gov/sites/default/files/eac_assets/1/28/Voting_System_Standards_Volume_I.pdf.

[6] V. Buterin, Moving beyond coin voting governance, August, 2021. Accessed on: October 1, 2021. Available: https://vitalik.ca/general/2021/08/16/voting3.html.

[7] Y. Liu, Q. Lu, L. Zhu, H.-Y. Paik, and M. Staples, "A systematic literature review on blockchain governance," *arXiv preprint arXiv:2105.05460*, 2021.

[8] Wharton Cryptogovernance Workshop. Accessed on: October 19, 2021. Available: https://cryptogov.net.

[9] R. v. Pelt, S. Jansen, D. Baars, and S. Overbeek, "Defining blockchain governance: a framework for analysis and comparison," *Information Systems Management*, vol. 38, no. 1, pp. 21–41, 2021.

[10] R. Beck, C. Müller-Bloch, and J. L. King, "Governance in the blockchain economy: A framework and research agenda," *Journal of the Association for Information Systems*, vol. 19, no. 10, p. 1, 2018.

[11] P. De Filippi and G. McMullen, "Governance of blockchain systems: Governance of and by distributed infrastructure," 2018.

[12] Y.-Y. Hsieh, J.-P. J. Vergne, and S. Wang, "The internal and external governance of blockchain-based organizations: Evidence from cryptocurrencies," pp. 48–68, 2017.

[13] D. W. Allen and C. Berg, "Blockchain governance: What we can learn from the economics of corporate governance," *Allen, DWE and Berg, C (Forthcoming)'Blockchain Governance: What can we Learn from the Economics of Corporate Governance*, 2020.

[14] N. Khan, T. Ahmad, A. Patel, and R. State, "Blockchain governance: An overview and prediction of optimal strategies using nash equilibrium," *arXiv preprint arXiv:2003.09241*, 2020.

[15] S. Venugopalan and I. Homoliak, "Always on voting: A framework for repetitive voting on the blockchain," *arXiv preprint arXiv:2107.10571*, 2021.

[16] H. Gersbach, A. Mamageishvili, and M. Schneider, "Vote delegation and misbehavior," *arXiv preprint arXiv:2102.08823*, 2021.

[17] D. Siddarth, S. Ivliev, S. Siri, and P. Berman, "Who watches the watchmen? a review of subjective approaches for sybil-resistance in proof of personhood protocols," *Frontiers in Blockchain*, vol. 3, p. 46, 2020.

[18] S. P. Lalley and E. G. Weyl, "Quadratic voting: How mechanism design can radicalize democracy," vol. 108, pp. 33–37, 2018.

[19] B. S. Srinivasan and L. Lee, Quantifying Decentralization, news.earn.com, July, 28, 2017. Accessed on: October 3, 2021. Available: https://news.earn.com/quantifying-decentralization-e39db233c28e.

[20] F. Brandt, V. Conitzer, and U. Endriss, "Computational social choice," *Multiagent systems*, pp. 213–283, 2012.

[21] K. J. Arrow, "A difficulty in the concept of social welfare," *Journal of political economy*, vol. 58, no. 4, pp. 328–346, 1950.

[22] A. Gibbard, "Manipulation of voting schemes: a general result," *Econometrica: journal of the Econometric Society*, pp. 587–601, 1973.

[23] M. A. Satterthwaite, "Strategy-proofness and arrow's conditions: Existence and correspondence theorems for voting procedures and social welfare functions," *Journal of economic theory*, vol. 10, no. 2, pp. 187–217, 1975.

[24] R. L. Rivest and E. Shen, "An optimal single-winner preferential voting system based on game theory," in *Proc. of 3rd International Workshop on Computational Social Choice*. Citeseer, 2010, pp. 399–410.

[25] B. Kluiving, A. de Vries, P. Vrijbergen, A. Boixel, and U. Endriss, "Analysing irresolute multiwinner voting rules with approval ballots via sat solving," in *ECAI 2020*. IOS Press, 2020, pp. 131–138.

[26] J. J. Bartholdi and J. B. Orlin, "Single transferable vote resists strategic voting," *Social Choice and Welfare*, vol. 8, no. 4, pp. 341–354, 1991.

[27] M. Balinski and R. Laraki, "Majority judgment," *Cambridge/Mass*, 2011.

[28] J. D. Cohen and M. J. Fischer, "A robust and verifiable cryptographically secure election scheme (extended abstract)," in *26th Annual Symposium on Foundations of Computer Science, Portland, Oregon, USA, 21-23 October 1985*. IEEE Computer Society, 1985, pp. 372–382. [Online]. Available: https://doi.org/10.1109/SFCS.1985.2

[29] A. Juels, D. Catalano, and M. Jakobsson, "Coercion-resistant electronic elections," in *Towards Trustworthy Elections*. Springer, 2010, pp. 37–63.

[30] B. Zhang, R. Oliynykov, and H. Balogun, "A treasury system for cryptocurrencies: Enabling better collaborative intelligence," in *The Network and Distributed System Security Symposium 2019*, 2019.

[31] E. Cuvelier, O. Pereira, and T. Peters, "Election verifiability or ballot privacy: Do we need to choose?" in *European Symposium on Research in Computer Security*. Springer, 2013, pp. 481–498.

[32] R. Gharadaghy and M. Volkamer, "Verifiability in electronic voting-explanations for non security experts," in *4th International Conference on Electronic Voting 2010*. Gesellschaft für Informatik eV, 2010.

[33] V. Cortier, D. Galindo, R. Küsters, J. Mueller, and T. Truderung, "Sok: Verifiability notions for e-voting protocols," in *2016 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2016, pp. 779–798.

[34] J. C. Benaloh and D. Tuinstra, "Receipt-free secret-ballot elections (extended abstract)," in *Proceedings of the Twenty-Sixth Annual ACM Symposium on Theory of Computing, 23-25 May 1994, Montréal, Québec, Canada*, F. T. Leighton and M. T. Goodrich, Eds. ACM, 1994, pp. 544–553. [Online]. Available: https://doi.org/10.1145/195058.195407

[35] J. Benaloh, "Simple verifiable elections," in *2006 USENIX/ACCURATE Electronic Voting Technology Workshop, EVT'06, Vancouver, BC, Canada, August 1, 2006*, D. S. Wallach and R. L. Rivest, Eds. USENIX Association, 2006. [Online]. Available: https://www.usenix.org/conference/evt-06/simple-verifiable-elections

[36] A. Kiayias, T. Zacharias, and B. Zhang, "Ceremonies for end-to-end verifiable elections," in *Public-Key Cryptography - PKC 2017 - 20th IACR International Conference on Practice and Theory in Public-Key Cryptography, Amsterdam, The Netherlands, March 28-31, 2017, Proceedings, Part II*, ser. Lecture Notes in Computer Science, S. Fehr, Ed., vol. 10175. Springer, 2017, pp. 305–334. [Online]. Available: https://doi.org/10.1007/978-3-662-54388-7_11

[37] J. Alwen, R. Ostrovsky, H. Zhou, and V. Zikas, "Incoercible multi-party computation and universally composable receipt-free voting," in *Advances in Cryptology - CRYPTO 2015 - 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part II*, ser. Lecture Notes in Computer Science, R. Gennaro and M. Robshaw, Eds., vol. 9216. Springer, 2015, pp. 763–780. [Online]. Available: https://doi.org/10.1007/978-3-662-48000-7_37

[38] C. A. Dykstra, "The quest for responsibility," *American Political Science Review*, vol. 33, no. 1, p. 1–25, 1939.

[39] R. W. Grant and R. O. Keohane, "Accountability and abuses of power in world politics," *American political science review*, vol. 99, no. 1, pp. 29–43, 2005.

[40] D. F. Sacco, S. V. Bruton, M. Brown, and M. M. Medlin, "Skin in the game: Personal accountability and journal peer review," *Journal of Empirical Research on Human Research Ethics*, vol. 15, no. 4, pp. 330–338, 2020, pMID: 32425095. [Online]. Available: https://doi.org/10.1177/1556264620922651

[41] D. Salman, Governance, Polkadot Wiki, September 17, 2021. Accessed on: October 1, 2021. Available: https://wiki.polkadot.network/docs/learn-governance.

[42] Y. Zhang and M. van der Schaar, "Reputation-based incentive protocols in crowdsourcing applications," in *2012 Proceedings IEEE INFOCOM*, 2012, pp. 2140–2148.

[43] C. Panagopoulos, "Extrinsic rewards, intrinsic motivation and voting," *The Journal of Politics*, vol. 75, no. 1, pp. 266–280, 2013.

[44] V. A. Shineman, "If you mobilize them, they will become informed: experimental evidence that information acquisition is endogenous to costs and incentives to participate," *British Journal of Political Science*, vol. 48, no. 1, pp. 189–211, 2018.

[45] Tezos Foundation, The Voting Process, Tezos Documentation, July 16, 2021. Accessed on: October 2, 2021. Available: https://gitlab.com/tezos/tezos/-/blob/master/docs/010/voting.rst.

[46] L. Dashjr, BIP Process, github.com, February, 4, 2016. Accessed on: October 14, 2021. Available: https://github.com/bitcoin/bips/blob/master/bip-0002.mediawiki.

[47] J. Schnelli et al., Contributing to Bitcoin Core , github.com, September, 26, 2015. Accessed on: October 14, 2021. Available: https://github.com/bitcoin/bitcoin/blob/master/CONTRIBUTING.md.

[48] P. Wuille, P. Todd, G Maxwell, and R. Russell, Version bits with timeout and delay, github.com, October, 4, 2015. Accessed on: October 14, 2021. Available: https://github.com/bitcoin/bips/blob/master/bip-0009.mediawiki.

[49] V. Buterin, "A Next-Generation Smart Contract and Decentralized Application Platform", github.com, 2013. Accessed on: November 15, 2021. Available: https://ethereum.org/en/whitepaper/.

[50] M. Becze, H. Jameson, et al., "EIP-1: EIP Purpose and Guidelines," Ethereum Improvement Proposals, no. 1, October 2015. Accessed on: November 15, 2021. [Online serial]. Available: https://eips.ethereum.org/EIPS/eip-1.

[51] "*Tezos Docs*", September 9, 2016. Accessed on: October 23, 2021. Available: https://gitlab.com/tezos/tezos/-/tree/master/docs.

[52] M. Brill, R. Freeman, S. Janson, and M. Lackner, "Phragmén's voting methods and justified representation," in *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 31, no. 1, 2017.

[53] A. Cevallos and A. Stewart, "A verifiably secure and proportional committee election rule," in *Proceedings of the 3rd ACM Conference on Advances in Financial Technologies*, 2021, pp. 29–42.

[54] "Decred Documentation", April 26, 2016. Accessed on: November 16, 2021. Available: https://github.com/decred/dcrdocs.

[55] "Decred Change Proposals", May 6, 2017. Accessed on: November 21, 2021. Available: https://github.com/decred/dcps.

[56] R. Leshner, G. Hayes, "Compound: The Money Market Protocol", compound.finance, 2019. Accessed on: November 16, 2021. Available: https://compound.finance/documents/Compound.Whitepaper.pdf.

[57] Coinbase Statistics on COMP, Accessed on: December 1, 2021. Available: https://coinmarketcap.com/currencies/compound/.

[58] H. Adams, N. Zinsmeister, M. Salem, R. Keefer, D. Robinson, "Uniswap v3 Core", 2021. Accessed on: November 16, 2021. Available: https://uniswap.org/whitepaper-v3.pdf.

[59] The Maker Protocol: MakerDAO's Multi-Collateral Dai (MCD) System. Accessed on: November 16, 2021. Available: https://makerdao.com/en/whitepaper.

[60] H. Aziz and N. Shah, "Participatory budgeting: Models and approaches," 2020.

[61] G. Benade, S. Nath, A. D. Procaccia, and N. Shah, "Preference elicitation for participatory budgeting," *Management Science*, vol. 67, no. 5, pp. 2813–2827, 2021.

[62] V. Buterin, Z. Hitzig, and E. G. Weyl, "A flexible design for funding public goods," *Management Science*, vol. 65, no. 11, pp. 5171–5187, 2019.

[63] Project Catalyst Community website. Accessed on: December 15, 2021. Available: https://cardanocataly.st.

[64] Kriss Baird, Introducing the Catalyst Circle. Accessed on: December 12, 2021. Available: https://iohk.io/en/blog/posts/2021/07/08/introducing-the-catalyst-circle/.

[65] E. Anshelevich, A. Filos-Ratsikas, N. Shah, and A. A. Voudouris, "Distortion in social choice problems: The first 15 years and beyond," *arXiv preprint arXiv:2103.00911*, 2021.

[66] "*Dash Docs*", February 13, 2018. Accessed on: October 17, 2021. Available: https://github.com/dashpay/docs.

[67] G. Howell, "One man, one vote," Manchester Selected Pamphlets. JSTOR 60239578, 1880.

[68] L. von Ahn, M. Blum, N. J. Hopper, and J. Langford, "CAPTCHA: using hard AI problems for security," in *Advances in Cryptology - EUROCRYPT 2003, International Conference on the Theory and Applications of Cryptographic Techniques, Warsaw, Poland, May 4-8, 2003, Proceedings*, ser. Lecture Notes in Computer Science, E. Biham, Ed., vol. 2656. Springer, 2003, pp. 294–311. [Online]. Available: https://doi.org/10.1007/3-540-39200-9_18

[69] J. Bethencourt, E. Shi, and D. Song, "Signatures of reputation," in *Financial Cryptography and Data Security, 14th International Conference, FC 2010, Tenerife, Canary Islands, Spain, January 25-28, 2010, Revised Selected Papers*, ser. Lecture Notes in Computer Science, R. Sion, Ed., vol. 6052. Springer, 2010, pp. 400–407. [Online]. Available: https://doi.org/10.1007/978-3-642-14577-3_35

[70] B. R. Taylor, "The psychological foundations of rational ignorance: biased heuristics and decision costs," *Constitutional Political Economy*, vol. 31, no. 1, pp. 70–88, 2020.

[71] C. Prato and S. Wolton, "The voters' curses: why we need goldilocks voters," *American Journal of Political Science*, vol. 60, no. 3, pp. 726–737, 2016.

[72] ——, "Rational ignorance, populism, and reform," *European Journal of Political Economy*, vol. 55, pp. 119–135, 2018.

[73] P. Emerson, "The original borda count and partial voting," *Social Choice and Welfare*, vol. 40, 02 2013.

[74] Maker Governance. Accessed on: October 18, 2021. Available: https://vote.makerdao.com/.

A FURTHER DETAILS ABOUT EACH GOVERNANCE SYSTEM

Following our high-level overview in Section 3, we use the appendix to provide a more complete picture, including the finer details of each platform and how these affect each property.

A.1 Bitcoin

Bitcoin [1] is the most prominent blockchain platform and it is a proof-of-work, mostly off-chain governed blockchain. The Bitcoin Improvement Proposal (BIP) process [46] is Bitcoin's primary mechanism for 'proposing new features, for collecting community input on an issue, and for documenting design decisions'. An individual or a group who wishes to submit a BIP is responsible for collecting community feedback on both the initial idea and the BIP before submitting it to the Bitcoin mailing list for review. Following discussions, the proposal is submitted to the BIP repository as a pull request, where a BIP editor will appropriately label it. BIP editors fulfill administrative and editorial responsibilities. There are repository 'maintainers' who are responsible for merging pull requests, as well as a 'lead maintainer' who is responsible for the release cycle as well as overall merging, moderation and appointment of maintainers [47]. Maintainers and editors are often contributors who earned the community's trust over time. A peer review process takes place, which is expressed by comments in the pull request. Whether a pull request is merged into Bitcoin Core rests with the project merge maintainers and ultimately the project lead. Maintainers will take into consideration if a patch is in line with the general principles of the project; meets the minimum standards for inclusion; and will judge the general consensus of contributors [47].

There are stages through which a BIP can progress, including 'Rejected' and 'Final'. In progressing to a status of 'Final', there are two paths:

- *Soft-fork BIP.* A soft-fork upgrade often requires a 95% miner super-majority. This is done via an on-chain signaling mechanism introduced in [48].
- *Hard-fork BIP.* A hard-fork upgrade requires adoption from the entire 'Bitcoin economy', which has to be expressed by the usage of the upgraded software.

We now have an overview of the upgrades decision-making process in Bitcoin, which we will use to perform rough evaluations against the properties developed in Section 2. It is important to note here that the Bitcoin decision-making mechanism is informal, at least with respect to other platforms. This results in rougher and less satisfying evaluations.

- **Suffrage**: Since miners are guaranteed to explicitly signal their approval or disapproval of soft-fork upgrades [48], mining-based suffrage is satisfied. Although those with previous positive contributions and relevant expertise are able to provide substantial inputs in the decision-making process, there is no explicit guarantee of their decision-making rights due to the informality of the process. However, since meritocracy still does play a significant role in the process, we will conclude that meritocratic suffrage is *likely* satisfied.

- **Pareto Efficiency**. Since the decision-making process is informal, there is no defined voting rule, which specifies how the inputs result in a final outcome. Therefore Pareto efficiency is *not* satisfied.
- **Accountability**. The platform does not define any way by which it can hold participants responsible or accountable for their individual actions. Therefore, accountability is *not* satisfied.
- **Confidentiality**:
  - **Secrecy**: Since the decision-making process among maintainers or reviewers is on public forums, an adversary might accurately guess each participant's input. Therefore, secrecy is *not* satisfied.
  - **Pseudonymity**: There are no defined requirements for participants to reveal their identities. Some choose to participate with their real identities and others do not. Therefore, pseudonymity is satisfied.
  - **Coercion-resistance**: Since the deliberation process among maintainers and others takes place on public forums, an adversary might accurately guess each participant's input. Thus, coercion-resistance is *not* satisfied.
- **Verifiability**. The signaling mechanism used as a voting process for certain decisions is on-chain. However, even though the deliberation process takes place in public forums, the decision-making process remains informal, which makes it difficult to identify how inputs are incorporated from which parties and how they are tallied. However, such inputs can be traced through the public forums and any changes that are merged can be tracked on Github. Therefore, verifiability is *mostly* satisfied.
- **Sustainability**: *Sustainable Development*. There are no explicitly defined incentives for contributors to develop BIPs. Therefore, sustainable development is *not* satisfied.
- **Sustainability**: *Sustainable Participation*. There are no explicitly defined incentives for community members to participate in discussions or reviews throughout the BIP process. Therefore, sustainable participation is *not* satisfied.
- **Liveness**. Although no specific mention of inputs of urgency are provided by the platform, given the informality and flexibility of the BIP system, it is likely capable of taking inputs of urgency and acting on them in an amount of time that is a function of the urgency. Therefore, the platform *likely* satisfies liveness.

A.2 Tezos

Tezos [51] is a more-recent proof-of-stake, on-chain governed blockchain platform, which defines its governance process as "self-amending". In Tezos, to participate directly in the governance process, a participant is required to have at least $8,000$ tokens. A unit of $8,000$ tokens is called a *roll* and it equates to a single vote. In this case, the participant is called a *delegate*. Alternatively, to participate indirectly in the governance process, a participant can delegate whichever amount of tokens they have (which can be less than $8,000$) to an existing delegate.

The voting process is currently divided in five governance periods, each period spanning roughly two weeks or 20480 blocks (i.e. 5 cycles). Note that for proposals to be submitted in Tezos, they need to be compiled without errors so that at the end of the governance process the proposal can be adopted automatically. The following is a breakdown of the five governance periods:

(1) **Proposal period**. Delegates can submit protocol amendment proposals using the proposals operation as long as the underlying codebase compiles with the change. Delegates then upvote their preferred proposal or proposals. The proposal with the most upvotes is selected. If there are no proposals, no proposals with upvotes of at least 5% of the possible votes, or a tie between proposals, a new proposal period starts.
(2) **Testing-vote period**. Delegates can cast one vote to test or not the winning proposal using the ballot operation.
(3) **Testing period**. A test chain is forked for the entire testing period to ensure a correct migration of the context.
(4) **Promotion-vote period**. Delegates can cast one vote to promote or not the tested proposal using the ballot operation.
(5) **Adoption period**. The adoption period serves as a buffer time for users to update their infrastructure to the new protocol. At the end of this period, the proposal is activated as the new protocol and a new proposal period starts. Here, the Tezos node software is aware that at the end of this period it needs to update to the new protocol, hence why the governance process is described as "self-amending".

In the **proposal period**, approval voting is used. In the **testing-vote** and **promotion-vote** periods, the voting method is as follows:

- Each delegate can submit a single vote of a "Yea", "Nay" or "Pass".
- If the participation reaches the current quorum and the proposal has a super-majority in favour, it goes through to the next stage.
  - The quorum is the participation threshold, it has maximum value of 0.7 and a minimum value of 0.2, and it changes after every vote.
  - A super-majority is when the number of "Yea" votes is more than 80% of the number of "Yea" votes and "Nay" votes summed together.

Similar to the previously evaluated platforms, we perform the evaluations of the governance process in Tezos against the properties developed in Section 2.

- **Suffrage**: Only token-holders are able to vote, with or without delegation. Therefore, token-based suffrage *is* satisfied.
- **Pareto Efficiency**. If a proposal receives less than 5% of the upvotes or is tied with another proposal, no proposal will pass, even though operators could have voted for some proposals. However, given the properties of approval voting outlined in Section 2.2, this effect is mild. In addition, the selected outcome is checked once again at the last step. Therefore, Pareto efficiency is *somewhat* satisfied.
- **Confidentiality**:
  - **Secrecy**: The delegation mechanism requires the public key of each delegate to be recorded on the ballot, and all ballots are public. Therefore, secrecy is *not* satisfied.

  - **Pseudonymity**: Voters are not required to reveal their real-life identities to participate in the governance process; therefore pseudonymity is satisfied.
  - **Coercion-resistance**. Since delegate votes (rolls) are tied to their chosen pseudo-identities, coercion-resistance is *not* satisfied.
- **Verifiability**. Since the votes and final tally are all public, verifiability is, by definition, satisfied.
- **Accountability**. Whether an operator is directly voting or delegating, the stake of each delegate is computed at the start of each voting period. This means that delegates can sell their stake before the adoption period ends and the proposal is activated. There are no accountability measures defined in Tezos. Therefore, accountability is *not* satisfied.
- **Sustainability**: *Sustainable Development or Participation*. There are no explicit or direct incentives given for developing successful proposals or participating in the governance process. Therefore, sustainability is *not* satisfied.
- **Liveness**. Given the lack of flexibility of the on-chain governance model, the Tezos governance system is incapable of taking inputs of urgency and responding to them in accordance to the severity of the issue. Although a Gitlab issue or a pull request could be initiated without going through the formal on-chain route, it is still not the officially documented, and certainly not the "self-amending", way by which the system processes inputs. Therefore, liveness is *not* satisfied.

A.3 Polkadot

Polkadot [41] is a proof-of-stake, *mostly-on-chain* governed blockchain platform. To make any changes to the network, *active* token holders and the *council* administrate a network upgrade decision. Whether the proposal is proposed by the public (token holders) or the council, it will go through a referendum to let all token-holders, weighted by stake, make the decision.

The council is an elected body of on-chain accounts that are intended to represent the passive stakeholders of Polkadot, currently consisting of 13 members [41]. The council has two major tasks in governance: (i) proposing referendums and (ii) vetoing dangerous or malicious referendums. The council implements what is called a *prime member* whose vote acts as the default for other members that fail to vote before the timeout. The prime member is chosen based on a Borda count [73]. With the existence of a prime member, it forces councilors to be explicit in their votes or have their vote counted for whatever is voted on by the prime. The council also controls Polkadot's treasury and allocates funds to successful proposals.

Voting for councilors requires locking 5 DOT tokens (the native token of the platform) and takes on an approval voting approach. A token-holder can approve up to 16 different councilors and the vote will be equalised among the chosen group, with each council term lasting 7 days. The approval voting method used is the weighted Phragmén election algorithm (e.g. [52], where the candidates with most approvals are elected and, afterwards, a process is run that redistributes the vote amongst the elected set. This reduces the variance in the list of backing stake from the voters to the elected candidates in order to ensure that the minimum amount of tokens required to join the council is as high as possible. Running the Phragmén algorithm cannot be completed within the time limits of production of a single block. And waiting would jeopardise the constant block production time of the network. Therefore, as much computation as possible is moved to an off-chain worker, where validators can work on the problem without impacting block production time. An in-house refinement of Phragmén called Phragmms [53] could be used in the future.

A significant part of Polkadot's governance is the *technical committee*, which is composed of teams that have successfully implemented or specified either a *Polkadot runtime* or *Polkadot Host* [41]. These teams are added or removed from the technical committee via simple majority votes within the council. The technical committee can, along with the council, propose emergency referendums, which are fast-tracked for voting and implementation (e.g., for emergency bug fixes)

Besides electing councilors, token-holders get to vote in referendums. Each referendum has a specific proposal associated with it. Proposals can implement backward-compatible or backward-incompatible changes. Proposals can be submitted by token-holders, the council or the technical committee:

- For token-holders to submit a proposal, a minimum amount of tokens must be deposited. If another token-holder agrees with the proposal, they can also deposit the same amount of tokens in the proposal's support. The proposal with the highest amount of bonded support will be selected to be a referendum in the next voting cycle. The referendum, in this case, will have positive turnout bias. That is, the smaller the amount of stake voting, the larger the super-majority necessary for it to pass [41]. Specifically the proposal would pass if
$$\frac{\text{against}}{\sqrt{\text{turnout}}} < \frac{\text{approve}}{\sqrt{\text{electorate}}}.$$
- Proposals can only be submitted by the council through a majority or unanimously. In the case of a unanimous council, the referendum will have a negative turnout bias, that is, the smaller the amount of stake voting, the smaller the amount necessary for it to pass:
$$\frac{\text{against}}{\sqrt{\text{electorate}}} < \frac{\text{approve}}{\sqrt{\text{turnout}}}.$$
In the case of a majority, the referendum will be a majority-carries vote (51% of the votes is required to win).
- The technical committee can propose emergency referendums subject to approval from the council.

If a proposal passes in a referendum, then Polkadot's logic automatically schedules it for enactment: autonomous enactment. This is unlike other systems where miners or validators often have unilateral power to prevent protocol changes by refusing to upgrade software. Proposals submitted by the council or token-holders are enacted 28 days after the referendum, whereas ones submitted by the technical committee can be enacted immediately.

To vote, a token-holder generally must lock their tokens up for at least the enactment delay period beyond the end of the referendum. This is in order to ensure that some minimal economic buy-in exists and to dissuade vote selling. It is possible to vote without locking at all, but the vote is worth a small fraction of a normal vote. It is also

possible to voluntarily lock for more than one enactment period, in which case, the weight of the vote increases proportionally. This mechanism exists to ensure that users with little stake but strong opinions can express their conviction in referendums.

- **Suffrage**: Token-based suffrage *is* satisfied since only token holders are allowed to vote. The council adds teams to the technical committee (which is able to propose emergency referenda) based on their positive technical contributions and expertise. However, those teams are chosen by council members only and a positive contribution does not equate to a guarantee of an input in a decision-making process. Therefore, meritocratic suffrage is only *slightly* satisfied.
- **Pareto Efficiency**. Council elections and referenda voting functions are Pareto efficient. In addition, the voters have the ability to lock their votes for an extended time, to signal the strength of their preferences. Arguably, a veto might not be Pareto efficient if there is 100% consensus in a referendum. However, this is an extremely contrived case. For all intents and purposes governance *is* Pareto efficient.
- **Confidentiality**:
  - **Secrecy**: Votes on Polkadot, whether it's in electing councilors, internal council votes, or voting in referenda, are not documented to be private. Therefore, secrecy is *not* satisfied.
  - **Pseudonymity**: Participants are not required to reveal their real-life identities to participate in the decision-making process.Therefore pseudonymity *is* satisfied.
  - **Coercion-resistance**: Since secrecy is *not* satisfied, coercion-resistance is *not* satisfied by definition.
- **Verifiability**. Since the votes and final tally are all public, verifiability *is* satisfied.
- **Accountability**. Voting in favour of a proposal requires funds to be locked in until the proposal is enacted. The documented rationale behind this is to hold voters responsible for a proposal that they vote for. Therefore, accountability *is* satisfied.
- **Sustainability**: There are no explicit or direct rewards given for participation, but successful proposals requiring funds can access the treasury, after approval from the council. As mentioned in the main text, Polkadot has explicitly chosen against direct voting rewards. Sustainable development is only somewhat satisfied, as the current mechanism is still a bit informal.
- **Liveness**. The Polkadot governance mechanism is capable of taking in inputs of urgency (i.e. emergency referenda) and acting on it if deemed urgent by the council, all whilst being able to terminate within an amount of time proportional to the urgency. Therefore, liveness *is* satisfied.

A.4 Compound

Compound [56] is a protocol running on the Ethereum blockchain that establishes money markets. These are collections of Ethereum assets (e.g. Ether, ERC-20 stablecoins, coins like DAI or ERC-20 utility coins such as Augur) that users can supply and borrow. These assets have algorithmically defined interest rates, dependent on supply and demand, that users collect or pay when supplying and borrowing respectively. Users can borrow depending on the value of the underlying asset they have as collateral and repay at any rate they want, paying the accrued interest. This provides the ability to quickly switch between tokens in a trustless manner.

Governance in Compound is fuelled by an ERC-20 compatible token called COMP [57]. The maximum number of COMP tokens is capped at 10,000,000. About 4,200,000 of them are distributed to the community at a rate of 2,312 per day. Of those, a fixed fraction of these tokens is allocated to every market on Compound, half of which goes to suppliers and the other half to borrowers and subsequently allocated proportionately within each group. Additionally, 2,400,000 tokens belong to the Compound Labs Inc. shareholders, 2,200,000 are allocated over 4 years to the Compound team (with an additional 320,000 reserver for future members) and finally 775,000 are reserved for the community.

Holders of COMP can delegate voting power and create *government* proposals. COMP tokens can be delegated to other addresses at rate of 1 vote per token, or delegated to oneself for a direct vote. A government proposal can then be created by any address holding at least 25,000 COMP. On top of that, any address with 100 COMP can create an *autonomous* proposal, which in turn can become a government proposal once that address receives 25,000 COMP or more in delegation. A government proposal is an executable piece of code, which could update some parameter (e.g. the rate at which COMP tokens are distributed), create a new money market or provide additional functionality to the Compound smart contracts. A single address cannot issue multiple proposals in parallel.

The governance process is controlled by two smart contracts: Governor Bravo and Timelock. Once a government proposal is created, it is put into a two day review period, followed by an election lasting 3 days. COMP holders can vote for or against the proposal, which passes if the majority was in favour *and* it received more than 400,000 votes in total. After that, it is put in Timelock for a mandatory 2 day waiting period, before it is executed. This is a safety measure: if an issue is found while in Timelock, the proposer can cancel it (or the users can start reacting before its too late). At any point prior to execution, the creator of the proposal (or any address if the creator has fewer than 25,000 COMP) can cancel the process. In addition the *Pause Guardian* (which is controlled by a community appointed multi-signature) can suspend the functionality of some Compound function (namely Mint, Borrow, Transfer, and Liquidate) allowing users only very benign actions such as closing their positions.

- **Suffrage**. Since voting eligibility depends only on having COMP tokens, which can be exchanged and are initially distributed to addresses with assets on Compound, token-based suffrage *is* satisfied. Some COMP tokens are distributed or reserved for members of the Compound team. Therefore, meritocratic suffrage is *slightly* satisfied.
- **Pareto Efficiency**. Once a proposal enters the voting phase, the voters only have two options: yes or no. This is clearly Pareto efficient and aligned with their incentives. Things get more tricky once there are multiple incompatible options (e.g., values of a specific parameter). In this case the proposals would have to be dealt with sequentially: the actual order could bias voters, which complicates their decisions and

leaks information. Therefore, Pareto Efficiency is *somewhat* satisfied (e.g., between two highly popular proposal, the slightly less popular one might win if it is up for election first and then the users might be less eager to implement another change).

- **Confidentiality**:
  - **Secrecy and Coercion Resistance**: Every step of the governance process, such as proposing, voting or delegating is on-chain, by interacting with smart contracts on Ethereum. This done through possibly pseudonymous addresses and is public and unencrypted. Therefore, *neither* property satisfied.
  - **Pseudonymity**: Users participate using their Ethereum address, therefore pseudonymity *is* satisfied.
- **Verifiability**. Since the votes and final tally are all public, verifiability *is* satisfied.
- **Accountability**. Once a proposal is executed, its creator and voters are completely independent from its future. Therefore, accountability is *not* satisfied.
- **Sustainability**: *Sustainable Development*. There is no mechanism to reward development efforts: the proposal should already be complete and executable. Therefore, sustainable development is *not* satisfied.
- **Sustainability**: *Sustainable Participation*. Although COMP tokens have an value and can be traded, there are no additional reward for voting or creating a government proposal. Therefore, sustainable participation is *not* satisfied.
- **Liveness**. The total time between creating a government proposal and voting for it takes 7 days, 2 of which are hard-coded into the Timelock. This is reasonable: in addition, if an exploit is found while in Timelock, the proposer can cancel it. Failing to do so, the users of Compound have some time to either move their assets or fork. This window for immediate action is typically only open right after a vote, however the Pause Guardian ensures that an 'emergency shutdown' feature is always available. Therefore, liveness *is* satisfied.

A.5 Maker DAO

Maker DAO [59] is a decentralized organization running on Ethereum and based on the Maker Protocol. It employs a two-token system, using Dai and MKR, both of which are ERC-20 compatible. The first, DAI, is a collateral-backed stablecoin which is soft-pegged to the U.S. dollar and is collateralized by a *mix* of other cryptocurrencies. The second, MKR, is a governance token is used by stakeholders to maintain the system and manage Dai. However, in addition to the previous governance token models, MKR, which is *not* a stablecoin, is also used to control the price of Dai, by creating favourable exchange rates between the two coins, depending on Dai supply and demand. In particular, 1,000,000 MKR were originally minted. The total supply is then kept as close to this number as possible, by burning or minting new tokens in exchange for Dai.

The governance model employed [74] combines some of the features of Compound (such as on-chain voting for some issues, executable proposals and a mandatory waiting period) and some off-chain features of Uniswap (such as forum discussions). Note that the two components are *not* officially coupled. The off-chain component takes place at the Maker DAO forum, which is public. In addition to usual forum posts, users can (and are encouraged to) create a *Forum Signal Thread*. The purpose is to get community feedback on some issue, possible on-chain proposals or generally any potential improvement to Maker DAO. At the end, the Forum Signal Thread is followed by a poll, where users vote pseudonymously. Every user has *one* vote, irrespective on the amount of MKR they may have. The intended function is that the discussion and poll results will inform the choices of an upcoming *on-chain* governance action.

There are two on-chain processes facilitated by smart contracts: *Governance Polls* and *Executive Votes*. The aim of Governance Polls is to ratify Forum Signal Threads, formally gauge consensus about important topics and select one of many alternative designs before an Executive Vote. The Governance Poll could contain multiple options and holders of MKR vote using instant-runoff. Governance Polls usually stay open for 3 to 7 days. The results of Governance Polls can then be turned into Executive Votes, although both processes could be initiated by any Ethereum address at any point. However, only Governance Facilitators can link specific Governance Polls and Executive Votes in the official forum.

The Executive Vote is the only way to enact changes on the smart contracts supporting of Maker DAO. Indeed, an Executive Vote should contain instructions to amend their code with the proposed set of changes. Executive Votes are selected via *continuous* approval voting, typically without having a fixed voting window. Specifically, holders of MKR can change their vote at any time and the Executive Vote with the highest approval would win. However, once an Executive Vote that was implemented loses to another one, it is deactivated and the only way to revert to the previous status is through a new vote. Once a new Executive Vote wins, the Governance Security Module imposes a 24 hour waiting period, during which the vote can be reversed.

Maker DAO also makes use of Emergency Shutdown. At any point if a total of 50,000 MKR are deposited into the Emergency Shutdown Module, an Emergency Shutdown is triggered. These coins are immediately burned and the Maker Protocol is shut down. Then, collateral supporting Dai (as well as the coins themselves) are returned to their owners. For various reasons, Dai takes lower priority than collateral and could be exchanged for less than 1$ per Dai.

- **Suffrage**. Since voting eligibility is only guaranteed to MKR token holders, token-based suffrage *is* satisfied.
- **Pareto Efficiency**. For Executive Votes, the voters only have two options: to vote yes or no. Even though these do not have to follow Governance Polls, the ranked-choice, instant runoff voting mechanism used there gives the voters the option to choose between multiple alternatives, avoiding the possibility of a sequential vote (e.g., as could happen in Compound). Therefore, Pareto Efficiency is *mostly* satisfied.
- **Confidentiality**:
  - **Secrecy**: Every step of the governance process, such as proposing, voting or delegating is on-chain, by interacting with smart contracts on Ethereum. This done through possibly pseudonymous addresses and is public and unencrypted. Therefore secrecy is *not* satisfied.

  - **Pseudonymity**: Users participate using their Ethereum address. Therefore, pseudonymity *is* satisfied.
  - **Coercion-resistance**: Since secrecy is not satisfied, coercion-resistance is *not* satisfied by definition.
- **Verifiability**. Since the votes and final tally are all public, verifiability *is* satisfied.
- **Accountability**. As with Compound, once a proposal is executed, its creator and voters are completely independent from its future. Therefore, accountability is *not* satisfied.
- **Sustainability**: *Sustainable Development*. There is no mechanism to reward development efforts: the proposal should already be complete and executable. Therefore, sustainable development is *not* satisfied.
- **Sustainability**: *Sustainable Participation*. MKR are crucial for Maker DAO as they help maintain the peg with Dai. However, the extra energy spent on deciding what to vote on is not explicitly compensated. Therefore, sustainable participation is *not* satisfied.
- **Liveness**. An Executive Vote can be implemented in 24 hours, once it receives enough votes. This gives both the ability to quickly prevent a bad proposal and relatively quickly enact a better one. In addition, there is also an Emergency Shutdown functionality. Therefore, liveness *is* satisfied.

A.6 Project Catalyst

Project Catalyst [63] is the on-chain governance system used by the Cardano blockchain. The role of Project Catalyst is to provide a mechanism through which users can collectively decide how Cardano's treasury funds should be allocated.

Governance in Project Catalyst occurs in 12 week intervals, called *Funds*. There are 4 primary types of agents participating: proposers, voters, Community Advisors (CA's) and Veteran Community Advisors (vCA's). Additionally, people can participate by referring projects to be funded and designing challenges that need to be addressed. Finally, the *Catalyst Circle* [64] is a small group of representatives of all types of agents involved, tasked with monitoring the current state and developing future plans for Project Catalyst. The Circle is currently not elected, but an election mechanism is discussed for future iterations. At the beginning of each fund a set of challenges is issued, either by users of Cardano or the Project Catalyst team. Then, the proposers offer proposals, which may, but are not required to, address a specific challenge. The proposals should contain a detailed set of goals, along with a specific plan to achieve them and a required budget. Then, the community advisors write reviews for any proposal they chose to, focusing on impact, implementability and auditability. These reviews are then reviewed again by the veteran community advisors and are assigned a grade that can be 'Excellent', 'Good' or 'Filtered Out', the last reserved for particularly uninformative reviews. Having all this information, the voters can vote 'Yes', 'No' or 'Abstain' for as many proposals as they want. Each vote has weight proportional to the users stake in ADA, which is the currency used by Cardano. Project Catalyst implements *fuzzy threshold voting* [30]. Voters express a 'Yes', 'No' or 'Abstain' opinion for each proposal. A proposal passes if the number of 'Yes' votes minus the number of 'No' votes is at least 5% of the total votes it received. The winning proposals are awarded their funds in the order of the margin by which they are passing, until either the entire budget is allocated or no more passing proposals exist. If a proposal has passed the voting threshold but insufficient funds remain to pay the full amount requested, it will not receive partial funding. Instead, any smaller proposals which have also passed the threshold that will fit in the budget will be funded, even if they have lower net approval than the larger proposal.

All agents involved in Project Catalyst are rewarded in some capacity. At every Fund each reward pool corresponds to a set percentage of the total. As a concrete example we will examine Fund7, which had total budget of $8,000,000 in ADA. This amount was further broken down as follows:

- $80\% \rightarrow \$6,400,000$ for funding proposals
- $13\% \rightarrow \$1,040,000$ for voting rewards.
- $4\% \rightarrow \$320,000$ for community advisors
- $1\% \rightarrow \$80,000$ for veteran Community Advisors.
- $1\% \rightarrow \$80,000$ for referral rewards.
- $1\% \rightarrow \$80,000$ for challenge teams rewards.

Any user with more than 500 ADA can become a voter. This is measured by a snapshot of the stake distribution taken before the election, but the funds are not locked. Each voter receives voter rewards proportional to their stake. Community advisors receive rewards relative to the quality of the reviews, but also depending on how many other reviews were written for the proposals they reviewed. An 'Excellent' review provides 3 times the reward of a 'Good' review and each proposal has rewards for 2 'Excellent' and 3 'Good' reviews. If these rewards are not enough to cover the reviews, a lottery is used. Veteran community advisors are rewarded equally, provided they reviewed a minimum number of reviews. Proposers are not rewarded explicitly, but can manage the funds received by their proposal and have to periodically submit progress reports to the community. The performance of community advisors and veteran community advisors is recorded, but there is no currently defined on-chain mechanism for a voter to become either of those. The promotion from voter (or proposer) to community advisor to veteran is centralized.

- **Suffrage**. Since voting eligibility depends only on having at least 500 ADA, token-based suffrage *is* satisfied. There are no guaranteed voting rights based on previous positive contributions. However, community advisors and veteran community advisors can affect the outcome of the votes through their reviews. Meritocratic suffrage is *slightly* satisfied.
- **Pareto Efficiency**. As noted in the main text evaluation, Pareto Efficiency is only *somewhat* satisfied.
- **Confidentiality**:
  - **Secrecy**: Everyone participates in Project Catalyst using their wallet address. Proposers, community advisors and veteran community advisors participate publicly. Voters submit *encrypted* ballots (padded with some randomness), using the public key issued by a committee. Then, these votes are tallied and the result is decrypted by the committee, if a majority of its members agrees. Furthermore, if the wallet address is linked to a real identity, the only information available is that this particular person voted,

but the actual vote is still secret. Therefore the vote is *mostly* secret.
  - **Pseudonymity**: Voters participate with their wallet address, therefore pseudonymity *is* satisfied.
  - **Coercion-resistance**: The system is somewhat coercion resistant. The ballot itself cannot be decrypted by the voter. Additionally, if the random padding is not kept, it is impossible even for the voter to convince anyone of the way they voted.
- **Verifiability**. The result of the vote can be independently verified. In addition, as long as a voter saved the random padding, they can verify that their particular vote was counted. Without the padding this is impossible, as the votes *cannot* be decrypted. As such, verifiability is only *mostly* satisfied.
- **Accountability**. There are no explicit, on or off-chain, penalties. Proposers need to submit periodic progress reports about their projects to keep receiving funding. Similarly, community advisors and veteran community advisors can be penalized for poor reviews or absence. As these are either centralized or community-driven without clearly described mechanisms, accountability is mostly *not* satisfied.
- **Sustainability**: *Sustainable Development*. Although there is no explicit incentive or reward given to the proposing group or individual, it is the responsibility of the proposer to request the amount which represents the value of their work. Therefore, sustainable development *is* satisfied.
- **Sustainability**: *Sustainable Participation*. Since all parties are rewarded for participating in the governance process and to an extent receive larger rewards for additional effort (e.g. community advisors and review quality), sustainable participation *is* satisfied.
- **Liveness**. Project Catalyst is primarily used for allocating treasury funds and each Fund follows a 12 week timeline. As such, liveness is *not* satisfied: even though the funds can be released in accordance with each proposal's progress, there is no direct mechanism to take urgent action. However, liveness is arguably not required for its purposes.

A.7 Dash

Like Bitcoin, Dash [66] uses a proof-of-work consensus mechanism. However, Dash's approach to governance takes a formal, on-chain form. The Dash Governance System (DGS) uses a 'budget and masternode voting system' to govern and fund the underlying blockchain's development and maintenance. Masternodes are nodes that can place at least a $1,000$ DASH, the platform's native token, as a collateral to participate in the consensus protocol and governance process. Each masternode has a single, public, approval vote expressing which improvement proposals the masternode approves of. In each voting cycle (which is roughly a month long), project proposals are submitted and then voted on. Even though anyone can submit a proposal, doing so comes at a cost of 5 DASH to ensure that only serious proposals are voted on.

The DGS implements a system very similar to Project Catalyst with one difference: A proposal is eligible for funding if the number of 'Yes' votes minus the number of 'No' votes is at least 10% of the *total* masternode count. Additionally, if there are two proposals with the same approval, then the one with a larger proposal transaction hash is ranked higher. The treasury is funded through various channels. When new blocks are mined, 45% of the block reward is reserved for the miner, 10% for the budget and 45% for the masternodes' reward. We now perform evaluations of the DGS against the properties developed in Section 2.

- **Confidentiality**:
  - **Secrecy**: Since the masternodes vote publicly, the DGS does *not* satisfy secrecy.
  - **Pseudonymity**: Masternodes are not required to reveal their real-life identities to participate in the governance process; therefore pseudonymity is satisfied.
  - **Coercion-resistance**: Since masternode votes are tied to their chosen pseudo-identities, coercion-resistance is *not* satisfied.
- **Verifiability**. Since the votes and final tally are all public, verifiability is, by definition, satisfied.
- **Pareto Efficiency**. As with Project Catalyst, Pareto Efficiency is only *somewhat* satisfied.
- **Accountability**. Although masternodes are required to lock $1,000$ DASH to vote, if a group of masternodes vote in a malicious proposal, they will face no negative consequences and will be able to unlock their funds before the malicious proposal is enacted. Therefore, accountability is *not* satisfied.
- **Sustainability**: *Sustainable Development*. Although there is no explicit incentive or reward given to the proposing group or individual, it is the responsibility of the proposer to request the amount which represents the value of their work. Therefore, sustainable development *is* satisfied.
- **Sustainability**: *Sustainable Participation*. Masternodes are rewarded with part of the block reward for their participation in the consensus and governance process. Therefore, sustainable participation is satisfied.
- **Liveness**. Given the lack of flexibility of the on-chain governance model, the DGS is incapable of taking inputs of urgency and responding to them in accordance to the severity of the issue. Although a Github issue or a pull request could be initiated without going through the formal on-chain route, it is still not the officially defined way by which the system processes inputs. Therefore, liveness is *not* satisfied.
- **Suffrage**. Since voting eligibility depends only on having at least $1,000$ DASH, token-based suffrage is satisfied.

A.8 Decred

Decred is a hybrid proof-of-work and proof-of-stake system that is mostly on-chain governed [54]. Such a hybrid implementation results in three main types of stakeholders: miners, voters and regular users. All three participate pseudo-anonymously. To have decision-making powers (in governance and block-validation), participants need to have 'tickets', which are bought or acquired through time-locking DCR (the native token of the platform). We will not go through the details of a ticket lifecycle, but the process is thoroughly outlined in [54]. Each block contains 5 pseudo-randomly sampled tickets (i.e. 5 votes).

Proposals can be handled either by an on-chain or off-chain procedure. Specifically, proposals regarding high level issues or that

require funds from the Decred Treasury are handled off-chain. They first appear in Politeia, the system's deliberation platform, to be discussed throughout the community. Administrators of the platform can flag spam proposals or comments. When a proposal owner decides to put their proposal for a vote, the administrators can then trigger the start of off-chain voting. A snapshot of the currently bought tickets takes place 256 blocks before the start of voting. Then, the ticket-voting interval of 2,016 blocks (approximately 1 week) formally begins, which means 10,080 pseudo-randomly sampled tickets have the opportunity to vote. Voting on Politeia is not recorded on chain, but it is still backed by cryptographic techniques which prevent Sybil attacks and unfair censorship. When the ticket-voting period ends, the proposal is formally approved or rejected. There is a quorum requirement for a vote to be considered valid: 20% of the eligible tickets must vote 'Yes' or 'No'. The threshold for a proposal to be approved is 60% 'Yes' votes. When a proposal with a budget and deliverables is approved, work can begin. The proposal owner can submit claims against the budget as deliverables are completed.

The on-chain governance is performed through Decred Change Proposal (DCP) [55], focusing on updating the consensus mechanism. With a DCP, the proposed node software must be developed and released. The new code will lie dormant until the change has been voted upon and accepted by the proof-of-stake voters. Each voting interval lasts for 8,064 blocks, which makes the maximum number of votes 40,320. A ticket can vote to accept the rule change, to reject it or to abstain (the default choice). Every vote has a quorum requirement of 10%. This means that at least 10% of all votes cast must be non-abstain for the result to be considered valid. If all non-abstaining votes fail to meet a 75% Yes or No majority threshold, the agenda vote remains active for next voting period. If 75% of all non-abstaining votes accept the proposal, the agenda is considered locked in and the consensus changes will activate 8,064 blocks (4 weeks) after the vote passed. If 75% of all non-abstaining votes reject the proposal, the agenda fails and the consensus changes will never activate. If an agenda reaches its expiration before ever reaching a 75% majority vote, the agenda expires and the consensus changes will never activate. After a ticket has voted, missed, or expired, the funds cannot be released for another 256 blocks.

If the quorum requirement is met, and more than 75% of the votes are in favour of activating the new consensus rules, then a 'lock-in' period begins of 8,064 blocks. During this period, all participants in the Decred network must upgrade their software to the latest version. All full nodes participating in the network will automatically activate the new rules on the first block after this period, so any nodes still running the old software will no longer be able to participate. Throughout the process, it is possible to verify the voting preference of a ticket.

With this brief overview in mind, we can now perform the evaluation of Decred's governance system against our properties.

- **Suffrage**. Since voting eligibility only depends on buying proof-of-stake tickets, token-based suffrage *is* satisfied.
- **Pareto Efficiency**. If a proposal vote occurs with a quorum of less than 10%, the proposal will not pass, even when it receives one or more approval votes. Furthermore, given the role of Politeia, it is unlikely that a truly controversial proposal will pass. Therefore, the most likely 'suboptimal' outcome is not selecting any proposal, when one might have had some support. Therefore, Pareto efficiency is *somewhat* satisfied.
- **Confidentiality**:
  - **Secrecy**: There are no explicit secrecy guarantees in the voting process. Therefore, secrecy is *not* satisfied.
  - **Pseudonymity**: Participants (miners, voters, and regular users) are not required to reveal their real-life identities to participate in the decision-making process. Therefore pseudonymity *is* satisfied.
  - **Coercion-resistance**: Since secrecy is not satisfied, coercion-resistance is *not* satisfied by definition.
- **Verifiability**. Since the votes and final tally are all public, verifiability *is* satisfied.
- **Accountability**. Although funds from the ticket cannot be released until 256 blocks after voting, the changes to the consensus rules are not applied until after 8,064 blocks. This implies that if a voter or a group of voters voted in a malicious proposal, they can withdraw their locked funds before the proposal is enacted. Therefore, accountability is *not* satisfied.
- **Sustainability**: *Sustainable Development.* Although there is no explicit incentive or reward given to the proposing group or individual, it is the responsibility of the proposer to request the amount which represents the value of their work. Therefore, sustainable development *is* satisfied.
- **Sustainability**: *Sustainable Participation.* Although voters can gain rewards from their tickets via validating blocks as part of the consensus protocol [54], there are no explicit additional incentives for voting (or participating in the governance process). Therefore, sustainable participation is *not* satisfied.
- **Liveness**. Given the lack of flexibility of the on-chain governance model, it is incapable of taking inputs of urgency and responding to them in accordance to the severity of the issue. Therefore, liveness is *not* satisfied.

ATTACHMENT 2

Decentralizing Information Technology: The Advent of Resource Based Systems

— version 0.77 —

Aggelos Kiayias
University of Edinburgh, IOHK
akiayias@inf.ed.ac.uk

Tuesday 28th December, 2021

Abstract

The growth of the Bitcoin network during the first decade of its operation to a global scale system is a singular event in the deployment of Information Technology systems. Can this approach serve as a wider paradigm for Information Technology services beyond the use case of digital currencies? We investigate this question by introducing the concept of resource based systems and their four fundamental characteristics: (i) resource-based operation, (ii) tokenomics, (iii) decentralized service provision, and (iv) rewards sharing. We explore these characteristics, identify design goals and challenges and investigate some crucial game theoretic aspects of reward sharing that can be decisive for their effective operation.

1 Introduction

A paradigm shift took place during the last decade in the way the consensus problem is looked at in Computer Science. Three decades after the seminal work of Lamport, Shostak and Pease [30], Satoshi Nakamoto with the Bitcoin blockchain protocol [25] put forth a novel way to solve the consensus problem. Traditionally, Byzantine consensus was considered to be the problem of reaching agreement between a set of processors, some of which may arbitrarily deviate from the protocol and try to confuse the ones who follow the protocol. Over time, significant research was invested into establishing the exact bounds in the *number* of deviating parties as well as the intrinsic complexity bounds of the problem in terms of round and message complexity.

The approach did not address the question who assigns identities to the processors or sets up the network that connects them, or how the processors agree about the identities of all those present in the particular protocol instance. These were tasks left to a system setup phase that, for all purposes, seemed sufficient to be a centralized operation carried out by a trusted party. The success of the Internet however and the development of peer-to-peer networks in the early 2000's set the stage for challenging this assumption. At the same time, Sybil attacks [11] posed a significant obstacle to apply known consensus protocol techniques to this new setting.

Given the above landscape, Nakamoto's solution is unexpected. The blockchain protocol design circumvents entirely the issue of identity and provides a solution for consensus that "takes advantage of information being easy to spread but hard to stifle" [26]. In the Bitcoin blockchain, it is the computational power that different participants contribute to the protocol execution that facilitates convergence to a unique view. And as long as the deviating parties are in the minority of computational power,

Nakamoto's blockchain protocol can be shown to converge to an unambiguous view that incorporates new inputs in a timely manner, as proven formally in [17] and subsequently refined in [18, 28].

The bitcoin blockchain however is much more than just a consensus protocol; it provides a service — transferring digital currency between principals — and also provides incentives to those who engage in service provision in the form of "mining" the digital currency following a regular schedule. In this way, agreeing to a joint view is not the primary objective but rather a precondition for the service to materialize. Participants need to agree on the ledger of digital asset ownership.

Becoming a system maintainer in Bitcoin does not require anything else other than possessing the software and necessary hardware to run the protocol. Remarkably, there is no need to be approved by other participants as long as the underlying peer to peer network allows diffusing messages across all peers without censorship.

Given the successful growth of the Bitcoin network at a worldwide level, a fundamental question arises: does its architecture suggest a novel way of deploying information technology (IT) services at a global scale? So far, in IT, we have witnessed two major ways of scaling systems to such level. In the "centralized" approach, we have organizations such as Google, Facebook and Amazon that offer worldwide operations with high quality of service. The downsides of the centralized approach is —naturally— centralization itself and the fact that long term common good may not necessarily align properly with company shareholder interest. In such settings, regulatory arbitrage may deprive the public any leverage against the service operator. A second approach is the "federated" one. In this case, we have the coordination of multiple organizations or entities with a diverse set of interests to offer the service in cooperation. Examples of such federated organization have been very successful and far reaching as they include the Internet itself. Nevertheless, for federated organization to scale, significant efforts should be invested to make sure the individual systems interoperate and the incentives of their operators remain aligned.

Viewed in this light, the decentralized approach offered by Nakamoto's Bitcoin system provides an alternative pathway to a globally scalable system. In this paper, we abstract Nakamoto's novel approach to system deployment under a general viewpoint that we term "resource-based systems." Preconditioned on the existence of an open network, a resource based system capitalizes on a particular resource that is somehow dispersed across a wide population of *resource holders* and bootstraps itself to a sufficient level of quality of service and security out of the self-interest of resource holders who engage with each other via the system's underlying protocol. Depending on the design, the resulting system may scale more slowly and be less performant than a centralized system, but it offers security and resilience characteristics that can be attractive for a number of applications especially for global scale IT.

In the next section we introduce the four fundamental characteristics of resource based systems and then we expand on each one in a separate section describing the challenges that resource based system designers must overcome in order to make them successful. We also identify an end-point in the effective operation of a resource based system that arises in the form of a centralized equilibrium. We discuss the ramifications of this result and conclude with some examples of resource based systems and directions for future research.

2 Fundamental Characteristics of Resource Based Systems

Consider a service described as a program $\mathscr{F}$ that captures all the operations that users wish to perform. A resource-based realization of $\mathscr{F}$ is a system that exhibits the following four fundamental characteristics, cf. Figure 1

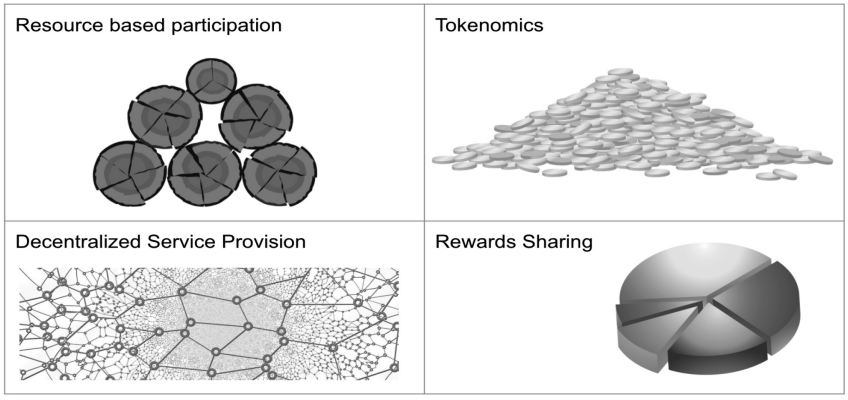


Figure 1: The four characteristic components of resource-based systems

- *Resource-based participation*. There exists a fungible resource that can be acquired by anyone interested in doing so, possibly at a cost. Entities in possession of units of the resource can exercise it to participate in the maintenance of the service, possibly incurring further costs.
- *Tokenomics*. The system issues a digital asset or currency that is used to tokenize the collective efforts of the maintainers and reward them. Such digital "coins" are maintained in cryptographic wallets and should be argued to be of sufficient utility to make system maintenance an attractive endeavor as a joint effort.
- *Decentralized service provision*. A user interacts with the service by submitting a transaction which is openly circulated in the network of maintainers provided it is well formed. Such well formedness may require the commitment of a sufficient amount of digital currency or other user expenditure to prevent spamming. The maintainers collectively take the required actions of $\mathscr{F}$ needed for the submitted transactions in a consistent and expedient fashion while the system records their efforts in a robust manner.
- *Rewards Sharing*. The digital assets that the system makes available to maintainers are distributed to the active maintainers in a regular and fair manner so that the system's safety and liveness properties emanate from their incentive driven participation. Any property violation should be a deviation from an equilibrium state that incurs costs to the perpetrators, hence ensuring the stable operation of the system.

Based on the above, implementing a given system functionality $\mathscr{F}$ by a resource based protocol requires the design of a protocol with suitable cryptographic and game theoretic characteristics. In the next four sections we delve into each characteristic in some more detail.

3 Resource-Based Participation

In classic distributed systems, system maintenance is offered by nodes that are authorized to do so either by common agreement (e.g., via a list of public-keys that identify them) or by the network connections that are assumed to exist between them (cf. [16] for an overview). Such configurations are commonly referred to in cryptographic modeling as setup assumptions.

Contrary to this, in the decentralized setting of resource-based protocols, participation to contribute to the protocol execution is attained via demonstrating the possession of a certain resource. This comes in the form of a *proof of resource*, commonly referred to as "proof-of-X" (PoX) in Bitcoin nomenclature, where X signifies the particular resource in question.

It is worth noting that this approach generalizes both the classic distributed setting, since the resource in question could be the possession of one of the authorized identities, as well as the centralized setting — in a trivial manner.

The two most widely cited such schemes are proof-of-work (PoW) and proof-of-stake (PoS). The case of PoW is exemplified in the Bitcoin blockchain protocol [25] and is essentially a proof of possession of computational power. Given the characteristics of the PoW algorithm, a specific logic or architecture may be more advantageous and as a result, maintainers may benefit from special purpose implementations. In such case, the PoW algorithm will not be a proof of general computational power, but rather a proof of ability to execute the particular algorithm utilized in the PoW scheme. This issue has brought forth significant criticism against the implementation of PoW utilized in the Bitcoin protocol (the hashcash algorithm [3] instantiated by the hash function SHA256) and subsequently a number of other PoW algorithms were developed and deployed in alternative blockchain protocols (these include scrypt, see [31], and ethash, see [33], which motivated research in memory-hardness with algorithms such as argon2 [5]).

Independently of the properties of the implementation, a common characteristic of PoW is that running the algorithm requires energy expenditure (needed to power the hardware executing the algorithm logic). This aspect, combined with the fact that the source of energy cannot be discriminated, lead to concerns about the use of non-renewable sources in the Bitcoin blockchain.

Contrary to PoW, a PoS scheme proves possession of a virtual resource (e.g., the possession of a certain amount of digital currency). A significant distinction in this class of algorithms is that issuing a PoS has cost independent of the amount of "stake" in possession of the prover, while PoW typically incurs a linear cost in terms of computational power. Examples of PoS schemes are Ouroboros [22] and Algorand [19].

Beyond stake and work, other types of resources, both virtual and physical, have been proposed and utilized. These include "proof of space", whereby the prover demonstrates possession of storage capacity, cf. [12], and "proof of elapsed time", supported by Intel SGX cf. [27], whereby the prover demonstrates that certain wait time has elapsed, just to name two examples.

An important property of PoX's in the way they are integrated within the underlying system is the fact that the freshness of the proof needs to be ensured. This is invariant of the specific resource used. In particular, it should be impossible to "replay" an old proof that refers to resources possessed at a previous point in time. This point is crucial since resources are transferable between participants and hence any proof should reflect the present state of resource allocation.

A second property that is also essential is that the verification of a PoX should be performed with low complexity, ideally independent of the level of resources involved in the generation of the proof. The reasoning behind this requirement is that verification is something that needs to be performed network wide, possibly even by entities that do not possess any units of the resource used in PoX, as such entities may still need to verify the state of the system.

4 Tokenomics

The key concept behind resource-based system tokenomics is the *tokenization* of the efforts of the system maintainers in the form of a *digital asset* that subsequently can be utilized in some way by the maintainers to influence the utility they extract from the system. The essential objective is that —collectively— maintainers' utility remains positive and hence maintenance costs can be covered and the system is viable. The necessary economics argument needed here gives rise to the term "tokenomics" as a portmanteau word derived from "token" and "economics."

The approach to achieve the tokenomics objective suggested by Nakamoto's design and built upon and extended in numerous follow up blockchain projects is *market based*. The underlying digital asset of the system becomes a native digital currency that is required for accessing the service. The system also facilitates the exchange of the digital currency between parties and hence a market is created for the IT service. Moreover, its availability for public trading allows speculators to estimate the value of the service in the near term and far future.

At system launch, it is possible to have a pre-distribution of digital coins. For instance, digital coins can be "airdropped" to token holders of a pre-existing digital currency. In other cases, digital coins can be made available to investors in a "pre-sale" stage whereby software developers of the platform may use to fund the development of the software pre-launch, cf. [7] for an exposition of some of the relevant economics considerations in this setting.

A key characteristic of the digital currency is that it should be easily transferable between parties. The coin can be listed on "cryptocurrency" exchanges and hence its value can be determined vis-à-vis other currencies (or commodities or other instruments) that potential system users may possess. Users should be able to keep the digital coin on a "wallet", an application running on a user's device. This means that a user should apply a cryptographic key in order to exercise ownership of the digital coins and issue a transaction. While users of the system have the option to perform the necessary key management themselves, they can also opt to delegate the custody of their digital assets to third parties.

After system launch, additional coins can become available and distributed following a certain ruleset to the system maintainers. Such ruleset is public knowledge and algorithmically enforced during system maintenance. Depending on the system, the rate of new coin availability can be constant per unit of time (as e.g., in Ethereum originally), or follow some function per unit of time (as e.g., in the case of Bitcoin, which has a finite total supply and hence relies on a geometric series to distribute coins to maintainers). In some cases, the number of new coins that become added to the circulating supply depend on the behavior of the maintainers, e.g., in the case of Cardano, higher coin "pledges" by the participants increase the rate that coins become available. While the ruleset is algorithmic, enforced in the system "ledger rules", it can be changed by modifying the software that supports the system, assuming there is wide consensus between the system maintainers to adopt the update (see [9] for a formal treatment of updates in blockchains). An example of such update was for instance the "London update" of Ethereum which made the total supply of coins a variable function that depends on the transactions processed by the system.

In some cases, an amount of coins is reserved to a development fund or "treasury" that the system can subsequently utilize to fund further research and development. This is exemplified in systems like Decred[1] and Cardano's Project catalyst[2] and also explored from first principles, see e.g., [34]. Such treasury can also receive funding in perpetuity by taxing the system users.

The ability to trade the system's coin enables the assessment of the system's potential value given its public tokenomics characteristics and its utility. A plunge in value of the system's coin suggest a loss of

[1] See `https://docs.decred.org/research/overview/`.
[2] See `https://projectcatalyst.org`.

faith in the system's utility and can lead to system instability due to weak participation in system maintenance or the total abandonment of maintenance and the inevitable "death" of the system. Examples of system instability are for instance the 51% attacks observed against a number of systems (e.g., Ethereum classic in [32]) while there are thousands of cryptocurrency projects that have been abandoned.[3] Trading also enables reinvesting rewards towards the acquisition of additional resources for protocol participation leading to interesting compounding effects, see e.g. [15, 20] for some interesting investigations in this direction.

While speculation can drive the price of the system's digital currency up, the real value of the token lies with the underlying functionality of the system. Ultimately, users should wish to obtain the token in order to transact with the system and engage in the functionality it offers. Given this, speculators may choose to acquire the token at an early time prior to the system's utility becoming fully realized in the hope of selling the token for profit at a future time.

To conclude, the key requirement for the above market-based tokenomics approach to achieve the essential objective identified in the beginning of this section is the following: the demand curve for the system token, as a function of time, when projected over the supply as determined by the digital currency schedule, should produce a price for the system token that offsets the collective cost of maintenance for a sufficient level of quality of service. This ensures that system maintenance, at least in the way it is encoded by the system software, is an attractive endeavor to engage in. As a final note, it is worth noting that the market-based approach, even though currently dominant in deployed resource based systems, may not be necessary for successful system tokenomics. In theory other mechanisms could also work, e.g., a reputation-based approach. As long the system is able to influence the utility of system mainainers to a sufficient degree so that quality of service is maintained, the tokenomics objective would have been met.

5 Decentralized Service Provision

Now we come to the key question how to offer the prescribed service functionality $\mathscr{F}$ while users have no specific point of contact to reach. Users package their desired input to a transaction and release that transaction to the open network. The software running in the system maintainer side should receive such transaction and in the right circumstances propagate it to the network. The system maintainers should act on this input in a timely manner and collectively the system should reach a state where the desired output is produced.

There are two important properties that the decentralized implementation of the service should provide: safety and liveness.

In terms of safety, the condition that is sought is that the system should exhibit consistency in the way it processes requests. In other words, despite being realized by a fluctuating population of system maintainers, the resulting effect of applying a certain valid input should never be incongruous to the effect that the same input would have if it was applied to $\mathscr{F}$. A safety violation for instance, would be that a user submits two mutually exclusive inputs, i.e., inputs that cannot be both applied to the state of $\mathscr{F}$ and subsequently some users observe the first input as being actioned upon by the system while others observe similarly the second input.

The liveness property refers to the ability of the system to react in a timely manner to users' input. Liveness, may be impacted both by congestion or even denial of service (DoS) attacks, where the system's capacity gets depleted as well as by censorship attacks where system maintainers choose to ignore the user's input. The expected responsiveness of the system may be affected by demand, but ideally,

[3] See for instance, `https://www.coinopsy.com/dead-coins/`.

the system should have the capability to scale up with increasing demand so that quality of service is maintained.

Given the decentralized nature of the implementation, it would be impossible to argue the above properties in all circumstances. Instead, what is sought is to argue that under reasonable resource restrictions the properties hold in the Byzantine sense – i.e., an adversary cannot violate them unless it controls a significant amount of resources. It is worth pointing out that while this is necessary, it is not sufficient; we would also want that given a reasonable modeling of the participants' utility functions, the desired system behavior is an equilibrium or even a dominant strategy, given a plausible class of demand curves for service provision. Such strategic considerations however will have to wait for the next Section on reward sharing.

While system maintainers utilize their resources to support service provision, it should be feasible for clients of the system's functionality $\mathscr{F}$ to engage in a "light weight" fashion with the system, i.e., while spending the minimum effort possible both in terms of communication as well as computational complexity and resource expenditures.

Mitigating DoS attacks can be a crucial consideration in resource-based systems given their open and distributed nature. For instance, it should be hard for malicious actor to generate a significant load of "spam" transactions and saturate the system's capacity. Collecting fees to process transactions in a native digital currency of the resource based system is a standard way that can help mitigate such DoS attacks while it also helps generating revenue for the maintainers that is proportional to the transactions processed.

A final important component of the system implementation is the ability of the system to collectively record at regular intervals relevant *performance metrics* for the system maintainers that engage with it. While not needed for providing the service to the clients, metrics are important so that the system records the efforts of maintainers so they can be rewarded appropriately. The performance metrics operation should be *robust* in the sense that, ideally, the metrics are resilient in the Byzantine sense: a set of maintainers, perhaps appropriately restricted, should not be able to manipulate the recorded performance of a targeted system maintainer. The Bitcoin blockchain uses a non-robust performance metric (the number of blocks produced by a system maintainer) which has given rise to attacks (cf. selfish-mining [14]). Other blockchain protocols in the PoW and PoS setting developed robust metrics, see [22, 29], enabling better game theoretic argumentation — e.g., proving the protocol an equilibrium in [22].

6 Rewards Sharing

In this section we come to the topic of "rewards sharing" that focuses on how individual system maintainers are being compensated and the strategic considerations that arise from that. As mentioned in section 4 the system may make digital coins available to the maintainers following a specific schedule. Additionally, maintainers may claim transaction fees that are provided by the users who engage with the system.

The operation of rewards sharing can be "action based" in the sense of rewarding directly specific actions (e.g., as in the setting of the Bitcoin blockchain where a miner who produces a block can obtain a certain amount of bitcoin as well as the fees of the transactions that are included in the block), or "epoch based" where the actions of all maintainers are examined in regular intervals and, based on performance, rewards are apportioned accordingly (e.g. in the case of the Cardano blockchain such epochs last 5 days). The distinction between action or epoch based is not very essential for the exposition of this section.

Let Ω be the finite universe of all resource units. Resource units can be exchanged between participants and some participants may hold a larger amount of resource units than others. What is a resource unit depends on the specific details of the system; it can be a hardware unit with software that is capable

of performing fast certain operations; it can be storage device; or, it can be a virtual unit controlled by a cryptographic key and maintained in a ledger.

We consider that at system launch each resource unit is labelled by its current owner and, overloading notation, we will use Ω for the set of such labelled units. The *owner partition* of Ω is a partition $O_1, \ldots, O_n$ that aggregates the units of all owners in separate sets, where n is the number of distinct owners. Such partitioning is dynamic, since resources can change hands and transfered between principals.

Resource units owners need not engage with the system as maintainers directly. Instead they can form "resource pools" where many of them together operate a system maintenance node. In such configurations it is common that one of the contributors is the operator and the others invest in the system operation — however other arrangements are also possible. Such pooling arrangements can take the form of a contract between various resource holders enabling them to operate in tandem as an organization with members having different responsibilities. The Bitcoin system over the years has exhibited significant pooling behavior and there were times that a single pool reached or even exceeded the critical threshold of controlling 51% of the total active resources.

We will use functions of the form $c : 2^{\Omega} \to \mathbb{R} \cup \{\perp\}$ to express the cost that maps a set of units to the numerical cost expenditure that is incurred when the owners of these resource units engage in the system over a fixed period of time. Note that we only require c to have a non $\perp$ value for sets of the owner partition of Ω and sets resulting by the joining of these sets.

A pooling configuration $\mathscr{P}$ is a family of mutually disjoint sets $P_1, \ldots, P_m \subseteq \Omega$ accompanied by a reward splitting strategy for each pool that describes how to distribute rewards to the resource holders who participate (if they are more than one). It is important to note that rewards sharing at the protocol level only goes up to the level of the pool; beyond that, by the nature of resource based systems, it can be infeasible for the system to distinguish between a pool of a single resource holder compared to one where many join their resources.

Pooling configurations are an important subject of study in resource based systems since they reflect the "decentralization" of the underlying system. A stable centralized pooling configuration, e.g., one where all operators have joined a single pool, Ω, indicates that the resource based system can be retired and substituted by a centralized system supported by an organization reflecting the constituent membership of the single pool. In such circumstances, the benefits of using a resource based system entirely dissipate. As a result, it is of interest to understand in what settings such centralized pooling configurations may arise.

Before we proceed, it is useful to introduce a metric for resource sets. We will use that metric to signify the influence that any single pool can exert on the protocol. We denote the measure $\sigma : 2^{\Omega} \to \mathbb{R}$ of the resources of a pool P by $\sigma(P)$. We require that $\sigma(\Omega) = 1, \sigma(\emptyset) = 0$ and $\sigma(P \cup Q) = \sigma(P) + \sigma(Q) - \sigma(P \cap Q)$.

Rewards sharing in resource based systems is controlled by a function ρ; without loss of generality we count the rewards distributed in a fixed period of time (the same period over which we also consider costs). Let $\rho(P, \mathscr{P})$ be the rewards provided to a given pool P by the system given a pooling configuration $\mathscr{P}$. A reward function $\rho(\cdot)$ is called *simple* if $\rho(P, \mathscr{P}) = \rho(P, \mathscr{P}')$ for any pooling configurations $\mathscr{P}, \mathscr{P}'$ that contain P. For simple reward functions we can write $\rho(P)$ to denote the rewards that are provided to P. Note moreover that $\rho(\emptyset) = 0$. A reward function is continuous if it holds that for every $P \subseteq \Omega, \epsilon > 0$ there is a $\delta > 0$ such that for any P', $|\sigma(P) - \sigma(P')| < \delta \implies |\rho(P) - \rho(P')| < \epsilon$. In the exposition of this section we consider only continuous simple reward functions.

The reward function ρ is a critical component of a resource based system. We put forth the following set of axioms regarding the reward function ρ. As we will see, these axioms have certain implications regarding the pooling configurations that may arise in the system.

– Resource fungibility. For any P, Q, $(\sigma(P) = \sigma(Q)) \to (\rho(P) = \rho(Q))$. This means that the system does not distinguish between particular resource units with respect to rewards.

– Sybil resilience. It holds that $\rho(P_1 \cup P_2) \geq \rho(P_1) + \rho(P_2)$ for any disjoint sets $P_1, P_2 \subseteq \Omega$. This reflects the desideratum that an operator controlling some resources will not gain anything by splitting their resources into two pools.

– Egalitarianism. It holds $\rho(P) \leq \rho(Q) + \rho(R)$ for any disjoint sets P, Q, R such that $\sigma(P) = \sigma(Q) + \sigma(R)$. This reflects the desideratum that a "rich" operator controlling resources P does not obtain more rewards than two "poorer" operators controlling in aggregate the same amount of resources.

Given the above axioms, we will prove that a centralized pooling configuration can be a Nash equilibrium in the strong sense, i.e., even taking into account arbitrary coalitions [2]. We need two more properties to be defined first.

Definition 1. Consider a pooling configuration $\mathscr{P}$. A pool $P \in \mathscr{P}$ is called: (i) *viable*, if and only if $\rho(P) \geq c(P)$, (ii) *cost efficient*, if and only if $c(P)/\sigma(P) \leq c(P')/\sigma(P')$, for any $P' \subseteq P$, i.e., its cost per unit of resource is no worse than any of its subsets.

We are now ready to state and prove the following theorem.

Theorem 1. *If Ω is viable and cost efficient, then there is a centralized pooling configuration that is a Strong Nash equilibrium.*

Proof. Consider first any pooling configuration $\mathscr{P}$ and $P \in \mathscr{P}$ such that it is viable and cost efficient. The rule to distribute rewards within P is the following. Any subset S of P corresponding to a participant receives rewards equal to $\sigma(S)(\rho(P) - c(P))$, i.e., a "fair" share of the total rewards available. We observe that:

$$\sigma(S)(\rho(P) - c(P)) \geq \sigma(S)\rho(P) - \sigma(P)c(S) \geq \sigma(P)\rho(S) - \sigma(P)c(S) = \sigma(P)(\rho(S) - c(S)) \tag{1}$$

The first inequality follows from the cost efficiency of P, which implies $c(S)/\sigma(S) \geq c(P)/\sigma(P)$.

For the second inequality we need to prove $\rho(P)/\sigma(P) \geq \rho(S)/\sigma(S)$, i.e., the rewards per unit of resource is no worse for P compared to S. We will prove something stronger. For any $x \in [0,1]$ we define $\hat{\rho}(x)$ to be equal to the value $\rho(P)$ for some P with $\sigma(P) = x$. The function $\hat{\rho}$ is well defined due to resource fungibility. Furthermore, observe that $\hat{\rho}$ is superadditive due to Sybil resilience, and subadditive due to Egalitarianism. It follows that $\hat{\rho}$ satisfies Cauchy's functional equation and as a result, due to the continuity of $\hat{\rho}(\cdot)$, it holds that $\hat{\rho}(x) = \gamma x$, for some $\gamma \in \mathbb{R}$. From this we derive that $\rho(S)/\sigma(S) = \gamma = \rho(P)/\sigma(P)$.

We conclude by setting $P = \Omega$. Due to $\sigma(\Omega) = 1$, by equation 1, the profit of S, equal to $\rho(S) - c(S)$, is no better than the rewards received as part of the centralized configuration which equals to $\sigma(S)(\rho(\Omega) - c(\Omega))$. This implies that any set of participants will be no better off operating their own pool separating from the centralized pool Ω. The same also holds in case they decide to run multiple separate pools. □

It follows that it is of interest to detect large cost efficient resource sets. To this end, we examine an important class of cost functions, that we call "operator-linear." First, let $O_1, \ldots, O_n$ be the owner partition of Ω. The cost function is operator linear if it holds that (i) for all $i = 1, \ldots, n$, $c(O_i) = c_i + d_i \cdot \sigma(O_i)$, and (ii) for any $P = \cup_{j=1}^{m} O_{i_j}$, it holds the cost of P is defined by the following function

$$c(P) = d_{i_1} \cdot \sigma(O_{i_1}) + \ldots d_{i_m} \cdot \sigma(O_{i_m}) + \min\{c_{i_1}, \ldots, c_{i_m}\}.$$

This class of cost functions captures, at a certain level of abstraction, both proof of work and proof of stake systems where pooling is organized so that the operator becomes the resource holder with the smaller individual fixed cost. For proof of stake, given the cost incurred for processing is independent of the resources held, one can set $d_i = 0$ for all $i = 1, \ldots, n$. For proof of work, we observe the linear dependency in the amount of resources held that can be reflected by choosing a suitable value for d_i derived from electricity costs and equipment characteristics used for performing the proof of work operation. We now prove the following proposition.

Proposition 1. *Given an operator-linear cost function, Ω is cost efficient, as long as $\Delta \leq \min\{c_1, \ldots, c_n\}$, where $\Delta = \max\{d_i - d_j \mid i, j \in [n]\}$.*

Proof. We want to prove that $c(\Omega) \leq c(S)/\sigma(S)$ for any $S \subseteq \Omega$. Let us denote by $x_i = \sigma(O_i)$, where $O_1, \ldots, O_n$ is the owner partition of Ω. Without loss of generality we assume that S includes the operators $O_1, \ldots, O_k$ for some $k \leq n$. We also denote by $c_j = \min\{c_1, \ldots, c_j\}$. We want to prove that

$$(c_n + \sum_{i=1}^{n} d_i x_i) \cdot \sum_{i=1}^{k} x_k \leq c_k + \sum_{j=1}^{k} d_j x_j$$

We observe that based on the condition in the proposition's statement, we have that $\Delta \cdot \sum_{i=1}^{k} x_j \leq c_k$ which implies that $\sum_{j=1}^{k} (d_i - d_j) x_j x_i \leq c_k x_i$. Summing for all $i = k+1, \ldots, n$, we have that

$$\sum_{i=k+1}^{n} \sum_{j=1}^{k} (d_i - d_j) x_i x_j \leq c_k \sum_{i=k+1}^{n} x_i \Rightarrow \sum_{i=k+1}^{n} \sum_{j=1}^{k} d_i x_i x_j \leq \sum_{i=k+1}^{n} \sum_{j=1}^{k} d_j x_i x_j + c_k \sum_{i=k+1}^{n} x_i$$

We add now in both sides of the inequality the terms $\sum_{i,j=1}^{k} d_i x_i x_j$ and $c_k \sum_{i=1}^{k} x_i$ and by the observation $c_n \leq c_k$, we have the inequality

$$c_n \sum_{i=1}^{k} x_i + \sum_{i=1}^{n} \sum_{j=1}^{k} d_i x_i x_j \leq \sum_{i=1}^{n} \sum_{j=1}^{k} d_j x_i x_j + c_k \sum_{i=1}^{n} x_i$$

From this we obtain $(c_n + \sum_{i=1}^{n} d_i x_i) \sum_{i=1}^{k} x_i \leq c_k + \sum_{j=1}^{k} d_j x_j$ that proves $c(\Omega) \leq c(S)/\sigma(S)$. □

Based on the above, we obtain that if Ω is viable and the conditions of proposition 1 are satisfied, the system will have a strong Nash equilibrium that centralizes to one operator. This applies to both proof of stake as well as proof of work in the case when differences in electricity costs are small across operators.

On the other hand, in settings where cost efficiency does not hold, the joining of two resource sets can become undesirable for one of the two operators. A weaker property for cost functions that captures "economies of scale" and dictates that $c(P_1 \cup P_2) \leq c(P_1) + c(P_2)$, (reflecting the property that merging two pools results in no higher costs compared to the two pools operating alone), is insufficient by itself to imply a centralized pooling configuration.

Even in the case of operator-linear cost functions however, careful design of the reward function and analysis of Nash dynamics can show that better equilibria arise and can be reachable by the participants. For instance, if costs for "off-chain" pooling are high, the rewards sharing schemes developed and analyzed in [6] can be seen to converge to highly participatory decentralized equilibria for constant cost functions.

7 A high-level blueprint for a stake-based system

Given the four characteristics outlined in the previous sections, we will provide an illustration how to apply those to develop and deploy a *stake-based* system. We assume as preconditions that the developer has already a classical distributed protocol implementation of the service $\mathcal{F}$ for, say, k parties and has an understanding of the service maintenance costs and user demand.

Adopting a stake-based approach, the resource will be digital coins. The developer mints an initial supply of such coins and disperses them over an existing population of recipients. This can be achieved by e.g., "airdropping" such digital coins to cryptocurrency holders of an existing blockchain platform. Due to this distribution event, the recipients become the stakeholders of the system.

A tokenomics schedule that takes into account the expected demand is determined and programmed into a smart contract $\mathscr{S}$. This contract will acknowledge the initial supply of coins as well as the schedule under which any new coins will be made available to the maintainers – the entities running the k-party protocol. Following market-based tokenomics the contract will also manage incoming transaction fees.

Decentralized service provision is comprised of four parts. One is the k-party protocol that implements $\mathscr{F}$; the second is a proof-of-stake blockchain protocol that offers "dynamic availability" (e.g., such as Ouroboros, [4, 22]) – i.e., a protocol that can handle a wide array of participation patterns without the requirement to be able to predict closely the active participation level). Inputs to the protocol will be recorded on chain, an action that will incur transaction costs to be withheld by $\mathscr{S}$. The third part is a "proof-of-service" sub-system that should enable any system maintainer running the k-party protocol to demonstrate their efforts in a robust way. The verifier of such proofs will be the smart contract $\mathscr{S}$ which will determine a performance factor for each maintainer. Finally, the fourth part is an algorithm that will parse the blockchain at regular intervals and determine the k parties to run the k-party protocol for $\mathscr{F}$. This can be done e.g., by weighted sampling [13], taking into account the stake supporting each operator.

For rewards sharing, we need a mechanism to incentivize the stakeholders to organize themselves into at least k well functioning nodes that will execute the multiparty protocol for $\mathscr{F}$ when selected. To achieve this we can deploy the reward sharing scheme of [6] over the underlying PoS blockchain; for that scheme it is shown how incentive driven engagement by the stakeholders can determine a set of k nodes at equilibrium. The reward scheme will be coded into the contract $\mathscr{S}$ and will reward the stakeholders at regular intervals using the available supply from the tokenomics schedule and the transaction fees collected. The performance factor of each operator will influence the rewards, adjusting them in proportion to the operator's efforts.

The developer will produce an implementation of the above system and will make it available for download. A launch date for the system will be set as well as an explanation for its purpose. At this point, the developer's engagement can stop. The stakeholders —the recipients of the newly minted digital coin— can examine the proposition that the system offers and choose whether to engage or not. If a non-negligible number of them chooses to engage out of their own self-interest (which will happen if the developer's predictions regarding the long term utility of $\mathscr{F}$ are correct) the system will come to life bootstrapping itself.

8 Concluding remarks

In this paper, we put forth a new paradigm for deploying Information Technology services inspired by the operation of the Bitcoin system. We identified four characteristics of resource based systems: (i) resource-based operation, (ii) tokenomics, (iii) decentralized service provision, and (iv) rewards sharing, and we elaborated on their objective and associated design challenges. We also presented a high-level blueprint showing how the paradigm can materialize in the form of a stake-based system.

In more details, we identified the cryptographic and distributed protocol design challenge which asks for a suitable PoX algorithm integrated with a protocol that facilitates decentralized service provision and the requirement of robust performance metrics. We also pointed to the economics and game theoretic considerations related to tokenomics and reward sharing.

We explored at some length game theoretic aspects of pooling behavior and proved that a centralized equilibrium can be a strong Nash equilibrium for a wide variety of reward and cost functions. This result is in the same spirit but more general than previous negative results presented in [1, 23, 24] as it does not rely on the distribution of resources across owners, or a specific "economies of scale" assumption that dictates a superlinear relation between rewards and costs, or the specific reward scheme used in Bitcoin,

respectively.

On a more positive note, existence of "bad equilibria" does not prohibit the existence of other equilibria with better decentralization profiles. Furthermore, centralized pooling configurations require coordination between agents that may prove difficult and costly to achieve. In this respect, "bimodal" systems, see [21], where users can perform two (or more) actions to engage in system maintenance (e.g., propose themselves as operators as well as vote others as operators) examples of which include [6, 8], show promise in this direction. Furthermore, being able to investigate the Nash dynamics of the system as e.g., performed in [6] is crucial to demonstrate that the system reaches desirable equilibria expediently and moreover it can be also possible to demonstrate that bad equilibria can be avoided. It is also worth pointing out that even if a resource based system manages to scale but eventually centralizes, the invested efforts may still not be completely in vain: the resulting constituent membership of the centralized pool organization may take over as a centralized system and offer the service.

The characteristics put forth in this paper are, in many respects, the minimum necessary. Other desirable features can be argued such as the existence of multiple, open source software codebases that realize the system's protocol as well as the existence of a governance sub-system that facilitates operations such as software updates not only for correcting the inevitable software bugs but also ensuring the system adapts to run time conditions that were unanticipated during the initial design. The problem of software updates in the decentralized setting is complex and more research is required, cf. [9] for some first steps in terms of formally defining the problem in the context of distributed ledgers.

The resource based paradigm is still in its very beginning. Nevertheless, we can identify some early precursors that include smart contract systems — e.g., Ethereum and Cardano, the name service of Namecoin, or the cross border payment system of Ripple. More recently, the Nym network [10] exemplified the paradigm in a novel context — that of mix-nets and privacy-preserving communications. Extending the paradigm to additional use cases will motivate further advances in cryptography, distributed systems and game theory and eventually has the potential to change the landscape of global information technology.

9 Acknowledgements

I am grateful to Dimitris Karakostas, Aikaterini Panagiota Stouka and Giorgos Panagiotakos for helpful comments and discussions.

References

[1] Nick Arnosti and S. Matthew Weinberg. Bitcoin: A natural oligopoly. In Avrim Blum, editor, *10th Innovations in Theoretical Computer Science Conference, ITCS 2019, January 10-12, 2019, San Diego, California, USA*, volume 124 of *LIPIcs*, pages 5:1–5:1. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2019.

[2] Robert J. Aumann. Acceptable points in general cooperative n-person games. In *Contributions to the Theory of Games*, volume IV of *Annals of Mathematics Studies*, pages 287–324, 1959.

[3] Adam Back. Hashcash. http://www.cypherspace.org/hashcash, 1997.

[4] Christian Badertscher, Peter Gazi, Aggelos Kiayias, Alexander Russell, and Vassilis Zikas. Ouroboros genesis: Composable proof-of-stake blockchains with dynamic availability. In David Lie, Mohammad Mannan, Michael Backes, and XiaoFeng Wang, editors, *Proceedings of the 2018 ACM SIGSAC*

Conference on Computer and Communications Security, CCS 2018, Toronto, ON, Canada, October 15-19, 2018, pages 913–930. ACM, 2018.

[5] Alex Biryukov, Daniel Dinu, Dmitry Khovratovich, and Simon Josefsson. Argon2 memory-hard function for password hashing and proof-of-work applications. *RFC*, 9106:1–21, 2021.

[6] Lars Brünjes, Aggelos Kiayias, Elias Koutsoupias, and Aikaterini-Panagiota Stouka. Reward sharing schemes for stake pools. In *IEEE European Symposium on Security and Privacy, EuroS&P 2020, Genoa, Italy, September 7-11, 2020*, pages 256–275. IEEE, 2020.

[7] Christian Catalini and Joshua S. Gans. Initial coin offerings and the value of crypto tokens. Working Paper 24418 https://www.nber.org/papers/w24418, March 2018.

[8] Alfonso Cevallos and Alistair Stewart. A verifiably secure and proportional committee election rule. In *AFT '21: 3rd ACM Conference on Advances in Financial Technologies, 2021*, 2021.

[9] Michele Ciampi, Nikos Karayannidis, Aggelos Kiayias, and Dionysis Zindros. Updatable blockchains. In Liqun Chen, Ninghui Li, Kaitai Liang, and Steve A. Schneider, editors, *Computer Security - ESORICS 2020 - 25th European Symposium on Research in Computer Security, ESORICS 2020, Guildford, UK, September 14-18, 2020, Proceedings, Part II*, volume 12309 of *Lecture Notes in Computer Science*, pages 590–609. Springer, 2020.

[10] Claudia Diaz, Harry Halpin, and Aggelos Kiayias. The nym network: The next generation of privacy infrastructure. https://nymtech.net/nym-whitepaper.pdf, February 2021.

[11] John R. Douceur. The sybil attack. In Peter Druschel, M. Frans Kaashoek, and Antony I. T. Rowstron, editors, *Peer-to-Peer Systems, First International Workshop, IPTPS 2002, Cambridge, MA, USA, March 7-8, 2002, Revised Papers*, volume 2429 of *Lecture Notes in Computer Science*, pages 251–260. Springer, 2002.

[12] Stefan Dziembowski, Sebastian Faust, Vladimir Kolmogorov, and Krzysztof Pietrzak. Proofs of space. In Rosario Gennaro and Matthew Robshaw, editors, *Advances in Cryptology - CRYPTO 2015 - 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part II*, volume 9216 of *Lecture Notes in Computer Science*, pages 585–605. Springer, 2015.

[13] Pavlos S. Efraimidis and Paul (Pavlos) Spirakis. Weighted random sampling. In *Encyclopedia of Algorithms*, pages 2365–2367. 2016.

[14] Ittay Eyal and Emin Gun Sirer. Majority is not enough: Bitcoin mining is vulnerable. In *Financial Cryptography*, 2014.

[15] Giulia C. Fanti, Leonid Kogan, Sewoong Oh, Kathleen Ruan, Pramod Viswanath, and Gerui Wang. Compounding of wealth in proof-of-stake cryptocurrencies. In Ian Goldberg and Tyler Moore, editors, *Financial Cryptography and Data Security - 23rd International Conference, FC 2019, Frigate Bay, St. Kitts and Nevis, February 18-22, 2019, Revised Selected Papers*, volume 11598 of *Lecture Notes in Computer Science*, pages 42–61. Springer, 2019.

[16] Juan A. Garay and Aggelos Kiayias. Sok: A consensus taxonomy in the blockchain era. In Stanislaw Jarecki, editor, *Topics in Cryptology - CT-RSA 2020 - The Cryptographers' Track at the RSA Conference 2020, San Francisco, CA, USA, February 24-28, 2020, Proceedings*, volume 12006 of *Lecture Notes in Computer Science*, pages 284–318. Springer, 2020.

[17] Juan A. Garay, Aggelos Kiayias, and Nikos Leonardos. The bitcoin backbone protocol: Analysis and applications. In Elisabeth Oswald and Marc Fischlin, editors, *Advances in Cryptology - EUROCRYPT 2015 - 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26-30, 2015, Proceedings, Part II*, volume 9057 of *Lecture Notes in Computer Science*, pages 281–310. Springer, 2015.

[18] Juan A. Garay, Aggelos Kiayias, and Nikos Leonardos. The bitcoin backbone protocol with chains of variable difficulty. In *Advances in Cryptology - CRYPTO 2017 - 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20-24, 2017, Proceedings, Part I*, pages 291–323, 2017.

[19] Yossi Gilad, Rotem Hemo, Silvio Micali, Georgios Vlachos, and Nickolai Zeldovich. Algorand: Scaling byzantine agreements for cryptocurrencies. In *Proceedings of the 26th Symposium on Operating Systems Principles, Shanghai, China, October 28-31, 2017*, pages 51–68. ACM, 2017.

[20] Dimitris Karakostas, Aggelos Kiayias, Christos Nasikas, and Dionysis Zindros. Cryptocurrency egalitarianism: A quantitative approach. In Vincent Danos, Maurice Herlihy, Maria Potop-Butucaru, Julien Prat, and Sara Tucci Piergiovanni, editors, *International Conference on Blockchain Economics, Security and Protocols, Tokenomics 2019, May 6-7, 2019, Paris, France*, volume 71 of *OASIcs*, pages 7:1–7:21. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2019.

[21] Aggelos Kiayias. Blockchain reward sharing - a comparative systematization from first principles. IOHK Blog, https://iohk.io/en/blog/posts/2020/11/30/blockchain-reward-sharing-a-comparative-systematization-from-first-principles/, November 30 2020.

[22] Aggelos Kiayias, Alexander Russell, Bernardo David, and Roman Oliynykov. Ouroboros: A provably secure proof-of-stake blockchain protocol. In *Advances in Cryptology - CRYPTO 2017 - 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20-24, 2017, Proceedings, Part I*, pages 357–388, 2017.

[23] Aggelos Kiayias and Aikaterini-Panagiota Stouka. Coalition-safe equilibria with virtual payoffs. In *AFT '21: 3rd ACM Conference on Advances in Financial Technologies, 2021*, 2021.

[24] Yujin Kwon, Jian Liu, Minjeong Kim, Dawn Song, and Yongdae Kim. Impossibility of full decentralization in permissionless blockchains. In *Proceedings of the 1st ACM Conference on Advances in Financial Technologies, AFT 2019, Zurich, Switzerland, October 21-23, 2019*, pages 110–123. ACM, 2019.

[25] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. http://bitcoin.org/bitcoin.pdf, 2008.

[26] Satoshi Nakamoto. Bitcoin open source implementation of p2p currency. http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source, February 2009.

[27] Kelly Olson, Mic Bowman, James Mitchell, Shawn Amundson, Dan Middleton, and Cian Montgomery. Sawtooth: An introduction. https://www.hyperledger.org/wp-content/uploads/2018/01/Hyperledger_Sawtooth_WhitePaper.pdf, January 2018.

[28] Rafael Pass, Lior Seeman, and Abhi Shelat. Analysis of the blockchain protocol in asynchronous networks. In *Advances in Cryptology - EUROCRYPT 2017 - 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Paris, France, April 30 - May 4, 2017, Proceedings, Part II*, pages 643–673, 2017.

[29] Rafael Pass and Elaine Shi. Fruitchains: A fair blockchain. In Elad Michael Schiller and Alexander A. Schwarzmann, editors, *Proceedings of the ACM Symposium on Principles of Distributed Computing, PODC 2017, Washington, DC, USA, July 25-27, 2017*, pages 315–324. ACM, 2017.

[30] Marshall C. Pease, Robert E. Shostak, and Leslie Lamport. Reaching agreement in the presence of faults. *Journal of the ACM*, 27(2):228–234, 1980.

[31] Colin Percival and Simon Josefsson. The scrypt password-based key derivation function. *RFC*, 7914:1–16, 2016.

[32] Zack Voell. Ethereum classic hit by third 51 CoinDesk `https://www.coindesk.com/markets/2020/08/29/ethereum-classic-hit-by-third-51-attack-in-a-month/`, August 2020.

[33] Gavin Wood. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper*, 151:1–32, 2014.

[34] Bingsheng Zhang, Roman Oliynykov, and Hamed Balogun. A treasury system for cryptocurrencies: Enabling better collaborative intelligence. In *26th Annual Network and Distributed System Security Symposium, NDSS 2019, San Diego, California, USA, February 24-27, 2019*. The Internet Society, 2019.

```
---------------------------
Version - Catalogue of changes
0.5  - first limited public release - Presentation at CBER Webinar. December 2nd 2021.
0.6  - various improvements to tokenomics section. first public release.
0.7  - inclusion of high-level blueprint section
0.75 - minor edits and improvements.
0.77 - typos and minor edits.
```


The CHAIRMAN. Thank you, Mr. Hoskinson.

At this time, Members will be recognized for questions in order of seniority, alternating between Majority and Minority Members. Members will be recognized for 5 minutes each in order to allow us to get to as many questions as possible. Please keep your microphones muted until you are recognized, especially on the Zoom, in order to minimize background noise.

I will now recognize myself for 5 minutes.

Mr. Brummer, should CFTC have direct statutory authority to regulate cash markets?

Dr. BRUMMER. Well, the CFTC, as I said, is certainly up to the job under a certain number of circumstances.

Number one, obviously it has to be financed and resourced properly. Second, and this is really the point of the conversation, all the regulatory agencies have to really have a change in their mindset. I think what you have heard from almost all the witnesses is that the underlying infrastructure is very different from the infrastructure upon which many of our both securities and derivatives laws are based, and to really adequately oversee these markets, some degree of familiarity with those markets is going to be necessary. So, whether or not the SEC or the CFTC, but the CFTC is certainly up to the job. It has certain kinds of comparative advantages, and it is those advantages that should be leveraged and to build upon those areas like disclosure where it has not traditionally wielded its authority.

The CHAIRMAN. Right. I am struck by the line in your testimony where you said it will necessarily involve revisiting longstanding assumptions about market infrastructures embedded in securities and derivatives law and adapting the regulatory system in creative ways that reflect the best of our experience and collective values. What does that mean?

Dr. BRUMMER. Yes, it means, for example, in the securities law context, our entire disclosure system is based of an assumption that issuers have non-public information that other expert actors don't have, and so, therefore, to make sure that that information is available to them and it kind of trickles down to your retail investor. So, it is based—the evolution part disclosure system, even in securities law, is for information to be filed but not really read.

When you go and you operate on a blockchain, it is completely different context. In part, because much of the material, not all, but much of the material information that you would need is already available on chain, but is only accessible to the expert actors. It is the retail folks who would not have the ability to read and understand the source code. So, that gets you into a question as to what should the disclosure system look like? It should probably have more consumer protection principles and to think about how do you get that information to those people in that system?

The CHAIRMAN. Yes, it is a great question, but the one before it is the one I am most interested in, which is who is best to do that? That brings me back to my first question, because I listened closely to your answer. I understand it is complicated and I understand the concerns about how it be done, which is actually very, very important. Is CFTC up to that?

Dr. BRUMMER. CFTC is up to the job. It has the experience, in some ways, more direct experience in some ways dealing with these issues than any other agency in the government. It is up to the job, but again, not to be too law professory, but context matters and it has to be properly resourced to do the job.

The CHAIRMAN. Right. Mr. McGonagle, good news. The professor says you are up to the job. Can you shed any light on my question, sir, because I think the thing where, at least that I am very interested in, is it seems clear we need to legislate in this area, and we need to understand the follow-on consequences of that. So, help me understand if we were to give direct statutory authority to CFTC for the cash, spot markets, what should that look like?

Mr. MCGONAGLE. Thank you, Mr. Chairman, I appreciate the question.

At the CFTC, we are a market regulator. We think about how individual market participants from all aspects of, say, the production and user chain might access our markets in order to hedge risk or manage risk exposure. So, interesting compared to the professor who is definitely spending some time thinking about, like, how the commodity could be used. The CFTC thinks about how individuals are interested in the change and value of that commodity or digital asset, and how that transaction and that interest in that change in value can be regulated. That is what our system of regulation is meant to accomplish. We look at market participants that are interested in trading value and they are doing that in a centralized marketplace where there is price transparency and where they have execution certainty. They are able to get the product, the interest that they want, and they are able to do that in a safe and secure manner.

The CHAIRMAN. Isn't the critical wrinkle here that there is more speculation in the spot market with digital assets than there would be with the traditional commodity, and are you guys better set up for that?

Mr. MCGONAGLE. So, for sure when you see in the commodity—in the spot market, there is significant speculative interest also on a leveraged basis, so putting a little money down——

The CHAIRMAN. At the retail level?

Mr. MCGONAGLE. Exactly, and trading significant funds with significant risks. In a regulated market space, we have the opportunity—again, talking about disclosure obligations—to help inform those customers about this is the type of transaction that you are getting into, and making sure to the best that we are able to facilitate customer protection so that they understand the risks and they are prepared to accept those risks. We also have safeguards in place to protect those assets to be more stable.

The CHAIRMAN. All right. Well, I thank the gentleman. If we have time for a second round, I would be particularly interested in the subject Dr. Brummer opened in terms of the innovative ways we have to think about this, given the differences between this and what we have traditionally dealt with.

I am pleased to recognize the Ranking Member and to extend her the same time allotment that I consumed.

Mrs. FISCHBACH. Thank you very much, Mr. Chairman, and I can't not comment on Dr. Brummer saying it is hard for him not to be too law professory. So, I was a law student. There is a lot of law professory stuff going on. So, I appreciate it.

But——

The CHAIRMAN. I was more struck by the fact that he said we are his favorite Members of Congress——

Mrs. FISCHBACH. There you go.

The CHAIRMAN. And this Committee.

Dr. BRUMMER. I am a kid from Arkansas.

Mrs. FISCHBACH. But turning back to a little bit—the chair was asking a little bit about the CFTC, and I just wanted to ask, Mr. McGonagle, the CFTC is often referred to as a principle-based regulator. Could you tell us a little bit about what that means gen-

erally in your experience with that approach as it has been applied?

Mr. MCGONAGLE. Yes, thank you.

The question around principle-based articulates that there are 23 core principles for designated contract markets that basically sets up the system of obligations that the entity has to comply with in order to list products for trading on our designated contract markets. And so, they will cover grounds including system safeguard, for example. Core principles also require that products that are listed not be readily susceptible to manipulation, and that there be customer protections available. Core principals also provide for the certainty of execution, for example, of the transaction, that you are able to have a counterparty that minimizes the risk, and we do that through a clearing system. Each market will have one clearing organization that will be the counterparty for all the market's transaction.

So, we are looking at a program of responsibility that not only is the CFTC administering the law through application review, compliance, and surveillance. These designated contract markets also have responsibility on the self-regulatory basis to make sure that their market participants are complying with the rules. And the CFTC has broad enforcement authority to make sure that those market participants comply with the Commodity Exchange Act and the regulations.

Mrs. FISCHBACH. Thank you, and maybe just, I have heard criticism about the CFTC, that it is a permissive light touch regulator, and would you agree with that, and if not, could you tell us some of your personal experiences why that criticism is unfounded?

Mr. MCGONAGLE. Absolutely. So, at the CFTC, we strongly value our enforcement program, and a strong enforcement program supports market integrity and customer protection. If people know that the rules of the road are supposed to be followed and that there is going to be a swift and strong response, that encourages compliance activity. So, while we have a comprehensive regulatory framework, we also have a very strong enforcement program.

As I mentioned in my opening remarks, we filed 50 cases on digital assets. We brought those cases starting in 2014. We are looking at fraud, pump and dump manipulation, illegal contracts that are being offered to U.S. customers, not only within the U.S., but also from entities outside of the U.S. If there is a violation of the Act or our regulations, the CFTC is a strong enforcement authority to deter that misconduct. If it involves a criminal violation, we work closely with our cooperative enforcement partners at the Department of Justice as well as the U.S. Attorney Offices.

Mrs. FISCHBACH. Thank you very much. I appreciate the information.

Mr. Hoskinson—did I say that—I am trying here.

Mr. HOSKINSON. Yes.

Mrs. FISCHBACH. Thank you very much, and I know we just have a few seconds left, but there is a lot of discussion about whether we should regulate certain cryptocurrency as commodities or securities.

What do you think are the benefits, and maybe you could talk just a little bit about that, what are the drawbacks, things like that?

Mr. HOSKINSON. Well, with 37 seconds——

Mrs. FISCHBACH. I know. I am sorry. Yes.

The CHAIRMAN. The gentleman can take as much time as he requires.

Mrs. FISCHBACH. Oh, thank you, Mr. Chairman. There you go.

Mr. HOSKINSON. Thank you.

The CHAIRMAN. I mean, don't push it, but——

Mrs. FISCHBACH. It is a fine line here.

Mr. HOSKINSON. You got to be careful. I am Italian.

So, when you look at cryptocurrencies in general, I have always viewed them like financial stem cells. They are kind of more fundamental than a particular category like a currency or a commodity. And really, it depends on the markets they are traded on and the use and utility that they have. But at the end of the day, you have to ask yourself what public policy considerations are you attempting to satisfy? Is it sanctions compliance? Is it consumer protection? Is it market stability? What we do as an industry is we are all about transparency. So, it is kind of funny that we are talking and debating about disclosure regimes. There is no other financial asset in the world that really is as transparent as a cryptocurrency. Every transaction from the very beginning—for Bitcoin, for example, from January 3, 2009, is known. Every single one. The holdings of the founder are known because all of these things are publicly available to everybody.

So, it is more about, in my view, understandability and the tooling required to make this work on a global basis. So, I don't think it would be wise to say, well, is it a security or a commodity, or fall into this temptation of who is the more permissive regulator or what is the regulatory arbitrage, but rather, just take a step back and say what things do we want to guard against? And we now have 13 years of history as an industry of six or seven collapses, a whole bunch of interesting new things like NFTs that have always pushed the limit, and a global marketplace with more than 100 million people floating around that we can draw from and we can look on a case-by-case basis, and build a framework that makes sense.

What is encouraging to me as an entrepreneur, briefly, is that there is a lot of great legislation that has been proposed recently, like the DCEA, the FIA, there are Executive Orders that have come through that are trying to force clarity amongst the Executive Branch. So, these things together create global dialogue, and if we are clever about it, I think we can converge to a reasonable compromise that we as an industry can live with and continue to be competitive with.

Mrs. FISCHBACH. Thank you very much. I appreciate that, and thank you, Mr. Chairman, for your indulgence.

The CHAIRMAN. I thank the gentlelady.

I would like to yield to the Ranking Member if he has any questions, Mr. Thompson.

Mr. THOMPSON. Mr. Chairman, thank you so much.

Mr. McGonagle, first of all, thank you for your dedicated service, and your experience at CFTC, it is much appreciated.

Earlier this year, as noted a number of times, I introduced the Digital Commodity Exchange Act (H.R. 7614), DCEA, along with Mr. Khanna, Mr. Emmer, and Mr. Soto. Among other things, the DCEA creates a new registered entity, a *digital commodity exchange, DCE,* that is subject to a registration and compliance regime. This is similar to the existing registered futures exchanges and swap execution facilities under the Commodity Exchange Act.

Can you please tell us generally about the requirements CFTC imposes on futures exchanges and the SEFs?

Mr. MCGONAGLE. I am sorry, Ranking Member. The door opened and I missed the last phrase. If you could just restate that for me?

Mr. THOMPSON. I just noted that under the DCEA, what we have done with DCEA and there was a similar—it was very similar to the existing registered futures exchange and swap execution facilities under the current Commodity Exchange Act. And so, the question was can you tell us generally about the requirements the CFTC imposes on future exchanges and SEFs?

Mr. MCGONAGLE. Great, thank you, Ranking Member, and I appreciate you indulging me with following up.

With respect to designated contract markets and swap execution facilities, those entities are responsible to establish and set up. They are self-regulatory organizations. So the rules that they implement on their platforms are the rules that they also have to ensure that there is compliance with. So, for example, they will establish trading protocols and they will establish prohibitions concerning market abuse. That self-regulatory organization responsibility is to make sure then that those market participants follow the rules of the road.

At the same time, the self-regulatory organization has responsibilities to the Commission and to Congress as part of the 23 core principles. So, for example, they need to make sure that their trading platforms are cyber resilient. That is, they must have the ability to operate in the event that someone attempts to breach their system, that they have capacity to roll over, for example, to another trading platform to allow trading to continue. It is incredibly important that our markets be able to operate efficiently at all times for our market participants who are trading in the markets who have risk exposure that they need to manage.

Mr. THOMPSON. Thank you for that.

Dr. Brummer, as Ranking Member Fischbach alluded to, there is some uncertainty about when and if an asset is a commodity or a security, and some argue that the vast majority of digital assets are just securities. Is the law clear on this?

Dr. BRUMMER. No, and if it was, all of my students would be getting an A in my securities law class. I mean, by definition, I mean, the Howie test, leads to some clarity in some instances, but in others, obviously, there is ambiguity, in part because each of the prongs of the Howie test, the SEC case that sort of defines when you have a *security,* are very much intended to be sort of contextually based. And, whether or not you may know that there is an investment of money, but when are you relying on the efforts of others? What does that actually mean in the digital context? What

does a common enterprise mean when you are operating on a platform? Certainly, when is money, *money,* which is a little bit more established under securities law, but in financial regulation at large, it can and often is subject to considerable debate.

But what is clear is that it is not the case that all digital assets are securities, even under established longstanding principles, and there have been various declarations made by leaders of both the SEC and the CFTC that some of those digital assets with the largest market cap are, in fact, commodities.

Mr. THOMPSON. In your testimony, you noted the CFTC and SEC have different regulatory strengths and that there are benefits to each. In many ways, this is what Mr. Khanna and I recognized in the DCEA. For example, we proposed the SEC would continue to regulate capital raising activities with their associated disclosures for investors, and the CFTC would govern the trading of any token which is a digital commodity using registered exchanges to fulfill the role of a gatekeeper for market participants.

As we continue to think about how we should structure this regulatory regime, what else should Congress consider?

Dr. BRUMMER. I think it is important, and some of the more recent cases have, particularly in the last 2 weeks, have sort of highlighted is that as this technology grows, as this technology scales, you are going to have different kinds of actors that can also be operating on chain. And, when we get to these very important questions like what is *decentralized* and what is a *decentralized actor,* what happens when you have more centralized actors who, by definition, may have off-chain operations that are more opaque? What does it mean when these digital markets intersect with the larger off-chain economy? And I think that that is going to be a critical question. There is a disclosure aspect to it. There is a market infrastructure question to that, and it is going to be something that lawmakers and regulators are going to have to think through.

Mr. THOMPSON. Very good. Well, thank you. Thank you to all of our witnesses, and thank you, Mr. Chairman.

The CHAIRMAN. I thank the gentleman.

The chair now recognizes the gentleman from Illinois, Mr. Rush.

Mr. RUSH. Thank you, Mr. Chairman, for today's hearing.

The timing of today's hearing is very apt. Cryptocurrency markets have been on a roller coaster in recent months, and the last 2 weeks have been an absolute and horrible meltdown as Bitcoin has lost over half of its value. As such coins melted down so horrifically to cause concern for the rest of the industry. Frankly, Mr. Chairman, I am concerned. I am concerned that this industry does not adequately expose its risks and volatility as it tries to lure in a new and unsuspecting money as it deals with multiple crypto exchanges showing ads during this year's Super Bowl. I am concerned about the lack of transparency for some of the cryptocurrencies, such as so-called stable coins, some of which have been recently collapsing and those could potentially cause harm to the rest of the global economy. As the Chairman of the Subcommittee on Energy within the Energy and Commerce Committee, I am concerned with the stress that cryptocurrency mining facilities are putting on our electric grid in the summer where there are

blackouts in south Texas, California, and some of the Midwestern states are already receiving warnings.

Finally, Mr. Chairman, as someone who cares deeply about this country, I am concerned about the growing political power of cryptocurrency companies and worried about the potential for regulatory capture by the industry and its new [inaudible] into dark money investment into political races, including my local race here in Chicago for my replacement in Congress.

Now, I understand that technology does not flow within the jurisdiction of the Agriculture Committee or the CFTC, and that certainly is not the subject of today's hearing.

Dr. Brummer, I would appreciate your testimony on financial inclusion, ensuring that communities like mine on the south side of Chicago that have been traditionally excluded from generating wealth are not excluded from the potential explosion of wealth that blockchain technologies could create. However, I am deeply concerned about this disruption of wealth that we are seeing in crypto markets this year. How do we prevent these markets from preying on overlooked and vulnerable communities, Dr. Brummer, and prevent those communities that have been robbed of so much from having their wealth further stripped by financial markets that illuminate overhead?

Dr. BRUMMER. Yes, that is an excellent question, and like you, this is something I have shared with many of the country's regulators, particularly with the state regulators around the country.

One of the primary challenges with the question of disclosure and the degree to which Black and Brown communities are preyed upon is that the degree of complexity in any kind of financial instrument, whether or not it be cryptocurrency or CDAs from 2008, complexity introduces the opportunity for vulnerability. And the question that all of our regulatory agencies are going to have to face—and this is getting back to this mindset question—is understanding that disclosure, particularly where you have large numbers of retail investors, the way in which you think about disclosure is going to have to be rethought, both because of the complexity of the financial instrument, and the kinds of assumptions that our regulatory space has traditionally made.

I do think that the industry itself is going to have to face some challenges as well, as this industry scales and it seeks both new customers, but also new kinds of ideas, it is going to have to have inputs from much broader sources of society, people from between the coasts, minority communities are all going to have to participate more. I think it is good on a number of levels. Number one, I think to the degree to which you have more sort of different kinds of people participating in the product design, you are going to be able to reach use cases that are much more applicable to a slice of the public. I think that when you have people from different backgrounds largely helping to think through the technology, there is a natural dream chute that comes from the consumer protection space. People sort of talk about what is required, frankly, for a real democratization of finance, and if you want to get some of the benefits that watching technology professes, opportunities like decentralized identity or opening up the credit box or decentralized credit scoring, closing the costs or reducing costs on mortgages, or fig-

uring out new kinds of compliance systems for MDIs and minority depositary institutions. You have to have more brainpower involved in different kinds of perspectives.

And I think, again, when you have those people participating in the room and in the design and in the strategy sessions for these companies that are still figuring out how they diversify their operations, that is going to be a critical piece to really speaking to the very real threats and challenges that are out there when vulnerable communities intersect with anything that is inherently complex.

The CHAIRMAN. The gentleman's time has expired.

The chair now recognizes Mr. Balderson from Ohio.

Mr. BALDERSON. Thank you, Mr. Chairman, and thank you to all the witnesses for being here today.

A common theme that I have heard when meeting with stakeholders in this space is that they believe the CFTC is the best position to assume oversight of spot markets for digital assets. Chairman Maloney touched on this, but I would like for you all to expand on it.

I will start with you, Mr. McGonagle, but if any witnesses have thoughts, please feel free to share them. Do you agree that the CFTC is well-suited to oversee spot markets for the digital assets, and what authorities, if any, does the CFTC need to assume regulatory authority over digital spot markets?

Mr. MCGONAGLE. Thank you, Congressman. Certainly, the way that digital assets are being traded in the cash market today very strongly resembles how digital assets are traded as a derivative. What I mean by that is where there is an interest in the change in the price of a particular commodity, and so, there is trading around that interest. That is an area that the CFTC——

The CHAIRMAN. The gentleman will suspend.

The chair just reminds Members to mute, please, if you are not on camera or speaking. Thank you.

The gentleman may proceed.

Mr. MCGONAGLE. Thank you.

So, the CFTC has a comprehensive oversight with respect to applications for contract markets, compliance by contract markets, and surveillance of activities on those contract markets. And I think all of those concepts, as well as the enforcement piece that I spoke about earlier, relate to trading that is occurring in digital asset spot markets.

With respect to the regulatory authority, I understand and appreciate that there is a lot of thinking around possible regulatory structures. I will point out just quickly that following Dodd-Frank, the CFTC received statutory authority with respect to swap execution facilities, and there was a determination by Congress to articulate 15 core principles, that are similar in scope and kind to the core principles that we have for designated contract markets. The Commission then entered into an extensive public comment period where we took the guidance that we had from Congress with respect to implementation of those core principles and set forth our proposed rules concerning trading on these platforms that are focused on market transparency, as well as clearing obligations and some dealer responsibility. So, not intermediary oversight like we

have currently in DCM space, but that would be something that would be important to evaluate in the digital asset spot complex.

Mr. BALDERSON. Thank you for that answer. Would anybody else like to add on to the question? Okay.

Mr. HOSKINSON. I will take a bite at it.

Mr. BALDERSON. All right, thank you.

Mr. HOSKINSON. I am not a securities lawyer or an expert on regulation, so take it with a grain of salt.

But I don't think it is a question of, as I mentioned before, who is more permissive or who is less restrictive. It is more of a question of efficacy, and when you look at commodities, commodities are intrinsically decentralized. So, I grow hay on one of my farms, and I didn't have to ask permission. There is no central hay agency. We are not the Soviet Union. We do not regulate things that way. And then suddenly when I cut it and I sell it, it enters into a global marketplace. Now, that marketplace has rules and principles and protections, and there is a retail component. People feed horses, and there is certainly an industrial component.

So, if cryptocurrencies are truly decentralized and that actually is a real thing, then it does make sense to embed that into a framework that is designed for things that are intrinsically this way.

You have to look out for cartels, market manipulation. You have to look out for where global actors try to come in, like China or others, and take over our market like they are trying to do the lithium markets. But that is a very different type of notion than a security in that respect.

So, in my view, the most effective thing that can be done over the next 12, 24 months is to have a really good notion of what is decentralization, and what are the factors that produce that? And if it gets past a certain threshold, it makes a lot of natural sense to regulate things like a commodity as opposed to a security. And if they don't, well then it is very obvious who has the disclosure requirement.

Mr. BALDERSON. Well done. So, thank you for your answer.

Mr. Chairman, with lack of remaining time, I will yield back. Thank you.

The CHAIRMAN. I thank the gentleman.

The chair recognizes Ms. Craig.

Ms. CRAIG. Thank you so much, Mr. Chairman, and thank you to Ranking Member Fischbach for today's hearing on digital asset regulation. Thanks so much to the witnesses for your expert testimony. Obviously, this is clearly a space with complex policy considerations and a great deal of public and private interest.

One of the things that I have been tracking today during this hearing and over the course of the 117th Congress is how many of these conversations about regulatory authority will impact many of the retail investors that have moved into the crypto space over the last few years.

With that in mind, I know we are giving you a bit of a workout today, but Director McGonagle, I am coming to you with my first question. Director McGonagle, can you speak about how Federal regulation of crypto trading platforms under the Commodity Exchange Act is related to market transparency, and ultimately to en-

suring that retail investors have access to the information they need to properly weigh the risk involved?

Mr. MCGONAGLE. Thank you, Congresswoman. I appreciate the question.

In thinking about spot markets, say, in particular the overlap of spot and derivatives markets, an issue that we are focused on for derivatives products deals with the concept of the prospect around leverage, and the understanding by the individual investor, particularly where that individual investor is a retail participant, that they know and appreciate the risk of trading. And while there may be good upside for putting, say, 50¢ down and having a dollar's worth of a position, there is incredible downside if the market moves against your position.

So, at the CFTC, we are focused not only on market integrity and having centralization or a place where market participants can come together and understand what the pricing is, but we also look to have a system of intermediary oversight that focuses on retail market participants, say, in particular with a disclosure regime that informs those market participants sort of based on who they are dealing with. So, for example, if it is a commodity trading advisor or commodity pool operator, the risk of that trading strategy is disclosed as well as associated fees add—those are disclosed. That individual market participant understands how their funds are being protected or utilized at a futures commission merchant, for example, that those funds are segregated, and how those funds can also be protected, for example, in the event of a bankruptcy.

So, we do look for execution certainty, as well as customer protection as part of our regulatory regime, and I think that is helpful to the dialogue here.

Ms. CRAIG. I don't want to take up too much more time, but I have been listening here for quite a while, and I hear you saying that your agency has the capacity and the expertise to take on any additional regulatory role in this digital asset space. Is that what I am hearing from you today?

Mr. MCGONAGLE. So, we definitely have the intellectual expertise, and we have ongoing responsibility now to implement and ensure regulatory compliance by new market participants that are currently seeking applications for designation as contract markets, for example, as well as ensuring that those entities continue compliance. So, we are able to take that skillset to the extent that we are dealing with like to like, similar types of core principles. We are able to transition that work, and I used earlier the example with respect to swaps. But that also involves, certainly, a resource determination, and depending on the number of applicants, for example, or the scope of the responsibility, from my perspective, that is a conversation that DMO has with the Chairman about priorities.

But at the same time, the Chairman has initiated an effort to accurately quantify the resources that would be needed in the event that there is some additional grant of authority.

Ms. CRAIG. Thank you so much.

I don't have time to ask the whole panel, but I wanted to ask Dr. Brummer here. In the time I have remaining, can you give me your assessment about how the principles-based approach of the

CFTC does or doesn't fit with the dynamic nature of the digital asset space now?

Dr. BRUMMER. That is an extraordinarily good [inaudible]. Thank you. I am a technology expert, but I just need to press the red button.

So, I think that is an important and critical question in part because one of the comparative advantages, one of the really interesting features of the derivatives regulatory framework is precisely because of the special relationship between the exchanges, the DCMs and the Commission whereby you can exercise various levels of granularity in terms of oversight, while at the same time leveraging the self-regulatory capacity of these exchanges to keep up with the innovation.

And so, I do think that is one interesting and important feature, particularly in a space that is constantly evolving and where the rulemaking is going to have to be very agile. So, that is something that I look to as a potential comparative advantage.

Ms. CRAIG. Thank you so much, Dr. Brummer, and seeing that I have exceeded my time, I thank the Chairman and yield back.

The CHAIRMAN. I thank the gentlelady.

The gentlewoman from Florida, Mrs. Cammack.

Mrs. CAMMACK. Well, thank you, Mr. Chairman and Ranking Member Fischbach. I appreciate all our witnesses for being here today, and has been discussed, since 2014 the CFTC has been regulating crypto derivatives, and has also been exercising its anti-fraud and anti-manipulation enforcement authority over digital asset sport markets. The agency clearly has extensive experience overseeing digital assets, including futures, which retail users have been trading through a direct access model.

Now, Dr. Brummer, isn't it the case that several exchanges registered with the CFTC today offer retail traders the ability to directly access exchanges without a broker, including through ICE, ARIS, and Kalishi exchanges?

Dr. BRUMMER. It is true to my knowledge that yes, there are some direct—I know [inaudible]. I am not entirely sure about the others, but yes.

Mrs. CAMMACK. Okay, and this is for you again, Dr. Brummer, and Mr. McGonagle.

I am going—I messed that up. I am so sorry. I would like to ask each of you, do you agree that Federal regulation of crypto trading platforms under the Commodity Exchange Act would raise the floor rather than establish a ceiling of required reporting and investor protections above that currently provided by the existing state-by-state money transmitters licensing regime?

Mr. MCGONAGLE. Yes. Thank you, Congresswoman.

Certainly, as a market regulator, it would establish a floor. We have a different purpose than the money exchange state licensing, and so, I wouldn't be in a position necessarily to compare how those state-by-state provisions may overlap in some instances. But to the extent that we are talking, again, about managing risk, CFTC has a system of regulation in place.

Mrs. CAMMACK. Dr. Brummer?

Dr. BRUMMER. That is right. The purposes of the money transmitter laws are different. They tend to be, at the state level, some-

what less resourced, but the entire focus is a little bit different. So, there would be some overlap, but it is a little bit of apples to oranges.

Mrs. CAMMACK. I know. I know, I am pushing you to try to get to a point here, but thank you both for your responses.

Mr. McGonagle, how does the CFTC's expertise and experience regulating complex derivatives markets translate to crypto markets?

Mr. MCGONAGLE. Thank you again, Congresswoman.

The CFTC offers the opportunity for multiple market participants to come together to execute transactions where there is price transparency. Individuals who are trading in the market understand the product that they are trading and they understand the price and volume for how they are trading that product. There are also rules in place with respect to how those customers possibly are entering their transactions on the market. And when I mean possibly—and you alluded to this earlier—to the extent that they are going through an intermediary, there are additional protections available to a retail market participant, including the types of risk disclosure, segregation and protection of assets.

And then ultimately, the transactions go to a clearing facility. Centralizing that clearing facility minimizes the risk that you may see currently for transactions on spot platforms, for example, who do not have centralized clearing and instead are exposed to individual counterparties' credit risk.

Mrs. CAMMACK. Thank you for that. I appreciate it.

One last question, since I have about a minute left. I understand that you all have been working closely with the SEC on exchange regulation in this space. A day doesn't go by that I don't catch an article about this. Regarding this coordination and cooperation, how productive are these discussions to coordinate going—how are they going, and do you see any concerns or gaps in the current conversations with SEC that still need to be addressed?

Mr. MCGONAGLE. So, thank you, Congresswoman. I was reflecting on——

Mrs. CAMMACK. Are you sure you want to say thank you?

Mr. MCGONAGLE. I was reflecting on 25 years with the CFTC. In my experience, we have a longstanding relationship, particularly on enforcement, but also on regulatory matters. We talk all the time. We need to talk and those conversations are always productive.

Mrs. CAMMACK. Are there any gaps that you see?

Mr. MCGONAGLE. As between the two agencies, we understand where our jurisdictions come together. We discuss when they overlap. In physical digital assets, we currently don't have regulatory authority over those products.

Mrs. CAMMACK. Thank you.

The CHAIRMAN. The gentlewoman's time has expired.

Ms. Kuster—and I will remind the Members that we do have a fourth witness who is up in the middle of the night in Asia. I haven't forgotten about you, Mr. Levin. The perils of being on Zoom.

Ms. Kuster?

Ms. KUSTER. Thank you so much, Mr. Chairman, and thank you for our panel being with us, especially you, Mr. Levin, joining us from South Korea. I will have a question for you.

We are in the midst of a brave new world of digital asset trading. Our Committee has given this issue worthwhile attention because of the role that the Commodity Futures Trading Commission has and will continue to play in regulating this trade. As more and more Americans invest in these assets, it is imperative for Congress to keep up as we regulate and oversee the digital realm, just as we do with more established markets.

As we have all seen recently, Bitcoin, the most popular cryptocurrency, has badly tumbled in the last few weeks and lost more than ½ its value in 2022 so far. Clearly, no marketplace is immune from severe vulnerability and uncertainty, be it Bitcoin or Wall Street, but we do need to assure digital markets are operating above board and that they are secure, and that investors have access to the information they need to fully understand the risks they are undertaking.

With that in mind, I am going to focus my questions on consumer protection as it relates to digital assets, and going to you first, Mr. Levin. Thank you for being with us from South Korea. Could you speak to how prevalent risky cryptocurrency exchanges are, such as those that lack know your customer rules, may have criminal ties, or may be connected to the dark web?

Mr. LEVIN. Thank you, Congresswoman, and yes, this is exactly what Chainalysis focuses on is mapping all of the different participants that actually facilitate transactions in cryptocurrencies. And to your point, we have seen over the last few years exchanges in offshore jurisdictions actually used to facilitate the laundering of proceeds from things like ransomware. And so, OFAC has taken action to designate certain of these exchanges like SUEX and TRAVEX as cryptocurrency exchanges that have facilitated that.

I think that does speak, though, to the ability for us to focus the discussion here on how do we appropriately equip a market regulator with overseeing the venues that we think should form the reference prices for these commodities and ensure the orderly functioning of markets. And also, we have seen Treasury take necessary action to enforce rules around AML across the board internationally as well, and that has been very clear in sort of the actions the Treasury has taken.

Ms. KUSTER. So, let's delve into that.

Director McGonagle, you mentioned in your testimony since 2014, the CFTC has brought more than 50 enforcement actions against digital asset markets for issues like fraud, manipulation, and false reporting. Could you speak to how the investigation process works at CFTC, and do you feel there is more authority or certainly financial support that you may need from Congress to strengthen CFTC's enforcement role?

Mr. MCGONAGLE. Thank you, Congresswoman. I appreciate the question.

When it comes to enforcement authority, the CFTC has very broad and strong authority. Our anti-fraud and anti-manipulation authority, as you mentioned, extends into the physical markets, where we have brought cases that involve all manner of misrepre-

sentations, including pump and dump schemes that are manipulating prices. There was a comment about the Bank Secrecy Act and money laundering. We brought cases where entities have a registration obligation with the CFTC because of the products they were offering, did not seek registration and also violated AML provisions. We also look at fraud in the context of illegal contracts. So, for example, if it is a leverage contract that doesn't result in the delivery of the actual physical currency within a period of time, that falls within CFTC's anti-fraud authority and it is treated as if it is a futures contract.

Ms. KUSTER. Can you elaborate on how these crimes work? You have given an example, but what you all have identified as emerging trends in illicit activity related to digital assets that you are on the lookout for. I know I do a lot of work in the addiction and opioid space, but also sex trafficking. It looks like my time is up, so we will have to see if we can beg the Chairman's indulgence for your response.

The CHAIRMAN. The gentleman may proceed.

Mr. MCGONAGLE. Yes, thank you.

And say, in particular, the attraction to leverage, so that sort of get rich quick because individual investors are at 50 to 1 leverage, for example. Like that is a significant risk concern.

We also see digital assets where they may not be the subject of the fraud, but they are the payment mechanism in connection with other fraud schemes, like for example, FOREX fraud that CFTC has jurisdiction over.

Ms. KUSTER. Excellent, thank you. Thank you, Mr. Chairman. I yield back.

The CHAIRMAN. The gentlewoman's time has expired.

Mr. Feenstra—excuse me, Mr. Scott.

Mr. AUSTIN SCOTT of Georgia. I——

The CHAIRMAN. Am I right, Mr. Scott? Okay.

Mr. AUSTIN SCOTT of Georgia. I apologize, I had to step out. I had a meeting in my office with constituents.

But I am going to start with you, Mr. McGonagle. This isn't—it is not corn; it is not gold. It is certainly not dollars, and there are a lot of questions here. One is if the U.S. is going to regulate, then it is CFTC *versus* SEC. Some have suggested even a new agency. Then there is the how if you do that, and then there is the who do you regulate?

So, my understanding is there are 20,000 approximately cryptocurrencies in the world worth about $3 trillion. Is that close, give or take a trillion on a day on the values? Is it somewhere around 20,000 currencies?

I mean, the question I have, 20,000 currencies, CFTC—how many people work at the CFTC today?

Mr. MCGONAGLE. Thank you, Congressman. Several hundred.

Mr. AUSTIN SCOTT of Georgia. Several hundred. So, you would be talking about—if they gave up everything that they are currently doing, you would be talking about 100 cryptocurrencies a person?

My point is, it is not possible to regulate all of these currencies. It is just not. And so, then the question becomes who, and I mean, is it that we are going to have a value if the currency reaches a certain dollar figure that all of a sudden we are going to regulate

it? I am interested in any comments that any of you may have on of the 20,000 cryptos, how you determine who should be regulated?

Mr. HOSKINSON. Well, one of the powers of our industry is the fact that regulation can become algorithmic. So, you don't have to think, well, which person is going to sit down and look at this big pile? Think of the IRS and tax returns. We could quadruple the size of the IRS, but we still couldn't audit every single American. It is just not possible. And so, what you have to do is say what tools do we have at our capability, and what is magical about cryptocurrencies is that in the transactions themselves, they can carry metadata. They can carry identity. Rule makers and policy makers can take a step back and say, "Well, these are the things that we care about and we can make sure inside the systems that those things don't settle and clear until those things are present."

So, it is really more of a conversation of what do you care about, and then what we can do as technologists is create a self-certification system, and then what can happen is when there are anomalies or special cases, which often would be rare, then the CFTC or another regulatory body could look through and say, "Well, let's investigate that." That is generally how we do law enforcement. We don't break into everybody's house. We wait until we get a warrant and you have to have some cause for it, so there has to be some social infrastructure.

Mr. AUSTIN SCOTT of Georgia. So, self-certification is different than an agency regulating?

Mr. HOSKINSON. Well, they are interconnected. So, you have SROs, you have market standards, you have principles, and in many cases, financial regulation is mostly done by SROs or private organizations.

If you look at, for example, compliance, it is not the SEC or the CFTC going out there and doing KYC and AML, it is banks that are doing these types of things. So, it is a public-private partnership, and what needs to be done is to establish those boundaries. And then what we can do as innovators is write software to help make that happen, and literally, that is what Chainalysis is doing right now, and their competitors.

Mr. AUSTIN SCOTT of Georgia. I think—I mean, I don't see a way for us to regulate them all. I do think there has got—if it is going to happen, there has to be some type of self-certification.

What I do fear—because I don't think that crypto should be a significant portion of the average investor's portfolio. I don't. I mean, and I do fear that if we all of a sudden are regulating it, then the average investor feels like there is more security and stability in the value of it, and I think that is a dangerous thing for the investors. And I will tell you, I would be very concerned about the average American citizen having more than five percent of their investments in the crypto markets. I am not talking about guys like you who know it inside and out, but I just—I have expressed my concerns. I appreciate your comments on the self-certification. I do think that is a path that we need to be considering.

And with that, Mr. Chairman, I will yield the remainder of my time.

The CHAIRMAN. I appreciate the gentleman yielding his 3 seconds.

Mr. Feenstra is recognized.

Mr. FEENSTRA. Thank you so much, Chairman Maloney and Ranking Member Fischbach. It is great that we have having this discussion today, and it is so important. Digital asset market regulation is critical.

Mr. McGonagle, in addition to requirements that apply to all CFTC regulated futures and derivative exchanges, would the CFTC require additional authority from Congress to promulgate additional crypto specific requirements if the CFTC were to be given primary regulatory authority over digital asset trading platforms by Congress?

Mr. MCGONAGLE. Yes, Congressman, we would need additional regulatory authority.

Mr. FEENSTRA. And what—going down that path, what are you looking for?

Mr. MCGONAGLE. Currently for both designated contract markets and for swap execution facilities, there is a system of core principles that the agency has. More recently, with respect to the swaps implementation, we engaged in extensive public comment around the establishment of setting up the operation of the facilities, trading facilities, clearing, as well as any other regulated or registered entity like swap dealers, for example.

Mr. FEENSTRA. So, do you agree that evolution or maturation of a digital asset and its underlying network has the potential to remove security-like characteristics over time for assets to become fully decentralized, or——

Mr. MCGONAGLE. Right.

Mr. FEENSTRA. Is there a parallel in that regard?

Mr. MCGONAGLE. Totally appreciate that question, and that is an interesting topic.

Digital assets are broadly defined to be *commodities.* If there is a determination under current law that the SEC determines that it is a *security,* then it takes it outside of CFTC jurisdiction, and there isn't currently a framework that would allow evolution of the product to put it back into CFTC jurisdiction.

Mr. FEENSTRA. That is correct, then that would be a problem.

So, is there a parallel there with regard to that evolution, then, of swaps?

Mr. MCGONAGLE. I think how we handled swaps is we divided the market, right, and so, characteristics of certain swaps that were more closely aligned with the SEC were at SEC. The SEC and the CFTC maintained a dialogue and worked together on rules that impacted both of our jurisdictions, so that is something that is available to the agencies.

Mr. FEENSTRA. So, one more question.

How do you think the notion of *fully decentralized* should be defined or determined, and at what point or what triggering event should that determination be made, and through what process? I know this is a tangled web here.

Mr. MCGONAGLE. Right, it is a tangled web, and I guess from the CFTC's vantage, I don't consider or look at how the thing presents whether it is so-called decentralized as opposed to is it something where there is a trading interest? There are many market partici-

pants that are interested in trading and understanding how it trades.

So, from our perspective, we probably would be encouraging not so much a definition of what is *decentralized,* but whether the underlying digital asset is something that should fall within regulation of the CFTC, under our structure as opposed to defining this other structure.

Mr. FEENSTRA. Yes. Right, and we do need more Congressional intent to go down that rabbit hole, that path?

Mr. MCGONAGLE. So, certainly if Congress wanted to further clarify the extent of CFTC's jurisdiction as it applied to any further legislation that would be appropriate. But as I mentioned, we currently have digital assets as a defined *commodity.*

Mr. FEENSTRA. Right. Right, okay. Thank you for your information. This is a great area, and we have to embrace it, and I appreciate your comments. Thank you.

The CHAIRMAN. I thank the gentleman.

Mr. Cloud?

Mr. CLOUD. Thank you, Mr. Chairman, and thank you all for being here, and thank you, Ranking Member, for hosting this.

I carry some of the concerns, I guess, about regulation that some of the former Members have carried, just because a lot of times the government will see mission creed. And so, one of the great appeals of cryptocurrencies when I talk to people who kind of dabble in it is the fact that there is not an intermediary at this point. And so, I also had the question about who and how and those sorts of things. How do we keep this limited? What is the current market failure we are trying to fix, basically, and how do we keep it—any sort of regulation narrowed to that and in such a way that over time it doesn't become very much invasive?

And if you can answer that, Mr. McGonagle, but I will point out Mr. Hoskinson mentioned the banks as an example of how this is done well. If you talk to the bankers, a lot of them will talk about how this is not done very well in the fact that they have to be the authoritarian arm of the Federal Government in a lot of different ways.

So, anyway, your thoughts on that, and feel free to chime in.

Mr. MCGONAGLE. Yes, thank you, Congressman, for the opportunity to address that particular issue around the certification of products. Currently, the CFTC is in a situation where an exchange can willy-nilly certify a product and allow that for trading. All core principles apply, but in particular, is the core principal that an exchange may only certify a contract that is not readily susceptible to manipulation. So, what we are getting at—is who is interested in trading this product, and why, and is there sufficient liquidity, for example, or sufficient interest by market participants that there actually is a market value to exchange or trade risks?

Certainly in our markets, we think about why individuals would want to hedge. They are producers, farmers, and users, and they have an interest in the actual underlying commodity, but we also see interest in past-settled contracts, these financially settled obligations. And I think that under our current system of regulation, we have an ability to winnow out activity or contracts that don't provide a market value.

Mr. CLOUD. Any of you want to speak to that, or—I have another question to move on to.

Mr. HOSKINSON. Sure. Can I comment on the KYC AML, sir?

I don't think anyone is doing KYC AML very well, and nobody wants to be a data broker. It is pretty crazy what is going on right now. I am a big believer that you have to understand what private industry has been doing over the last century or so. If you look at Google, you look at Facebook, you look at these companies, they are more than companies. They don't just go and make sprockets in cars or something and they compete in a fair market. They are ending up getting a lot of control and power over foundational resources.

So, if we look at the prior centuries like Standard Oil, it got control over the energy industry, and then we said, "Boy, that is probably not a good idea. We should do something about it." Now when we look at Google, Facebook, and these other companies, they have gained so much control over information, thought, speech, and other foundational resources, hosting. They actually can define an entire marketplace and decide who gets to compete and who doesn't. It is relevant to cryptocurrencies and the blockchain industry because at the end of the day, it is deliberation of those resources. That is what we are really doing here to separate the wheat from the chaff. We are talking about a resource-based economy. The point of decentralization is saying that maybe nobody should be in control of our freedom of expression or commerce or association.

So, that requires a fundamentally different way of interfacing with those marketplaces, different way of handling identity and compliance——

Mr. CLOUD. I only have a minute, so if I can jump in here.

Mr. HOSKINSON. Sure.

Mr. CLOUD. The fact that you are talking about big tech I think is very interesting in this, because you also mentioned that one of the features of regulation is that we can use algorithms now.

Mr. HOSKINSON. That is right.

Mr. CLOUD. We have seen them use algorithms to limit people's freedom of speech and to do all of these other nefarious things. So, if we give the government that power, especially as the Federal Reserve is looking toward creating a digital currency potentially and we already have banks being thrust upon them to enforce ESG scores, and in China, we see where there ESG scores simply become personal scores on individuals. It is not a far step technologically and in the way we see some of the agencies working right now to begin to target those algorithms toward people and their personal habits, and their spending.

So, how do we compete economically on the world stage without threatening the privacy rights of Americans, going forward? This is a very dangerous slope if not handled correctly.

Mr. HOSKINSON. Yes, I couldn't agree more. I am deeply concerned by social credit, deeply concerned by some of the proposals for CBDCs because you can have transactional discrimination against any ethnic group you want, or any political philosophy you want.

So, the point is the algorithms out to be built out in an open-source process, transparent and available to all, and people have to have the ability to opt in instead of opt out. So, the power of our industry is we didn't have a governing agency or some central actor say oh, here is cryptocurrency. It was the tireless work of millions of people, many of which never met each other, around the world coming together voluntarily and building a new economy worth trillions of dollars. That is the way we ought to think about it, not how do we create some government agency or how do we create some central bank or central algorithm that will control everything. And then you ask yourself about the outcomes you desire.

So, it is clear that there have been some problems over the past 13 years, and we are working our way through that, but at the same time, we have created value for millions of people, and we shouldn't lose sight of that.

The CHAIRMAN. The gentleman's time has expired. I thank the gentleman.

That concludes our initial round of questions. Seeing no other Members in the room, I am going to extend an opportunity for a selective round of additional questions, if the Ranking Member has anything, I am happy to yield to her.

Mrs. FISCHBACH. If we are prepared to, and I don't see any others, but I just wanted to express another thank you to everybody because this has been an incredible informational kind of hearing that we have been able to have, and I, again, thank the chair for bringing us together. But thank you to all of the witnesses.

The CHAIRMAN. Well, I thank the gentlewoman. I take it that those are your closing remarks. I appreciate that.

Thank you to all of today's witnesses. I want to be respectful of your time.

Let me just say in closing, given this Committee's jurisdiction over the Commodity Futures Trading Commission, market volatility and continued growth of this industry, it is important we remain active and engaged as a participant and have these conversations to consider and determine appropriate and necessary legislation and regulation in this industry.

As you know, since Bitcoin was released in 2009, the digital asset market has experienced explosive growth and innovation and evolution, and the testimony we have heard today certainly highlights those market evolutions and indicate that that will be a key characteristic of the digital asset industry for the foreseeable future. And of course, as recent developments have shown, we also understand the volatility of these markets and the risks that come with that.

The potential solutions this technology can offer are worthy of a regulatory regime that will allow for continued innovation while also establishing and requiring platforms adhere to a uniform set of standards and guidelines, and will protect those who choose to participate. While there are many more conversations to be had, I am certainly glad that our Committee is remaining active in this discussion regarding the future of the digital asset regulation. Also, I want to stress the importance we all put on the United States having a leadership role in this space.

I would like to thank the Committee Chairman, Mr. Scott, for the opportunity to chair the Subcommittee. I am also very proud to take this leadership role at this critical time, and I look forward to conducting additional hearings. We are just getting started, and of course, we will be eager to hear additional relevant testimony here at the Commodity Exchanges, Energy, and Credit Subcommittee. I want to thank the Ranking Member, Mrs. Fischbach, for joining me today. I want to thank particularly our witness in Asia for getting up late.

And with that, the Committee stands adjourned. Excuse me, I have to do one other piece of housekeeping, I believe, which is to tell you that under the Rules of the Committee, the record of today's hearing will remain open for 10 calendar days to receive additional material and supplementary written responses from the witnesses to any questions posed by a Member.

And with that, this hearing of the Subcommittee on Commodity Exchanges, Energy, and Credit is adjourned.

[Whereupon, at 12:18 p.m., the Subcommittee was adjourned.]

[Material submitted for inclusion in the record follows:]

SUBMITTED STATEMENT BY SAMUEL "SAM" BANKMAN-FRIED, CO-FOUNDER AND CHIEF EXECUTIVE OFFICER, LEDGERX LLC D/B/A FTX US DERIVATIVES

Introduction

Chairman Maloney, Ranking Member Fischbach, and other distinguished Members of the House Agriculture Committee's Subcommittee on Commodity Exchange, Energy, and Credit (the "Committee"), FTX appreciates the opportunity to provide this statement to the record for the hearing on "The Future of Digital Asset Regulation." We applaud the Committee for assembling an excellent panel of experts to discuss this topic of critical importance for the future of the digital asset industry and U.S. capital markets. FTX largely agrees with many of the statements made in the hearing that the Commodity Futures Trading Commission (CFTC) is well-situated to exercise more oversight of non-security digital assets. In the statement below, we offer a vision for the expanded role the CFTC could play in overseeing digital assets markets. Going forward, FTX is pleased to provide the Committee and its Members with as much information needed to ensure a fully informed and robust conversation around whether and how this Committee could address key issues involved with regulating the digital asset space.

Background on FTX

FTX was established by three American citizens, Samuel Bankman-Fried, Gary (Zixiao) Wang and Nishad Singh, (FTX Founders) with international operations commencing in May 2019 and the U.S. exchange starting in 2020. The FTX Founders sought to build a digital asset trading platform and exchange with a better user experience, customer protection, and innovative products, and to provide a trading platform robust enough for professional trading firms and intuitive enough for first-time users.

Today, FTX is the parent company of several entities across the globe, including a U.S.-based digital asset spot market exchange (FTX.us) and a derivatives exchange and clearinghouse (FTX US Derivatives). FTX.us is registered with the Department of Treasury (via FinCEN, as a money services business) and holds a series of state money transmission licenses. FTX.us is also a registered broker dealer with the Financial Industry Regulatory Authority (FINRA). FTX US Derivatives is licensed by the U.S. Commodity Futures Trading Commission (CFTC) as an exchange and clearinghouse. FTX's international exchange, which is not available to U.S. users, holds a series of marketplace licenses and registrations in many non-U.S. jurisdictions. For additional information regarding FTX's business operations and licensing, please refer to the *Exhibit A* of this statement.

Discussion

This statement covers the following topics: (1) an overview of the products offered by FTX; (2) the current U.S. regulatory landscape and existing regulatory gaps; and (3) a vision for the CFTC as a digital-assets market regulator for the U.S. Throughout this discussion we use 'digital assets' generally to refer to digital asset tokens that are generally considered to be a commodity rather than a security.

1. FTX Products and Their Role in the Digital-Asset Economy

Core Product: Digital Asset Exchange. FTX's core products are its digital asset exchanges, *FTX.com,* FTX.us and FTX US Derivatives (*https://derivs.ftx.us/*)—FTX.us and FTX US Derivatives are being integrated into one user-experience platform and web site. While *FTX.com* offers both spot market and derivatives trading, those two categories are separated in the United States, with spot market trading on FTX.us and derivatives trading offered through FTX US Derivatives.

On *FTX.com* and FTX.us, users can trade digital assets with other users for cash, stablecoins and other digital assets. On the spot markets, users can set a variety of different order types on a central limit order book (CLOB). Users are able to offer orders at a specific price (limit order) or trade on the book at the best price shown. A robust price and time priority matching engine sits in between these orders to connect buyers and sellers and display the best available prices.

Futures and volatility contracts related to digital assets also are listed on the platforms as well, with or without leverage. On *FTX.com,* leverage is limited to a maximum of 20x (*i.e.,* minimum margin of 5%), and is much less in most cases; as of now leveraged trading is not available to users of FTX.us (although there is facilitation of other forms of credit to Eligible Contract Participants—see below). The *FTX.com* platforms have listed quarterly-settled (as well as perpetual) futures contracts that are cash settled. Additionally, MOVE volatility contracts are offered on *FTX.com* and are similar to futures except, instead of expiring to the price of a digital asset, they expire to the USD amount that the price of Bitcoin (BTC) has moved in a day, week or quarter. *FTX.com* also offers BTC options for trading. Finally,

FTX US Derivatives offers to U.S. users both Bitcoin (BTC) and Ethereum (ETH) derivatives.

To cover initial and maintenance margins, derivatives and leveraged-product users can post collateral in the form of cash, stablecoins or other digital assets held in their account. The exchanges also have integrated risk-management and back-office systems to perform clearing and settlement of trades, which includes updating records of ownership of the digital asset or digital asset futures and options contracts traded (clearing), and transferring value between users' accounts (settlement), using either delivery *versus* payment or delivery *versus* delivery. Importantly, FTX's risk model avoids the systemic warehousing of such risks over a weekend or other period of market closure, and instead addresses at-risk positions and accounts immediately, in real time, 24/7/365.

Off-exchange Portal for Arranging and Matching User Orders. FTX also offers an off-exchange portal that enables users to connect with other, large users, enabling them to request quotes for spot digital assets and trade directly. This facility forwards requests for quotes to large users, returning prices offered and enabling users to then place an order. The portal is similar to other facilities found in traditional markets where a central limit order book is not used to match trades.

Third-Party Lending. FTX platform users can lend their digital assets to those who seek them for spot trading. Users (including eligible users on FTX.us) wishing to trade digital assets they do not have may borrow them from users willing to lend them by posting collateral in the form of cash, stablecoins or other digital assets held in their account. The FTX platform maintains a borrow/lending book and matches users wanting to borrow with those willing to lend.

NFT Marketplace. FTX operates a marketplace for users to mint, buy and sell non-fungible tokens (NFTs). NFTs are tokens that are not fungible with any other tokens. They can take a number of forms and, for example, can be redeemed for a physical object, or an experience (such as a movie or phone call), or can be linked to a digital image, *etc.* FTX's NFT marketplace is conducted through an auction system. Alternatively, users can purchase directly at the prevailing selling price set by the seller. Users can choose to display their NFT collection on the FTX NFT marketplace portal, and/or to continue to buy or sell on the NFT marketplace.

FTX Pay. FTX Pay is a service offered to merchants to accept payments in digital assets or fiat. Users have the option to top up their FTX accounts with ACH or credit cards, which are then used to make payments to enrolled merchants. For digital asset payments, the relevant user's FTX account would be debited by an amount in the chosen digital asset that is equivalent to the amount that is payable to the merchant. FTX facilitates the payments to the merchant by providing the payment infrastructure. This allows merchants to accept digital asset payments, without having to assume any volatility risk for the assets.

Staking. *FTX.com* offers the ability for users to "stake" certain supported digital assets on the platform. By staking such digital assets, users can earn staking rewards; in addition, for some tokens, users can receive and unlock certain benefits on FTX, such as reduced trading fees, withdrawal fees, as well as other rewards. Generally, users can "unstake" their digital assets at any time, subject to an unstaking or unbonding period.

Types of Digital Assets on FTX Platforms. FTX has developed listing standards and a framework for determining which digital assets to list on the platforms. Part of that framework entails evaluating the assets to assess factors such as security, compliance risk, legal risk, technological risk and other factors. On *FTX.com,* which again is unavailable to U.S. users, FTX has listed approximately 100 stablecoins and other digital assets on its spot exchange. Digital assets include tokens such as Bitcoin (BTC), Ether (ETH), Uniswap Protocol Token (UNI), Chain Link token (LINK), Solana (SOL), and Aave (AAVE).

On FTX.us, the company has taken what we believe to be a conservative approach to listing digital assets for trading. Consequently, there are far fewer tokens listed for trading on FTX.us due to much stricter listing standards for this platform. Care has been taken to avoid listing assets with features viewed to be similar to securities in the U.S. The assets and tokens listed more closely resemble BTC and ETH, two tokens expressly addressed by the CFTC to be commodities subject to its jurisdiction.

On FTX US Derivatives, users can trade a Bitcoin Mini Option or Ethereum Deci Option, a Next-Day Bitcoin Mini Swap or Next-Day Ethereum Deci Swap, and a Bitcoin Mini Future. All of these contracts are fully collateralized. FTX is in discussions with the CFTC about expanding our derivatives offerings to U.S. customers.

In sum, the products available now in the digital-asset economy and on the FTX platforms are very similar to ones found in the traditional finance space. A key

differentiator from traditional finance is that investors can get access to all of them without going through multiple intermediaries. FTX believes the market structure for digital-asset platforms is risk reducing compared to others because it facilitates more effective risk management and eliminates unnecessary points of failure. In addition, all market data is made public and free—all users are given full knowledge of the orderbook and trades. Easy access to financial products and solutions on one, easy-to-use platform is a powerful feature that empowers investors, consumers and entrepreneurs. By simplifying access to these tools, users of the products can focus more on the core of their everyday financial goals and needs while making more informed decisions—ultimately this is what FTX believes will promote financial inclusion and economic security for more people.

2. Current Regulatory Landscape for Digital Assets and the Role of the CFTC

The current U.S. landscape for the regulation of the trading of digital assets is a patchwork of Federal market regulations and state-level money-transmission laws. As explained above, FTX US offers "cash" or "spot" markets and FTX US Derivatives offers access to derivatives markets,[1] but the regulatory treatment of each type of market is different. ***For cash markets*** in the U.S., if a digital asset is a security as defined by the Securities Act of 1933, then the digital asset is subject to the jurisdiction of the SEC, and the asset as well as any platform that lists it for trading generally must be registered with the SEC. A digital asset that does not meet the definition of a security under U.S. law would generally still meet the definition of a "commodity" under the Commodity Exchange Act (CEA).[2] * Historically, the CFTC generally has not exercised jurisdiction over the operation of spot markets for commodities (with few exceptions), but FTX believes the CFTC could assert jurisdiction over digital-asset spot markets under certain circumstances,[3] even where the agency has not done so to date—more on this below.

In any case, there are no U.S. platform operators of only ***cash markets*** for digital assets supervised by the SEC or the CFTC today. Many states have taken the view that their money-transmission laws apply to digital-asset platforms that have customers in their states, which requires state licensure, but these laws do not possess the hallmarks of Federal market regulation and its market-integrity and investor-protection principles.[4] At the time of this writing, FTX US and the other largest U.S. digital-asset platforms offering cash markets have many state money-transmission licenses and continue to pursue others. A money-transmission business also implicates the U.S. Bank Secrecy Act and by doing so must register with the U.S. Department of Treasury via FinCEN, unless otherwise exempted; FTX US is so registered.

For derivatives markets in the U.S., if the digital asset referenced in the contract is a commodity and not a security, the trading of derivatives on that digital asset is subject to the jurisdiction of the CFTC. The CFTC today oversees the trading of BTC and ETH derivatives on multiple U.S. trading platforms, including FTX US Derivatives, which as mentioned lists futures, swaps and options on these digital assets. FTX believes that there are many other digital assets that are not securities, and so derivatives on those digital assets would fall under the CFTC's jurisdictions as well and could be listed by appropriately registered platforms such as FTX US Derivatives.

This patchwork of regulations increases the operational complexity of digital-asset platform operators, decreases capital efficiencies for customers, and hampers the ability of platform operators to optimize their risk-management programs. It also re-

---

[1] Cash or spot markets are markets where the asset being purchased is delivered immediately. Derivatives markets are ones where contracts or agreements between two parties are traded, and the contract's value is based upon an agreed-upon referenced asset or set of assets, like an index.

[2] "The term 'commodity' means . . . all . . . goods and articles, except onions (as provided by section 13–1 of this title) and motion picture box office receipts (or any index, measure, value, or data related to such receipts), and all services, rights, and interests (except motion picture box office receipts, or any index, measure, value or data related to such receipts) in which contracts for future delivery are presently or in the future dealt in." *See* CEA section 1a(9).†

* **Editor's note:** footnotes annotated with † are retained in Committee file.

[3] *See Retail Commodity Transactions Involving Certain Digital Assets* † ("Actual Delivery Guidance"), 85 FED. REG. 37734 (June 24, 2020), *https://www.cftc.gov/sites/default/files/2020/06/2020-11827a.pdf*.

[4] FinCen defines money transmission as "the acceptance of currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means." See 31 CFR § 1010.100(ff)(5)(i)(A).†

veals gaps in ***Federal market oversight*** due to the interplay of the CFTC and SEC regimes:

- First, the scope of the CFTC's jurisdiction does not indisputably apply to all ***cash markets*** for (non-security) digital assets, and consequently U.S. customers of the operators of these markets do not have the benefit of legally enforceable, market-integrity and investor-protection requirements of those markets enforced by a Federal market regulator; and
- Second, not all digital assets indisputably meet the definition of a security under U.S. law, and consequently there are not clear, consistent and enforceable disclosure standards to inform investors about key information to assess risk relating to those digital assets.

As such, there is *no* clear market oversight for spot trading of (non-security) digital [assets].

Additionally, along with the unclear application of the "securities" definition as it applies to some digital assets, these gaps to date have discouraged participation by many in the U.S. digital-asset markets, including entrepreneurs, institutional market participants and other investors. In part due to these points, the vast majority of trading volumes in digital-assets markets (which FTX estimates to be roughly 95% of global volume) takes place on non-U.S. trading platforms, even though much of the human and intellectual capital driving the industry comes from U.S. persons—many of whom have left the U.S. to build and grow their businesses.[5] FTX believes this current state is harmful to U.S. competitiveness and is denying our country many of the benefits from the growing digital-asset industry, including attracting to the U.S. more capital formation, the best of the global workforce, intellectual property and tax revenue. In addition, hundreds of billions of dollars of digital asset stablecoins are currently backed by the USD dollar, a state that clear and consistent regulatory guidelines could help maintain.

U.S. Retail Commodity Transactions and the CFTC's Actual Delivery Guidance. Another piece of the U.S. regulatory patchwork for digital assets is the CFTC's treatment of retail commodity transactions. The CEA provides that a commodity transaction (including one involving a digital asset) must be listed on a CFTC-registered market, and is subject to CFTC's anti-fraud authority, if (1) it involves a retail participant, and (2) leverage, financing or margin is offered or used, *unless* the sale "results in actual delivery within 28 days".[6] The CFTC provided guidance to the public about how to interpret "actual delivery" under the statute—thus, there are circumstances when a retail, digital-asset transaction ***would*** fall under the CFTC's jurisdiction, and others when it would not.[7] Below we discuss FTX's views about how bringing all retail commodity transactions involving (non-security) digital assets under CFTC jurisdiction would be beneficial to the public.

The Regulation of Stablecoins. Another important part of the digital-asset ecosystem globally and in the U.S. are stablecoins, which are frequently used as a means to transfer collateral to and from digital-asset platforms and used as collateral once on the platform. Their regulatory treatment is also part of the overall patchwork of regulations that apply to the digital-asset ecosystem. There are several stablecoins used on U.S.-based digital-asset platforms that have been issued by U.S. state-regulated trust companies, and thus have the benefit of state-level prudential supervision.[8] Other stablecoins, some widely used, are not issued by a U.S. institution licensed at the Federal or state level. The ***President's Working Group on Financial Markets'*** recently released "Report on Stablecoins" ("***PWG Report***") provided a number of recommendations for the regulatory treatment of stablecoins, and FTX has shared its own recommendations for how to ensure the safety and soundness of stablecoins (included here as an exhibit), the core of which is a robust auditing and registration framework overseen by a Federal agency.[9]

There are other regulatory issues affecting the digital-asset industry in the U.S., but the foregoing are the most relevant to this Committee. Next, we address how this Committee, the Congress and the CFTC could rationalize the regulatory frame-

---

[5] *See https://ftx.com/volume-monitor* for data on trading volume on offshore *versus* U.S. platforms.

[6] *See* CEA section 2(c)(2)(D).†

[7] *See id.* at n. 5.

[8] Paxos Standard ("PAX"), issued by Paxos Trust Company, and the Gemini Dollar ("GUSD"), issued by Gemini Trust Company, are issued by Trust companies regulated by the New York State Department of Financial Services ("NYDFS").

[9] *See Exhibit B* to this statement; FTX's recommendations also can be found at *https://www.ftxpolicy.com/stablecoins*.

work for digital assets and pursue policies that would better protect investors and increase U.S. competitiveness.

3. A Vision for the CFTC as a Digital-Asset Supervisor

The CFTC already has considerable experience and expertise in the regulation of digital assets, and FTX believes Congress would be wise to leverage that expertise for the benefit of the public as well as the digital-asset industry. The CFTC authorized the first BTC-derivative-contract listing in 2014, nearly 8 years ago,[10] and the FTX US Derivatives business—the first crypto-native platform approved by the CFTC—has been licensed and supervised by the CFTC for nearly 5 years.[11] The CFTC-licensed, more traditional exchanges with some of the largest global volumes of derivatives-trading activity have had digital-asset derivatives trading on their platforms for more than 4 years, all under active supervision by the exchanges themselves as self-regulatory organizations, in addition to the oversight of the CFTC.

These facts show that there has been substantial capacity building at the CFTC over the years regarding digital assets. No other market regulator from a mature, major global economy can make this claim of experience and expertise about the digital-asset ecosystem, and Congress should actively consider how the agency can build on this to better deliver market-integrity and investor-protections goals to the public and ensure the benefits of the industry's growth can be maximized in the U.S. The following are recommendations for this Committee that would achieve those goals.

Expand the CFTC's Jurisdiction over Digital-Asset Spot Transactions. FTX recommends broadening the CFTC's jurisdiction to include, at a minimum, all spot transactions in (non-security) digital assets involving retail investors, regardless of whether the transactions currently fall within CFTC's jurisdiction under CEA section 2(c)(2)(D). This recommendation is consistent with relatively recent steps Congress has taken to expand the CFTC's jurisdiction over retail cash markets, including through the passage of the Dodd-Frank Wall Street Reform and Consumer Protection Act in 2010. This could be accomplished in several specific ways.

First, Congress should encourage the CFTC to work with industry to permit retail commodity transaction contracts related to digital assets to be listed on boards of trade registered with the CFTC, pursuant to the agency's existing authority over these transactions as established by CEA section 2(c)(2)(D) and as affirmed in the 2020 Actual Delivery Guidance. This would clearly promote the public interest and would not require further legislation, being consistent with the current authority of the CFTC.

Second, Congress could eliminate the 28 day "actual delivery" period in the CEA as it relates to digital-asset transactions, on the basis that doing so would clearly bring to more of these retail transactions the full panoply of protections from the CEA, which FTX believes also would clearly promote the public interest.[12]

Third, Congress could more broadly amend the CEA so that the CFTC has jurisdiction over all (non-security) digital-asset spot trading activity, not just retail commodity transactions under CEA section 2(c)(2)(D), and derivatives involving (non-security) digital assets. Such a step also should involve a consideration of the appropriate disclosure regime for digital assets that ensures investors are adequately informed of their risks.[13] In the meanwhile, Congress in general should actively encourage the CFTC to appropriately broaden its interpretation of its authority over digital-asset spot transactions to better rationalize and condense the patchwork of regulations governing U.S. digital-asset activity, facilitating the offering of both market types on one platform.

In ***FTX's Key Principles for the Market Regulation of Crypto-Trading Platforms (Market Regulation Key Principles),*** we outlined the benefits to offering these two market types under one unified system, with one rule book and one technology platform to manage risks related to all trading activity in customer accounts.[14] This approach facilitates one collateral and risk-margin program for cus-

---

[10] *See* TeraExchange, LLC's Filing under CFTC Regulation 40.2, Certification of BTC Swaption Contract,† April 24, 2014; *https://teraexchange.com/style/images/rnd/instr/Tera%2040.2%20Filing%20-%202014-22%20Listing%20of%20Swaption.pdf.*

[11] *See* CFTC Orders Granting DCO, SEF and DCM licenses to LedgerX.

[12] This approach would encompass those crypto transactions that, per the 2020 Actual Delivery Guidance, are not offset in any way, and whose proceeds are fully withdrawn to external, customer-controlled wallets within 28 days.

[13] *See* 'Token Issuances' at *https://www.ftxpolicy.com/areas-for-crypto-regulation* for a sketch of a possible disclosure regime for digital asset issuances.

[14] *See Exhibit C* to this statement, and *https://www.ftxpolicy.com/*.

tomer accounts holding both cash and derivatives positions, allowing the platform to better manage market risk, and reducing operational risk owing to a single technology stack for the front end (the user interface) to the back end (settling and risk managing positions). Public policy should permit this one-rule-book model due to its risk-reducing and customer-protection attributes.

Fourth, as recommended in ***FTX's Market Regulation Key Principles,*** Congress, the CFTC and the SEC should pursue a scheme where a digital-asset platform operator could opt into a program of joint supervision by the CFTC and SEC when there is joint jurisdiction over digital assets listed on the platform (*e.g.,* when listings include non-security digital assets as well as digital assets that are securities). Under these circumstances, FTX recommends that one of the market regulators serve as the primary regulator, and the other as the secondary regulator, for market oversight. This type of paradigm is familiar to market regulators globally and could include the accommodation of one rule book, one matching engine and risk engine supported by one technology stack. FTX believes this approach could largely be created under existing CFTC and SEC authorities, but Congress should encourage the agencies to leverage their authorities today with these goals in mind and consider legislating such an approach when feasible.

Embrace the Direct-Membership Market Structure of Digital-Asset Platforms. The CFTC should continue to permit and embrace a market structure that allows investors to become direct members of the CFTC-licensed exchanges and clearinghouses that offer digital assets, without the need for intermediation. FTX's CFTC-regulated business has been operating with this type of market structure for nearly 5 years, without any loss of customer funds or significant platform outages, and has demonstrated that such a business model can comply with the CEA and continue to deliver on important investor protections embodied by the CEA. U.S. policy should remain market-structure neutral and allow non-intermediated markets for digital-asset products, so long as key investor protections can be adequately ensured. Every major incumbent U.S. derivatives trading venue offers a direct member clearing solution, and certain incumbent platforms have the majority of their users as direct members—this is not a new concept for the CFTC and its surveillance and risk teams.

FTX also published ***FTX's Key Principles for Ensuring Investor Protections on Digital-Asset Platforms*** ("***Investor Protection Key Principles***"), where we identified the most important components of an investor-protection regime (which the CEA and CFTC rules also reflect), and how FTX offers those protections today with the direct-membership model.[15] These components include:

- maintaining adequate liquid resources to ensure the platform can return the customer's assets upon request;
- ensuring the environment where customer assets are custodied, including digital wallets, are kept secure;
- ensuring appropriate bookkeeping or ledgering of assets and disclosures to protect against misuse or misallocation of customer assets;
- ensuring appropriate management of risks including market, credit/counterparty, and operational risks; and
- avoiding or managing conflicts of interest.

While the CFTC's rules reflect these important principles today, they often contemplate an intermediary such as a "futures commission merchant" (FCM) bearing the responsibility of those protections to the investor. The CFTC wisely has allowed a direct membership market structure so long as those investor protections are ensured and enforced.

The ***Investor Protection Key Principles*** touch on two key points that the CFTC has recognized. *First,* technology advances have enabled a non-intermediated market structure that, combined with effective platform operations, can provide the above-identified protections more effectively, ultimately leading to an overall risk-reducing market structure, for the benefit of investors. *Second,* to the extent that legacy regulations or policies would assume or require an intermediary to provide these protections, that approach often imposes unnecessary burdens and costs (including fees and both capital and operational inefficiency) on investors and markets and obscures market-data without corresponding benefit. The CFTC and Congress should address and update any such rules through continued, appropriate interpretations in the case of the CFTC, and refinements to corresponding legislation in the case of Congress, to ensure equitable access to financial markets.

---

[15] *See Exhibit D* to this statement, and *https://www.ftxpolicy.com/investor-protections*.

Ensure the Safety and Soundness of Stablecoins. Stablecoins have become a critical component of the digital-asset ecosystem, and policy makers have raised concerns about their growing market size and whether the lack of uniform Federal oversight presents systemic concerns. While the ***PWG Report*** investigated bank-like supervision for ***all*** stablecoin issuers, such an approach might not be necessary so long as the core requirements of stablecoin oversight are met. These include:

- Daily attestations of what assets (cash, bonds, *etc.*) are backing a stablecoin;
- Periodic audits to confirm the asset backing is as claimed;
- Federal oversight and ability to inspect the assets;
- Haircuts for assets with moderate risk; and
- An open line for law enforcement to blacklist addresses and persons associated with financial crimes.

The CFTC could play an important role in creating a workable framework with these requirements.

First, the Congress could give the CFTC authority to license stablecoin issuers and subject them to these core requirements, perhaps by creating and authorizing a new registration scheme for stablecoin issuers or by otherwise allowing them to seek an existing CFTC license with new commiserate authorities, such as a DCO license. Indeed, a DCO is well accustomed to taking custody of assets, providing relevant reports to ensure their safekeeping, undergoing related audits (*see* ***FTX's Investor Protection Key Principles***), and managing risks through appropriate collateral management and marking to market. The appropriate duties and responsibilities of a stablecoin issuer are much the same.

Second, the CFTC without any new legislation could require DCOs providing settlement and clearing services for digital-asset platforms to condition the acceptance of stablecoins as collateral by the DCO on the stablecoin issuer meeting these same core requirements, and the stablecoin issuer providing the needed attestations and audits to verify they are being met. The CFTC could require this through review and enforcement of DCO policies and procedures related to the DCO's approved risk-management program. To be sure, considerable public policy could be made through creative use of the CFTC's existing authorities as suggested, leading to standardized practices for stablecoin issuers that would protect the safety and soundness of the broader financial system.

We believe there is some urgency to create a practical regulatory solution that promotes disclosure and transparency, but that does not inhibit the value that stablecoins provide to markets and market participants. All aspects of digital asset regulation will be iterative and done in phases. For stablecoins, getting a general principles-based disclosure and transparency requirement in place now (perhaps via CFTC guidance, as a follow-on to certain CFTC stablecoin enforcement initiatives), while deferring a decision on the approach to some of the broader questions (such as whether "registration" is required and which agency should oversee that registration), would deliver a substantial amount of regulatory value.

Adequately Fund the CFTC to Ensure Resources to Protect Digital-Asset Investors. Finally, the successful implementation of most of the foregoing recommendations would depend on the CFTC having adequate resources to do so. FTX supports reasonable steps to provide those resources, including by contributing its own fair share of funds for use by the CFTC to expand its purview over digital assets. A program for generating and conveying such resources to the CFTC could be designed in a variety of different ways, and FTX stands ready to engage with this Committee and the Congress more broadly to assist in designing and contributing to such a program.

Conclusion

FTX is grateful to this Committee for the opportunity to share information about the digital-asset industry, our business, as well as the recommendations for how the CFTC in particular can contribute to the industry's growth. FTX believes the CFTC and this Committee could play an even more prominent role in the digital-asset ecosystem and bring greater investor protections by closing some of the regulatory gaps identified in this statement. FTX believes that such efforts would combine the best aspects of traditional finance and digital-asset innovations, one of our primary goals, and further empower investors and consumers by consolidating access to the tools they seek for economic security, all in one place, and from a singular, risk-reducing platform.

Sincerely,

SAM BANKMAN-FRIED,
Co-Founder and CEO of FTX.

EXHIBIT A

The FTX group of companies (FTX Group or FTX) was established by three American citizens, Samuel Bankman-Fried, Gary (Zixiao) Wang and Nishad Singh, with international operations commencing in May 2019 and the U.S. exchange starting in 2020. The business was established in order to build a digital-asset trading platform and exchange with a better user experience, customer protection, and innovative products, and to provide a trading platform robust enough for professional trading firms and intuitive enough for first-time users. In the U.S., the company operates a federally regulated spot exchange that is registered with the Department of Treasury (via FinCEN, as a money services business) and also holds a series of state money transmission licenses. Our U.S. derivatives business is licensed by the U.S. Commodity Futures Trading Commission (CFTC) as an exchange and clearinghouse. FTX US also holds a FINRA broker dealer license. FTX's international exchange, which is not available to U.S. users, holds a series of marketplace licenses and registrations in many non-U.S. jurisdictions.

The core founding team had unique experience to develop an exchange given their experiences in scaling large engineering systems at premier technology companies, combined with trading experience on Wall Street. This brought to the effort an understanding of how to build the best platform from scratch, as well as what that platform should look like, unencumbered by legacy technology or market structure. ***FTX has aimed to combine the best practices of the traditional financial system with the best from the digital-asset ecosystem.***

Early International Success. The international *FTX.com* exchange has been extremely successful since its launch. This year around $15 billion of assets are traded daily on the platform, which now represents approximately 10% of global volume for crypto trading. The FTX team has grown to over 200 globally, the majority of whom are responsible for compliance and customer support. The FTX Group's primary international headquarters and base of operations is in the Bahamas, where the company is registered as a digital asset business under The Bahamas' Digital Assets and Registered Exchanges Act, 2020 (DARE).

FTX % Global Volume, 15d

In addition to offering competitive products, the FTX platforms have built a reputation as being highly performant and reliable exchanges. Even during bouts of high volatility in the overall digital-asset markets, the *FTX.com* exchange has experienced negligible downtime and technological performance issues when compared to its main competitors. We believe the dual-track focus on customers and reliability, plus compliance and regulation, are key reasons why FTX has also experienced the fastest relative volume growth of all exchanges since January 2020.

The core product consists of the *FTX.com* web site that provides access to a marketplace for digital assets and tokens, and derivatives on those assets. Platform users also can access the market through a mobile device with an FTX app. The core product also consists of a vertically integrated, singular technology stack that supports a matching engine for orders, an application programming interface or API, a custody service and wallet for users, and a settlement, clearing and risk-engine system. In a typical transaction, the only players involved are the buyers, sellers, and the exchange, without any other intermediaries.

The FTX Group has operations in and licenses from dozens of jurisdictions around the world, including here in the U.S. and in Europe. At the time of this writing the FTX platforms have millions of registered users, and the FTX US platform has around one million users. For *FTX.com,* roughly 45 percent of users and customers come from Asia, 25 percent from the European Union (EU), with the remainder coming from other regions (but not the U.S. or sanctioned countries, which are blocked). In comparison to the international exchange, nearly all users of FTX.us are from the U.S.

U.S. Operations. FTX services U.S. customers through the FTX US businesses, which includes the spot exchange, FTX US Derivatives, the NFT marketplace, and a soon-to-go-live FINRA broker dealer (FTX Capital Markets). FTX US is housed under a separate corporate entity from FTX international and is headquartered in Chicago, IL. It has a similar governance and capital structure to the overall corporate family, and also has its own web site, FTX.us, and mobile app. As with *FTX.com,* the core product is an exchange for both a spot market for digital assets as well as a market for derivatives on digital assets. Like other crypto-platforms in the U.S., the spot market is primarily regulated through state money-transmitter laws.

The U.S.-derivatives-market product is provided by FTX US Derivatives, which was formed through the acquisition and re-branding of LedgerX and is being integrated with the overall FTX US platform. The product offers futures and options contracts on digital assets (or commodities) to both U.S. and non-U.S. persons. FTX US Derivatives operates with three primary licenses from the U.S. Commodity Futures Trading Commission (CFTC): a Designated Contract Market (DCM) license, a Swap Execution Facility (SEF) license, and a Designated Clearing Organization (DCO) license. Prior to its acquisition, this business was the first crypto-native platform issued a DCO license by the CFTC in 2017, which was a milestone for the agency and the digital-asset industry. That license was later amended in 2019 to permit the clearing of futures contracts on all commodity classes and not just digital assets.

Commitment to a Diverse Workforce. We are proud of our workforce at FTX and believe that one of our key strengths is a culture of mutual respect and cooperation. This type of culture is borne from the diversity of our team, which necessitates a spirit of empathy, understanding and humility. These traits in our workforce are good for business and are much of the reason we have been successful at understanding our customers and their needs, and executing on products that meet their needs. FTX has employees from all over the world with diverse ethnic backgrounds, and 60 percent of women in our workforce are in senior management positions. The majority of our global leadership comes from diverse backgrounds.

Commitment to Mitigating Climate Impacts. FTX is very serious about minimizing our impact on the global environment where we live and work, and as a company we have taken several important steps to ensure this. Here, I would like to share several key points to explain why FTX's environmental impact is *de minimis,* but nonetheless explain the additional steps the company has taken to reduce even further this impact. *First,* FTX has no factories or physical products and therefore does not leverage global shipment networks, a substantial source of energy consumption. FTX has a small workforce with a small physical-office footprint, renting only a few small offices spread out around the world, and operates online. FTX corporate operations, therefore, do not have direct impacts on climate change at a globally relevant scale.

Second, while digital asset deposits to and withdrawals from FTX platforms unavoidably require some energy consumption as public blockchains facilitate and record those transactions, on FTX over 80 percent of deposits and withdrawals use low-cost, carbon-efficient Proof of Stake (PoS) blockchains. These PoS networks contrast with Proof of Work (PoW) blockchains such as the Bitcoin (BTC) blockchain, which consume significant amounts of energy to maintain the network. By using PoS blockchains for the vast majority of FTX deposits and withdrawals, FTX massively reduces the overall climate impact of blockchains. To facilitate the remaining approximately 20 percent of deposits and withdrawals, energy consumption is relatively small, but FTX subsidizes the blockchain network fees to share in paying the costs of that energy consumption. Separate from deposits and withdrawals, transactions and transfers on the FTX exchanges themselves (which is the overwhelming majority of our user activity—100% of our $15 billion in average daily trading volume occurs on the exchange itself) do not require public blockchain activity and require only the amount of energy needed to run a cloud-based trading venue.

Third, FTX also has endeavored to take ownership of our portion of the environmental costs of mining associated with public blockchains and has purchased carbon

offsets to neutralize those costs. Estimating the costs of energy consumption and carbon output associated with blockchain mining is difficult because mining is decentralized, and discerning how much energy is coming from which source is elusive. Nonetheless, FTX estimates that it costs $1 million per year to take ownership of those costs, and has purchased a total of 100,000 tons of carbon offsets through two providers for $1,016,000. Additionally, FTX through its affiliated arm, FTX Climate, created a comprehensive program to focus on the most impactful solutions to climate change possible. In addition to achieving carbon neutrality, our initial program funds research that we believe can have an outsized impact, as well as supports other special projects and carbon-removal solutions. FTX plans to spend at least $1 million per year through FTX Climate. Those interested in learning more about these initiatives can find more information at *https://www.ftx-climate.com*.

Fourth, FTX believes energy consumption by PoW blockchains and its impacts should be assessed within the appropriate context, which we believe should include consideration of their benefits, an understanding of their differences with PoS networks and how each type of network is being leveraged and growing, as well as a comparison to other energy-consuming activities or even industries. For example, BTC has delivered benefits to many as measured by access to financial products, asset transmission, and wealth creation, which should be weighed against the network's energy costs.[16]

Additionally, while PoW networks attract attention for their energy consumption, transactional activity on PoS networks is growing substantially due to their ability to process a greater number of transactions in a shorter period of time at a lower cost. FTX believes these PoS networks will become increasingly important over time, which will continue to minimize the overall climate impact of blockchains. And finally, the energy consumption by PoW blockchains is relatively small when compared to other industries to which the BTC network in particular is often compared.[17] Of assets whose futures trade on CFTC-regulated venues, BTC actually ranks fairly low in terms of environmental impact, relative to traditional, physically mined commodities, oil, livestock and other environmentally impactful assets.

Commitment to Giving Back. FTX is committed to improving the lives not just of our customers through superior products, but also the lives of those in the broader global community. Toward this end, FTX created the FTX Foundation, which was founded with the goal of donating to the world's most effective charities. FTX has pledged to donate one percent of net revenue from fees to the foundation, and its founders have pledged to donate the majority of what they make. FTX, its affiliates, and its employees so far have donated over $50 million to help save lives, prevent [suffering and] ensure a brighter future.

EXHIBIT B

Stablecoin Regulation

Context on stablecoin regulation

As the cryptocurrency industry matures, it's vital that a robust regulatory regime grows alongside it which takes seriously its duty to protect consumers, ensure transparency, and prevent illicit activity, while still allowing for innovation and growth.

Stablecoins play a crucial role in the cryptocurrency ecosystem; the majority of all transactions in crypto are settled via stablecoins, and they are one of the most promising payment tools for the broader financial sector. It is also, as of now, unclear exactly what regulatory regime stablecoins will end up being placed in.

What is a stablecoin?

Let's start with the core question: what exactly is a stablecoin?

There are a wide variety of stablecoin designs that have been utilized in the cryptocurrency ecosystem. For illustrative purposes, in this article we will assume a stablecoin on the U.S. Dollar, although parallel assets do exist on EUR, GBP, and other currencies. We will also imagine that it is 1:1; that is, 1 token represents 1 U.S. Dollar. We will imagine that the token's ticker to be STBC.

---

[16] *See* "Everything We Want Costs Energy, Including Bitcoin," by Benjamin Powers, *Coindesk,* Apr. 22, 2021; *https://www.coindesk.com/tech/2021/04/22/everything-we-want-costs-energy-including-bitcoin/; see also* "The Bitcoin Mining Network: Trends, Average Creation Costs, Electricity Consumption & Sources," CoinShares Research, June 2019 Update, *https://coinshares.com/assets/resources/Research/bitcoin-mining-network-june-2019-fidelity-foreword.pdf*.

[17] *See* "On Bitcoin's Energy Consumption: A Quantitative Approach to a Subjective Question," *Galaxy Digital Mining,* May 2021, Rachel Rybarcyzk, Drew Armstrong, Amanda Fabiano. *https://docsend.com/view/adwmdeeyfvqwecj2*.

In this construct, this imaginary stablecoin, STBC, is a blockchain-based asset that can be exchanged for a U.S. Dollar. That would typically be accomplished through the following mechanics and arrangements:

Reserves: Typically, a stablecoin is backed by one or more USD accounts or other similar assets, generally held at a bank, in an account under the name of the stablecoin sponsor, issuer, or other similar body. The USD value of the assets should be at least the supply of the stablecoin.

Token: A blockchain-based token, STBC, where one token represents $1 (as supported by the creation / redemption process, described below). These could be issued by a private company, a central bank, or a decentralized protocol.

Creation/Redemption: In order to create 1 STBC token, an eligible user must send $1 to the reserve account. In return, the protocol mints 1 new STBC token and sends it to the user.

Similarly, an eligible user may send 1 STBC token back to the protocol to redeem it for $1. The protocol destroys the token and sends $1 back to the user.

What are the benefits of stablecoins?

We believe that stablecoins are one of the most important innovations of the cryptocurrency industry.

Let's say you want to send $20 to a friend. What are your options?

(a) You could hope that both you and your friend use the same peer-to-peer transfer app (*e.g.,* Venmo), and then separately each of you figure out how to send money to/from that app.

(b) You could send a $20 wire transfer to your friend. This would likely take a day and cost $5+ in fees; and if it's international, it might take a week and cost substantially more in fees.

(c) You could send $20 via ACH, if both you and your friend use U.S.-based USD bank accounts. Then, the transfer would not fully settle for months, exposing both parties to "chargeback risk".

(d) You could go to an ATM, withdraw $23 paying a $3 fee, and hand $20 to your friend, who would then have to find a way to use the physical dollar bills.

(e) You could send 20 STBC to your friend's cryptocurrency wallet; if you use an efficient blockchain (or both use the same exchange), it will arrive in less than a minute, costing a tiny fraction of a penny in fees.

Option (e), the stablecoin, has a compelling case here as an efficient means of transfer.

Taking our real-world use case a step further, consider that a user wants to build a blockchain-based application. How should the application's users contribute and withdraw assets?

Here, the users face the same potential options and cost structures as before; once again, stablecoins are the cheapest, safest, and fastest way for a user to engage with that application.

What are the risks of stablecoins?

There are three major intertwined risks associated with stablecoins.

Reserve volatility risk

If the stablecoin is backed by something other than U.S. Dollars in a bank account, the asset might depreciate against USD. If, for instance, you were to back a stablecoin with 1,000,000 tokens issued with $1,000,000 of the SPY (S&P500) ETF, and stock markets decreased 5% in price, you would be left with only $950,000 backing 1,000,000 stablecoins—meaning that the "stable" token had in fact fallen in value, at least in regards to the reserves it is purported to be redeemable for!

Unlike investment products where customers gain from appreciation in the assets backing the product, there is generally no way for a stablecoin to be worth more than $1, as customers can always create more for $1 each. This means that the core philosophy behind the assets backing a stablecoin should be to focus on assets with low volatility which are very similar to USD. U.S. Treasury bonds may be an appropriate asset for a stablecoin's reserves; if Bitcoin is used, it has to be over-collateralized to an extent that there is very little risk of loss to the stablecoin holders. Backing 100 stablecoins with $101 of BTC is untenably risky: a mere 2% decrease in Bitcoin markets would cause the stablecoin to be under-backed and no longer fully redeemable for $1. Backing 100 stablecoins with $400 of BTC, on the other hand, is substantially more defensible, as there is very little risk of a 75% move before the reserves would have a chance to de-risk. Any stablecoin issuer or

designer must have a transparent, robust risk model to mitigate the volatility of its reserves, including determining which assets are appropriate for its reserves.

Redemption risk

A related worry is that a user might own 1,000 STBC, go to the issuer to redeem their STBC, and be denied.

This might happen if the reserves had in fact run out of dollars and so there was nothing left to redeem STBC for; this would likely imply the reserves had not been in USD, and had fallen in value.

Alternatively, this could happen if the issuer arbitrarily decides to block your redemption, possibly to try to keep more impressive metrics for STBC.

Either way, the lack of ability to redeem (or a lack of transparency related to redemption process and requirements) presents a risk to the user.

Financial crimes

One final risk of stablecoins is that they could be used for financial crimes, or to finance illicit activities.

Any stablecoin issuer or designer must include creation, redemption, and use mechanics that, in harmonization with regulation, address and avoid this use case.

What is a sensible stablecoin regulator framework?

As noted above, we believe that stablecoins have presented a significant positive use case to the world, and they continue to hold the potential to revolutionize the payments and remittances industry. Stablecoins could in the future revolutionize the payments industry, drastically reducing friction and transaction costs, delivering to many around the world the benefits that come with having access to reliable and usable value transmission. As such, we think it is important to ensure that the ongoing regulatory discussions around the approach to a framework for stablecoins be based on a practical structure that solves equally for usability, reliability, transparency, consumer protection, and the identification and prevention of financial crimes.

We look forward to engaging with regulators on examples of what such a framework might look like. There are many different approaches and we remain open and excited for feedback and engagement from regulators and from other participants in the cryptocurrency industry.

As outlined above, there are real risks associated with stablecoins, and any framework should work to mitigate those.

As such, while we look forward to continuing dialogue on the details, we would be in favor of a proposal for a transparency-based reporting and registration regime for stablecoins.

A proposed framework might look like the following:

(a) All stablecoins issued to U.S. users must be registered on an official list of "regulated stablecoins" under the oversight of one or more U.S. regulatory department(s).

(b) The registration itself would be focused on transparency and reporting, on a notice filing basis, coupled with clear obligations on recordkeeping, reporting, and regular examination. The regulatory departments authorizing the program would have the ability to decertify registered stablecoins.

(c) The registration would involve publishing a daily Reserves List which details what the total net value of the stablecoin's reserves are, and breaks that down into exact quantities of specific categories (*e.g.,* "100 USD in Bank XYZ; $95 of short-term U.S. treasury bills; $50 of Tier-1 commercial paper of U.S. companies; $30 of Tier-1+ commercial paper of European companies; $10 of [other suitable assets as permitted by the regulation and by that stablecoin's registration document]")[.]

(d) The registration would require that the issuer maintain "sufficient" reserves. This could be defined by a set of haircuts on various types of reserves. *E.g.,* perhaps a 0.10% haircut on USD in an FDIC insured bank account; a 1% haircut on short-term U.S. treasury bills; a 10% haircut on Tier-1+ commercial paper; a 15% discount on Tier-1 commercial paper; a 20% haircut on EUR, GBP, JPY, CHF, CAD, AUD, SGD, HKD, *etc.;* and a 50% haircut on Bitcoin.

(e) The registration would require semi-annual audits by an accounting firm to confirm that the reserves are as represented.

(f) The registration would require stablecoins to have clear and transparent redemption requirements (*e.g.,* based on Know Your Customer documentation) and a clear customer complaint process if a redemption is denied.

(g) To address financial crimes, all registered stablecoins would have to be on a public ledger, and the creation and redemption process must be sufficiently structured in order to ensure that stablecoins associated with illegal activity (as observed via on-chain surveillance and analytics tools, via a suite of standard blockchain surveillance software) cannot be redeemed.

As noted above, this is a basic strawman framework for how the key components of a potential stablecoin registration program might look. Each of these points are designed to preserve the usability of stablecoins while solving for regulatory considerations that need addressing. If designed in the right way, this framework could enhance the ultimate usability of stablecoins. We very much look forward to engaging with policymakers, regulators, and market participants on these concepts.

EXHIBIT C

FTX's Key Principles for Market Regulation of Crypto-Trading Platforms

In this piece we identify a series of ten principles (and in some instances, proposals) that should guide policy makers and regulators as they build the regulatory framework for spot and derivatives crypto markets. FTX does not propose specific legislation here but rather principles and proposals that could be reflected in policy making, whether in the form of legislation, rulemaking, or other regulatory action. Many of these principles are familiar to traditional securities and derivatives markets, but some of the principles reflect market-structure choices made by FTX and other crypto-platform operators that we believe lead to superior outcomes for investors and, indeed, the public. FTX therefore believes public policy should not only permit these choices but promote those that lead to such outcomes. Some of the discussion here focuses on the U.S. marketplace, but the principles and proposals are applicable in any jurisdiction globally. FTX appreciates being able to engage in this dialogue with policy makers and regulators, and we are always happy to pursue follow-up discussions with interested parties. *See* our prior policy blog posts at *https://www.ftxpolicy.com*.

1. Proposing One Primary Market Regulator with One Rule Book for Spot and Derivatives Listings

In the U.S. regulatory ecosystem, spot markets and derivatives markets are subject to different regulatory programs, and this can lead to inefficient and non-optimized market structures. In this post we propose as a solution an alternative regulatory approach that would provide market operators the ability to opt in to a unified regulatory regime for spot and derivatives marketplaces, through a primary regulator model.

As many know, the CFTC is the primary regulator of commodity derivatives marketplaces, while the SEC is the primary regulator of cash securities marketplaces, and the two agencies share oversight responsibility for certain aspects of security derivatives marketplaces.

In parallel, there is a further regulatory split for spot markets (sometimes called "cash markets" in the traditional commodities or securities context), where the applicable regulatory program depends on whether the product being traded is categorized as a security (where the SEC regulates) or a commodity that is not a security (where the states largely regulate, via money transmitter or money services business licensing).

Against that backdrop, and particularly outside of the U.S., we observe that many crypto-native trading-market operators offer for trading both spot transactions on crypto assets as well as derivatives on those assets, under a unified rule book, one collateral and risk-margin program, and a single technology stack. This model is generally not found in the U.S. given the jurisdiction's historically fragmented approach to market regulation. Nonetheless, we believe that for traded crypto markets, the key principles for market regulation (customer and investor protection, market integrity, preventing financial crimes, and system safety and soundness) generally apply equally across spot and derivatives markets, and commodities and securities markets. That is, the regulatory label on a given product or market need not change the core goals of regulation, and the same rulesets should generally apply across all markets. For that reason, we strongly support offering a single unified regulatory program for crypto market operators.

Specifically, in jurisdictions where there is a primary derivatives-market regulator separate and distinct from a primary cash-markets regulator (such as in the U.S.), policy makers and regulators should seek to permit qualified crypto markets operators to run a single rule book, risk program, and technology stack, approved and overseen by a primary regulator (perhaps chosen by the marketplace on an opt-in

basis and supported thereafter by inter-regulator cooperation and information sharing, with the possibility of the primary regulator shifting if the underlying product mix evolves in a certain way), that governs the listing and trading of both spot cash transactions in crypto assets as well as derivatives on crypto assets.

Much of this can be achieved today under existing statutory authority and with creativity and cooperation by and among market regulators. With some specific issues, however, clarity might be needed from legislation. Under the current U.S. paradigm, for example, we acknowledge that it is unlikely to be absolutely clear at any given moment, absent legislation, whether all of the crypto products listed on such a venue are definitively "within" or "without" the jurisdiction of either of the market regulators. However, between two possible regulatory solutions under this paradigm—which are (1) that regulators can prohibit the marketplace altogether (via indecision, decree, or a combination of the two), or (2) that regulators can innovate and cooperate to ensure that key regulatory and policy goals are met in a clear and robust way while also permitting the marketplace to operate—we think the second approach offers a compelling option.

Said more explicitly, in jurisdictions where there are two mature market regulators, FTX proposes the permissibility and adoption of a reasonable and rigorous framework that would allow a crypto-markets platform operator to elect one market regulator as its primary regulator for a unified spot and derivatives trading book, subject to adherence to a cooperative framework in which the other market regulator acts a secondary regulator while maintaining appropriate visibility into the platform's operations, but not day-to-day supervisory responsibilities. (Indeed, a similar approach is used today when a market regulator from one jurisdiction "recognizes" the framework of a different jurisdiction where a primary, "home" regulator resides, and then defers to that primary regulator's regulations and rulesets so long as they are sufficiently comparable.)

We propose a functional-based approach, where the regulation and the trading venue rule books that comply with that regulation should be largely modeled after existing market regulations for securities and derivatives markets, on the basis that most jurisdictions will follow this same approach. FTX believes that there is a unique current opportunity for U.S. regulators to take a leadership position in the global crypto markets regulatory discussion, and we believe that modeling a primary regulator model on existing market regulation will foster standardization and harmonization of regulation globally, paving the way for international adoption and reciprocal jurisdictional recognition.

To underscore why we are so focused on these regulatory issues—it is because we believe that getting crypto market regulation appropriately calibrated is critical for the continued development of healthy, transparent, and well-functioning global crypto markets, which we believe will deliver knock-on positive effects to the global economy as a whole. And we think our proposed approach, in addition to solving for regulatory uncertainty and fragmentation, would also reduce operational complexity by allowing matching engines for both spot and derivatives transactions to operate on the same platform with the same user interface. This in turn would reduce operational risk to the platform, and promote capital efficiency by allowing collateral in support of both order books to rest on the same platform. In the rest of this piece, we discuss in more detail various additional practical benefits of crypto marketplace operators being subject to unified primary regulator oversight.

2. Full-Stack Infrastructure Providers and Maintaining Market-Structure Neutrality

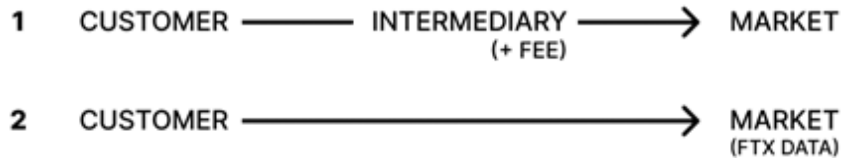
Regulation should be market-structure agnostic, provided that the core regulatory issues (identified above as customer and investor protection, market integrity, preventing financial crimes, and system safety and soundness) are addressed. Technology has enabled any capable entity to perform the various functions involved with the pre-trade, execution, and post-trade phases of the lifecycle of an asset trade or transaction in a single regulatory stack—in fact, to split up those functions, from a technology perspective and when building a market from the ground up, would require a forced and artificial deconstruction.

However, one of the things that prohibits an entity from taking on any or all of these functions can be the specifications of a regulation. To say it another way, much of current market structure is a creation of regulatory artifact rather than a reflection of a thoughtful and holistic approach to marketplace design, efficiency, transparency, and risk management. FTX built and continues to evolve its trading ecosystem with the latter approach in mind.

We believe that so long as the various needed functions necessary to the lifecycle of a transaction are being met, policy makers would do well to remain otherwise neutral on how a market is structured (so long as appropriate customer protections also are in place, discussed below). For one example, most market regulation today

envisions an intermediated marketplace where an intermediary such as a broker interfaces directly with a customer (think back to calling in, or mailing in, your order to a broker that had access to the physical exchange floor). In contrast, crypto-asset platforms largely dispense with this mode in favor of a direct-membership market structure, where end investors onboard directly to the platform for trading, and not through an intermediary or broker (although service providers such as internet and data-center providers are involved).

A non-intermediated market allows all users to get the same access to market data (consider that FTX's data is free, globally, *versus* much of the global trading venue industry where data fees are a material commercial component of the business), connectivity, and key features related to functionality and risk management, regardless of the sophistication of the user. The positive implications of this are potentially enormous, and are only just beginning to be seen, interestingly, around the direct-to-consumer crypto marketplace models. The public is better served if the barrier to entry to transact competitively with global markets is an internet connection, rather than a $100,000 (or more) data-subscription fee and a costly fee- or commission-based relationship with a broker that merely plugs you into the trading venue's technology. Non-intermediated markets create a more level playing field that's often lacking in many traditional financial systems, whose market structures have created a number of challenges including real and perceived conflicts of interests between intermediaries and their customers.



Consequently, a direct membership market structure should be expressly permitted (not required, but permitted) so long as the relevant customer protections continue to be afforded, in this case by the platform provider.

3. Custody of Crypto Assets—Key Functional and Disclosure Requirements

For crypto assets, the asset is safekept in a wallet, where custody can be performed by the asset owner or by a wallet holder on the customer's behalf. Where custody is performed on a customer's behalf by a platform operator or intermediary, appropriate safeguards should be disclosed in policies and procedures of the custodian. Key areas of focus and disclosure should include: wallet architecture; whether insurance is provided by the custodian; how private keys are kept secure, managed and transferred; managing risks related to insider collusion or fraud; and physical security of data centers.

Importantly, in the case of platform operators, consideration should be given to the increasingly common practice of using third-party providers for data centers (*i.e.,* cloud-service providers) as well as custodial services. In these instances, the platform operator will not itself perform these functions but nonetheless will be held responsible by users for them, and users should be given visibility into how third parties will address the aforementioned issues. Market supervisors should require regulated platform operators to perform regular diligence on their vendors and to have sufficient business continuity and disaster-and-recovery programs in place in connection with their vendor suite.

4. Full-Stack Market Infrastructure Providers and the Lifecycle of a Trade—Addressing Risk Related to Token Issuance and Asset Servicing, Orderly Markets and Settlement of Trades, Cross Margining and Risk Management of Positions

Again, native crypto-trading platforms integrate into a whole the system for custody, issuing tokens, settlement of trades, and risk managing positions with one technology stack. In creating or fine-tuning a regulatory framework for these platforms, policy makers should ensure that market supervisors understand this system through well developed and clear policies and procedures disclosed by the platform operator. The framework should address the following key issues related to the lifecycle of a spot or derivatives trade.

Token Issuance and Asset Servicing

Token issuers who have access to the platform for purposes of issuing a token should be governed by disclosed policies and procedures that explain the listing standards for tokens. In some cases, existing securities laws will apply, in which

case the policies and procedures should explain how such laws are complied with by the platform as it relates to issuing the security tokens.

This document does not address whether existing securities laws should be amended to account for distributed-ledger technologies and new methods of issuing securities in tokenized form. Suffice it to say here that some of the traditional requirements for central securities depositories might not be appropriate for platforms that offer these services, but others will be.

To the extent a token is not a security but has some security-like features at some point in time, and policy makers otherwise have not addressed whether such tokens should be treated as securities, a platform operator in any case should be required to disclose, or otherwise facilitate disclosure of (*i.e.,* most material information for a token can be easily found on the Web, and a platform could direct a platform user to this information), key material information about the token issuer as part of the platform's listing standards.

Likewise, in the case of all tokens, the platform operator should develop and disclose policies and procedures for how a token issuer will interact with the platform for purposes of facilitating asset servicing, so that supervisors and platform users both can understand and assess the risks to the platform posed by token-issuance functionality. This would be especially relevant in the case of security tokens, where dividend payments and changes in ownership, for example, would impact the token and the owner of the token.

Market Surveillance

Good public policy would require that a crypto-platform operator has policies and procedures concerning the practices and technology used to perform market surveillance of the platform's trading environments in order to curb market manipulation and promote orderly markets. This is standard policy for traditional supervised markets and should be carried over to supervised crypto markets as well.

Settlement

With regard to settlement, our recommended policy would require the platform operator to have clear and transparent policies and procedures that explain when settlement of a transaction becomes final, and the conditions and circumstances under which the platform provider would reverse settlement due to errors, *etc.* By and large, regulated venues do this today in their terms of service, *etc.,* and we think it is important they continue to do so.

One of the hallmarks of the FTX trading experience is to allow users to pair in a transaction nearly any combination of assets for purposes of settlement—for example, a user could exchange BTC for USDC or for SOL. Sound policy would allow the platform to settle transactions by pairing the assets with any of the others listed on the platform, including stablecoins or cash fiat currencies (see below for discussion of stablecoins) but also other crypto assets, so long as the platform otherwise made clear how and when settlement becomes final.

Another hallmark of full stack trading experiences is access to credit to ensure and promote liquidity on the platform. Public policy should allow platform operators to facilitate the provisioning of credit to platform users so long as this service and function are well documented and explained to the supervisor and market participants on the platform. This is a clear example of where services previously provided by intermediaries can be solved by the trading venue itself.

Because crypto platforms have led the way in exchange innovation, public policy should anticipate that crypto firms will become more and more integrated with traditional payment rails and similar systems. Policy makers should consider whether and when to expressly delineate under what circumstances these platforms could access government-sponsored payment systems created for the settlement of securities, for example. Other policy initiatives will address whether and under what circumstances securities, including government-issued securities, can be reflected in tokenized form, but if such tokenization is permitted, an otherwise properly supervised platform operator should be allowed to access existing payment systems to facilitate settlement of such securities, even if interaction with that system is not on a real-time basis. Such a policy is recommended because otherwise access to this payment system would involve an intermediary, introducing various types of counterparty, operational, and credit risks to the platform that would not be in the interests of the participants on the platform (which itself would be highly supervised under our proposed framework).

Cross Margining and Risk Management

The regulatory framework for crypto should clearly allow for the cross-margining of both derivatives and spot positions on the platform with any and all assets permitted in the customer wallet and account, subject to appropriate risk weights and

haircuts, as applicable. For the settling and risk management of crypto asset transactions on a crypto platform, the settlement and risk systems are automated and the relevant software interacts with the wallet and account that contain customer assets.

A well-designed regulatory framework would allow a single platform to perform all risk functions, and require the appropriate standards on those functions. For example, in addition to the custody requirements mentioned above, the settlement and risk-management systems should be appropriately explained to the market supervisor through the platform's rule book, and the regulator should be made aware of major changes to the system.

Sound policy also should ensure that risk-management systems used by a platform operator are configured to prevent customer accounts from going net negative across positions. A risk-management system that effectively performs this function with this goal, including through liquidations of customer positions, should not be allowed to do so in an arbitrary manner. Instead, the rules, risk parameters and business logic that trigger any actions taken by the customer platform as it relates to customer assets should be clearly disclosed and appropriately explained to the supervisor as well as the platform users in the platform's rule book, which should be approved by the primary market supervisor.

In permissioning the use of a risk-management system for clearance and settlement, policy makers should take care to remain technology and methodology neutral, so long as the platform operator can effectively demonstrate its responsibilities can be adequately met.

5. Trading Platform Providers—Ensuring Regulatory and Market Reporting

Regulatory reporting of transactional activity should be required in order to provide market supervisors appropriate visibility into the trading platform, and to better allow supervisors to police for market manipulation and other unfair trade practices.

Policy makers should consider carefully how best to provide this data—a requirement should be considered that would mandate that trading platforms create an API for the beneficial use of market supervisors to directly ingest data from the platform itself, rather than require a separate entity to undertake reporting responsibilities.

With respect to market reporting, a hallmark of the crypto-asset industry (as previewed above) is the provisioning of market data to users free of charge. Policy makers should carefully consider the standards under which platforms are permitted to charge users a fee for the provisioning or use of market data related to trading that takes place on said platform along with the implications of that activity for market access, transparency, and fairness policy initiatives. The right standards could incentivize the platform operators to focus on risk management, user experience, and product innovation for competitive advantage rather than fees based on trading activity brought to the platform by the user.

6. Ensuring Customer Protections

As suggested, crypto-asset platforms have ushered in an evolution of market structure in favor of anon-intermediated model, where entities separate from the platform are not needed in order to access the platform and the trading environment.

In this market structure, however, key customer protections should remain in place. From a policy perspective, one approach could be a very general and non-prescriptive one that requires that platform providers or intermediaries develop and disclose policies and procedures to ensure the best interests of all customers are protected at all times, and leave it to the entity's discretion. This would allow investors to choose a platform provider based on the robustness of those policies and procedures.

If a more detailed or prescriptive approach is favored, such an approach should consider whether specific requirements related to practices impacting platform customers such as front-running trading activity, market manipulation, general risk disclosures related to the assets and instruments listed for trading, appropriate and non-misleading communications with customers, and avoidance of entering into conflicts of interest with customers. Again, appropriate customer-protection requirements can be borrowed from the traditional finance space—the key is to ensure that the platform provider can provide them rather than insisting that an intermediary perform the function. FTX believes that marketplace operators are properly positioned (perhaps best positioned) to deliver these types of disclosures and materials to users in a way that can be built directly into the trading venue user interface/user experience.

7. Ensuring Financial Responsibilities are Met

As with traditional markets, ensuring that customer assets are protected to the maximum extent possible should be a principle for regulating crypto-asset markets.

Again, the prominence of the wallet as a tool for storing assets is key to the crypto-asset space, and apart from requirements to ensure that the wallet itself is safely maintained and secured, policy makers should ensure that customers have access to real-time information about their account levels at all times (and redundant access paths, in the event of disruptions on one access path), particularly if and when a platform operator commingles customers' assets in an omnibus manner. If a platform provider elects to provide this infrastructure, operational complexity can be substantially reduced while customer assets are meaningfully protected.

In the case of a platform operator or an intermediary, policy makers should consider whether to adopt a minimum capital requirement (or other financial wherewithal condition) to ensure there are adequate resources to address operational and other types of risks that could jeopardize customer assets in custody. For platform operators, this could take the form of ensuring operational resiliency but in addition also ensuring adequate resources to address defaults and liquidations performed by a risk-management system (see above discussion on platform risk management). The goal should be to ensure platform operators need not depend on off-platform resources for settlement and risk management.

With respect to margining customer accounts, there should be a policy that expressly allows portfolio margining of all customer positions in all assets on the platform. This risk-management approach promotes capital efficiency and reduces operational risks to the platform or intermediary managing the customer account.

8. Ensuring Stablecoins Used on Platform Meet Appropriate Standards

A platform operator that permits the use of stablecoins for settlement of transactions should be required to explain the standards the platform operator uses in deciding which stablecoins it permits for such purposes. FTX has articulated and explained its policy recommendations for stablecoin issuers (*see https://blog.ftx.com/policy/context-stablecoin-regulation/*).

The reason such a policy is recommended is that stablecoins are exposed to reserve-volatility as well as redemption risk, and platform users should be entitled to some understanding of whether and to what extent those risks could impact their activity on the platform, including their impact on settlement of transactions (which might not be direct, but nonetheless indirect).

For example, a stablecoin backed by risky and volatile assets and not transparently backed by an adequate amount of such assets with appropriate haircuts, could become exposed to price risk. This price risk could interfere with settlement finality on the platform, insofar as the value of the stablecoin delivered as payment for the crypto assets in a transaction on the platform are suddenly not equal. Ensuring that stablecoins allowed for use on the platform meet adequate standards set by the platform operator (or by public policy makers if applicable) mitigates this risk, and should better protect the users of the platform.

9. Full-Stack Infrastructure Providers—Ensuring Appropriate Cybersecurity Safeguards are Kept

Market regulators in recent years have developed comprehensive cybersecurity requirements for market infrastructure providers. Policy makers should either apply the relevant safeguards already in place for exchanges, or otherwise require that the platform provider develop and disclose to market participants its policies and procedures regarding cybersecurity safeguards. In the case of platform operators already licensed by a market regulator, system-safeguard requirements already will be in place. In the case of platform operators not already licensed, one consideration for policy makers is to adopt a policy that helps facilitate standardization of these safeguards domestically as well as globally.

10. Full-Stack Infrastructure Providers—Ensuring Anti-Money Laundering and Know Your Customer Compliance

Platform operators must perform appropriate KYC as part of user onboarding and must conduct regular anti-money laundering surveillance of user activity (both on the trading venue and via the scrutiny of related on-chain transfers in and withdrawals out). Many platforms, including FTX, use a combination of vendors and internal compliance personnel to assist with these functions today. However accomplished, it is critical that crypto marketplace regulation continues to require significant focus on the performance of KYC and AML obligations. To ensure this, marketplace operators should be performing periodic self-audits and should also be subject to regular review and exam by their primary regulator on these requirements.

EXHIBIT D

FTX's Key Principles for Ensuring Investor Protections on Digital-Asset Platforms

Introduction

FTX strongly believes that ensuring investor protections is critical to the successful operations of digital-asset platforms, including our own, as well as to ensuring a positive user experience for our customers. FTX also believes that non-intermediated "direct access" markets, such as the FTX exchanges, can and do provide a level of investor protection that meets and exceeds the policy goals and purposes of traditional investor protection regulation (notwithstanding the absence of an intermediary or "broker"). Technology continues to displace the need for an investor to rely on intermediaries and brokers to access certain markets or asset classes, and one of the most important innovations of the digital-asset industry is a simplified market structure that does not need to rely on intermediaries for access to markets. From this observation, this paper addresses the key investor protection principles (described below) applicable to any market and the ways in which non-intermediated "direct access" digital-asset platforms can and do provide these protections for their users.

The goal of this paper is to support two critical propositions:

- The investor protection principles we describe in this paper can be provided directly by a digital-asset exchange or platform, using a non-intermediated market model, at an effectiveness level that exceeds relying on a series of intermediaries to provide similar protections and that ultimately leads to what FTX believes will be an overall risk-reducing market structure, for the benefit of investors.
- To the extent that legacy regulations or policies would assume or require an intermediary to provide these protections, we believe that approach often imposes unnecessary burdens and costs (including fees and both capital and operational inefficiency) on investors and markets without any corresponding benefit—and any such rules should be updated and modernized.

If market structure policy is truly to be technology neutral (which is an important and often stated principle expressed by policy makers), market regulators must acknowledge that intermediated market structures are due, in many instances, to the fact that technology was less robust when those markets were first developed. While intermediaries previously were helpful because the cost and complexity of accessing (1) a market for trading assets or (2) the assets themselves (especially when securities, for example, were in material or paper form) were substantial enough that it was economically efficient for an investor, especially an individual investor, to rely on an intermediary to provide such access and attendant services. However, intermediated market access is **not** an *a priori* first principle of market structure design, and technology has meaningfully changed what is possible.

Today, the only tools necessary to access a centralized marketplace for assets directly are (1) a computer or mobile device; (2) relevant "trading" software accessible on that hardware; (3) access to broadband services to transfer data over the internet, and (4) an application programming interface (API) to allow the trading software to be built and integrate with the trading platform's software. As a result, while investors might elect to use intermediaries for various reasons, those intermediaries are no longer indispensable for gaining access to financial products if the investor has the aforementioned tools.

We believe this has led to the possibility of the reduction of many types of risks, as explained in ***FTX's Key Principles for Market Regulation of Crypto-Trading Platforms*** (hereinafter "***Market Regulation Key Principles***"; *see https://www.ftxpolicy.com/*). Combined with other best practices and enhanced risk-management techniques utilized by FTX, this simplified market structure forms the basis for our argument that a well-designed and operated non-intermediated "direct access" digital-asset platform can be ***risk reducing*** relative to traditional market infrastructure. Building on FTX's ***Market Regulation Key Principles,*** this paper continues the discussion about critical investor protections and our view that platform operators should be allowed to provide these protections, and be held accountable for them, rather than insisting that they be fulfilled by intermediaries on the platform.

While not the core goal of this paper, we also note that intermediation can reduce transparency and information available to the customer. Traditionally, most users are not given full market data; neither are they allowed full access to exchanges,

preventing equitable access. FTX's disintermediated structure ensures that all users have equal access to its information and markets.

Key Investor-Protection Principles

Ultimately, all policies affecting the operation of a digital-asset market ensure the protection of the investor on the platform, and FTX's ***Market Regulation Key Principles*** paper addresses those.[18] Here we focus on specific principles related to the core of protecting customers' interests and their assets kept on a digital-asset platform. These include (1) maintaining adequate liquid resources to ensure the platform can return the customer's assets upon request; (2) ensuring the environment where customer assets are custodied, including digital wallets, is kept secure; (3) ensuring appropriate bookkeeping or ledgering of assets and disclosures to protect against misuse or misallocation of customer assets; (4) ensuring appropriate management of risks including market, credit/counterparty, and operational risks; and (5) avoiding or managing conflicts of interest. Each of these is addressed in turn.

1. Maintaining Adequate Resources to Return a Customer's Assets

A hallmark of the investor-protection regimes for markets globally and in the U.S. are requirements to ensure that the intermediary holding a customer's assets has adequate liquid resources available at all times to ensure that the customer can redeem her assets when she chooses. Often these policies are designed to ensure that there is (1) ***no delay*** in returning customer securities upon request, or (2) ***no shortfall,*** where an amount lesser than the value of the customer's assets can be returned to the customer.[19] This principle often involves other restrictions on the custodian, including, for example, a restriction of the use of customer assets to finance other business expenses or initiatives.[20] To ensure adequate liquid assets, familiar policies require a reserve of funds or qualified securities that is at least equal in value to the net cash owed to customers.[21] U.S. derivatives policy is very similar and also requires a cushion of resources to be held by the entity managing a customer's derivatives positions to ensure timely return of customer assets.[22]

FTX recommends policy makers consider a policy embodying this principle for digital-asset platform operators: fashioning a requirement, to be reflected in the platform's policies and procedures or otherwise, where the platform operator is accountable for keeping adequate liquid resources to ensure it can deliver customer assets back to the customer upon their request. This principle is sound for all asset types, and while the policy today tends to fall on intermediaries, it can just as easily be applied to the platform operator; in general, it should apply to whichever entity is custodying customer assets. Such a policy as applied to digital-asset platform operators would be independent of other requirements to ensure adequate capital to cushion losses (see discussion below).

To the extent existing regulations have implemented this principle by fashioning restrictions on intermediaries, most market supervisors—including those in the U.S.—have other authorities that would permit appropriate or conditional application of such a duty on a market operator. The fact that customer assets include digital assets and tokens in principle need not alter the basic policy of ensuring there is the availability of liquid assets.

FTX has policies and procedures for its platforms today that reflect this basic principle by maintaining liquid assets for customers withdrawals, including a sufficient balance of digital assets funded by the company for its non-U.S. platform. The resources are funded to provide sufficient cover against user losses under certain events and extreme scenarios in order to, among other purposes, ensure a customer without losses can redeem its assets from the platform on demand.

---

[18] *See https://www.ftxpolicy.com/*.

[19] *See, e.g.,* SEC Rule 15c3–1, Rule 15c3–3 Adopting Release, Exch. Rel. No. 9775, 1972 WL 125434, at *1 (Sept. 14, 1972). *See also* FINRA Rule 2150.

[20] *Id.*

[21] The amount of net cash owed to customers is computed pursuant to a formula provided by the rule. While the formula itself is somewhat complex, it embodies a basic concept for the responsible stewardship of customer cash: if a broker-dealer owes more to its customers than its customers owe to it, the broker-dealer must set aside at least an amount equal to that difference so that it is readily available to repay customers. *See also https://www.sec.gov/divisions/enforce/customer-protection-rule-initiative.shtml*.

[22] *See, e.g.,* CEA Sections 4d(a)(2), 4d(f), and 30.7. The CFTC's customer-protection rules for FCMs are very similar, and the rules embody, *inter alia,* the concepts of "segregation of customer assets" as well as "targeted residual interest," which like the SEC's requirements require that adequate resources provided by the FCM itself, in this case, are included in the customer's segregated account to ensure there is efficient and adequate return of customer assets upon request.

2. Securing Environment Where Customer Assets Are Custodied

Another key customer-protection principle is making sure that the environment itself, where customer assets are kept, is safe and secure. Existing market regulation often looks to the requirements of other financial custodians and intermediaries that also custody assets as a proxy for safety and security. For example, U.S. policy has the concept of requiring the use of a "qualified custodian" for the custody of customer cash and securities,[23] which in many instances is another intermediary that is also supervised and otherwise equipped to ledger and track a specific customer's funds.[24] Interestingly, the CFTC explicitly recognizes that a clearinghouse is subject to sufficiently rigorous standards and supervision that it can be entrusted with safekeeping customer assets.[25] In any case, this principle mandates that appropriate arrangements to safeguard the clients' rights in client assets and minimize the risk of loss and misuse are in place, which can be accomplished by ensuring that the custodian of the assets maintains adequate levels of financial integrity, physical and cyber security, as well as transparency to customers about the locus and availability of their assets.[26]

Regarding a digital-asset platform operator, the assessment of whether the environment delivers on this principle is different from that for traditional assets because the ecosystem often involves traditional fiat currencies as well as digital assets and tokens related to public blockchains. For digital assets, the digital wallet is central to the custody arrangements. For fiat currency, FTX and other platform operators will necessarily rely on licensed banking institutions to custody a customer's fiat currency; for traditional, non-tokenized securities, the custody function will follow the lines of the traditional market structure, unless some exemption is provided to allow some other arrangement—in the U.S., for example, existing regulations would require that custody be performed by a licensed intermediary legally permitted to custody such securities. (It certainly would be interesting, however, for policy makers to consider permissioning platform operators with the proven resources to custody these assets as well—again, derivatives regulation allows clearinghouses to custody assets.)

For digital assets, however, where policy is much less developed, custody involves control of private keys to digital wallets, and physical security involves the safekeeping of those private keys. When digital assets are left in the custody of platform operators such as FTX, safekeeping private keys can be performed in-house by the platform operator, or by the platform operator contracting with a third-party (the platform operator would remain accountable for regulatory requirements under this arrangement). Notably, both approaches have been permitted by market regulators and embraced by market participants.

Multiple architectures exist for the storage of private keys, which can be accomplished through use of a "hot wallet," cold storage, multi-signature wallet, or even by a smart-contract wallet. To be sure, policy makers could decide if a particular approach should be allowed or prohibited based on a particular policy emphasis—each approach has tradeoffs related to security and efficiency—but at this time, the best policy approach is likely allowing market participants to decide their preferred custody approach by electing to transact with the platform operator that offers it. This approach necessarily would require that a platform operator adequately disclose its wallet architecture and security practices. In any case, limiting access to the private keys under custody through appropriate permissioning, and ensuring adequate cyber-security protections, are critical to discharging this principle regarding securing the environment where assets are kept.

Some have suggested that allowing the platform operator to serve as the digital-asset custodian might present a conflict of interest for the platform operator, presenting more opportunities for misuse or misallocation of customer assets. It is far from clear to FTX that contracting with a third party for custody would in every instance lower the risks of misuse or misallocation of a customer asset, particularly when the platform operator would presumably remain accountable and, indeed, liable in every case; and each additional party added to a customer's experience adds

---

[23] Under the SEC's framework, "qualified custodians" typically include banks, broker-dealers, and futures commission merchants. *See* SEC Rule 206(4)–2(c)(3).

[24] *See, e.g.,* Securities Exchange Act of 1934 Rule 15c3–3. The CFTC's rules mandate that customer assets held at an FCM be segregated and clearly identified as customer assets, and be custodied by a bank or trust company, a registered clearing house, or another FCM. *See* CEA Sections 4d(a) and 4d(b) and CFTC Regulation 1.11.

[25] In the United States, some CFTC regulated clearinghouses already have direct clearing relationships with traders and are therefore holding customer funds without using intermediaries.

[26] *See IOSCO Final Report on Recommendations Regarding the Protection of Client Assets* ("IOSCO—Protection of Assets"), Principle 3 (Jan. 2014) *http://www.iosco.org/library/pubdocs/pdf/IOSCOPD436.pdf.*

another potential point of failure. We believe that rather than focus on any perceived conflict, policy makers should instead focus on the first principles described above for asset safekeeping (*i.e.,* regular auditing of the cybersecurity aspects of the custody plan along with auditing the actual assets held in custody), and perhaps consider requiring the platform operator to disclose any remaining potential conflicts while developing policies and procedures to address them.

FTX uses both approaches, using a third-party custodian in part for the U.S. derivatives platform and a proprietary in-house custody solution for the other platforms. For its in-house wallet solution and to maximize security, FTX leverages best-practice, hot- and cold-wallet standards whereby only a small proportion of assets held are exposed to the internet and the rest are stored offline. FTX policies and procedures also address and dictate other key components to the security of private keys, including applicable multi-signature arrangements, as well as the storage of relevant backup information. FTX's custody solutions comply with all relevant regulations, including those of the U.S. CFTC, and the company takes pride in the confidence in our security measures our customers have given to us.

3. Ensuring Appropriate Ledgering and Disclosures of Assets to Protect Against Misuse

Another key investor-protection principle is making sure there is adequate bookkeeping (and related records) to track the customer's assets, combined with appropriate disclosure and reporting.[27] This is to ensure that whoever is in control of a customer's assets is not misallocating or misusing those assets, particularly in furtherance to their own purposes at the expense of the customer's best interests. The basic concept here is that there should be controls in place to ensure the custodian has books and records that keep track of and identify which customer owns what, and there is adequate regulatory and customer reporting, as well as independent auditing, to verify the same.

In keeping with this principle, FTX provides a user experience that enables any user to easily view account balances for all assets, for all of its platforms, in real time. By logging in to the customer's account at FTX, the customer can immediately view the types of assets they own held in custody by FTX. The assets are ledgered and easily identifiable to the user (but held in an omnibus wallet in the case of the customer's tokens in order to better promote liquidity on the platform) pursuant to internal policies and procedures, and FTX regularly reconciles customers' trading balances against cash and digital assets held by FTX. Additionally, as a general principle FTX segregates customer assets from its own assets across our platforms.

Relatedly, and previewing the risk management discussion below, FTX ensures redundancy, resiliency, and disaster-recovery preparedness by using multiple geographically dispersed cloud and data service vendors and facilities to ensure industry-leading 24/7 service.

4. Conducting Adequate Risk Management to Protect Digital Assets

The next key principle is ensuring that any market participant in possession of customer assets is performing adequate risk management to protect those assets, regardless of their particular role in the ecosystem. There are multiple types of relevant risks that are inherent to any market structure, including but not limited to credit or counterparty risk, market risk, funding liquidity risk, and operational risk. (All of these in turn have a bearing on or contribute to systemic risk within the overall ecosystem.)

Credit and counterparty risk refers to the risk that a counterparty will fail to perform its obligations. Market risk is defined as the potential for losses arising from the change in value of an asset. Liquidity risk is the potential that a position in an asset cannot be unwound due to a lack of depth or a disruption in the market for the asset. Operational risk includes a risk of loss from a failure of internal processes at an organization, which can be caused by human error, technology-system breakdowns, or communication-network failures; they also can include losses caused by external factors such as "acts of God" or other naturally occurring events.[28]

Market participants in any market, including digital-asset market operators, must address each of these risks to ensure against substantial or catastrophic losses that could lead to existential threats against their own firm, thereby imperiling the assets of their customers. In general, policy makers that develop market regulation

---

[27] *See IOSCO—Protection of Assets,* Principles 1 through 3.

[28] For source of definitions, s*ee The Joint Forum of the Basel Committee on Banking Supervision, the International Organization of Securities Commissions, and the International Association of Insurance Supervisors, Risk Management Practices and Regulatory Capital,* November 2001, p. 15, at *https://www.iosco.org/library/pubdocs/pdf/IOSCOPD122.pdf.*

have required that both market operators as well as intermediaries manage risk by developing appropriate policies and procedures to address them, which contemplate the use of quantitative methods to measure risk, pricing products according to their risks, establishing risk limits, active management of risks through hedging and other techniques, and the building of cushions to absorb losses.[29]

FTX is a full-stack infrastructure provider, combining the matching engine and the clearing function on the same platform, providing a unified user experience for the trading of assets as well as the clearing and settlement of those assets. FTX's ***Market Regulation Key Principles*** addressed other risk-management considerations for the trading venue itself, but here we focus particularly on risk management embedded in the clearing and settlement functions that relate to investor protections.

Clearinghouses in traditional markets again are subjected to substantial regulatory rigor and are required to develop written policies, procedures, and controls that establish an appropriate risk-management framework which, at a minimum, clearly identifies and documents the range of the aforementioned risks and more to which the DCO is exposed, addresses the monitoring and management of the entirety of those risks, and provides a mechanism for internal audit.[30] Public policy typically provides clearinghouses discretion in setting, modeling, validating, reviewing and back-testing margin requirements that build the cushion to absorb potential losses, but must develop such requirements nonetheless; those models are then evaluated by appropriate regulators.[31] Clearinghouses are required by regulation to frequently check the adequacy of initial-margin requirements, value initial margin assets, back test products that are experiencing significant market volatility, and conduct stress tests with respect to each large trader who poses significant risk.

FTX platforms improve upon these requirements today in a number of material respects, and indeed the FTX US derivatives platform complies with the specific requirements of U.S. policy. First, the FTX international exchange imposes on its users a dynamic maximum leverage limit depending on their absolute position, which is limited to maximum leverage of 20 times the notional value of the user's account, and substantially lower in the case of larger positions. The limit is calculated as a function of market liquidity and volatility, along with the positions and collateral that the user holds. Second, FTX platforms check customer-account levels and asset amounts, including those used to collateralize positions, multiple times per minute as opposed to once per day, as standard policy requires today. Third, customer positions are liquidated if the net balance of all of a customer's positions becomes negative, or positions fall below the maintenance-margin threshold, and the FTX risk engine performs this function automatically. FTX uses an advanced and user-friendly liquidation process that gradually reduces a user's position to bring it to solvency, instead of closing the entire position. Fourth, FTX's risk-management program requires that digital-asset collateral be placed on the platform itself, rather than pledged but not delivered to the platform, to ensure the platform has immediate access to the collateral for purposes of managing market risks. And fifth, FTX's markets are open 24 hours a day, 7 days a week, which protects against delayed management of customer positions or market conditions, and the consequent build-up of market risk.

FTX undertakes this risk-management program without any reliance on intermediaries, depending only on its own systems and personnel. Historically, in traditional market structures, intermediaries provided a first or outer layer of risk management, as the entity typically responsible for onboarding customers and maintaining the customer relationship, and thereby exposing that intermediary to all of the attendant risks from that relationship. Market operators and clearinghouses are beneath or within that outer layer and, as explained above, also engage in management of the risks outlined above.

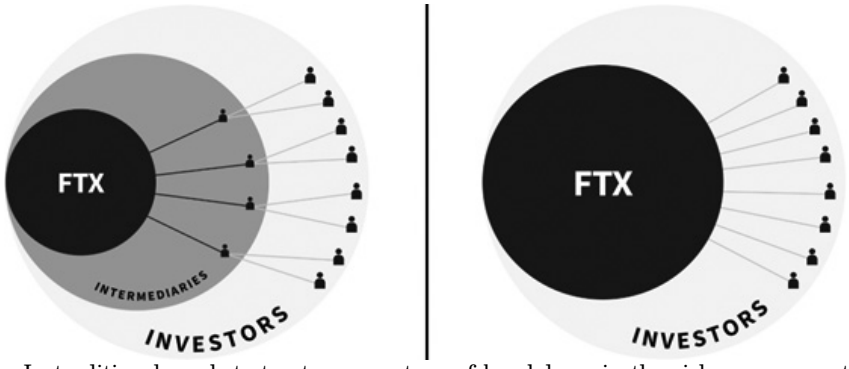
---

[29] *See id.*.

[30] *See, e.g., Derivatives Clearing Organization General Provisions and Core Principles ("DCO Final Rule"),* 76 FED. REG. 69334, 69335 (Nov. 8, 2011); *see also Standards for Risk Management and Operations of Clearing Agencies ("Clearing Agency Rule"),* SEC Rule 17Ad–22, 17 CFR Part 240.

[31] *See id.*.

Intermediated *versus* Non-Intermediated



In traditional market structure, any type of breakdown in the risk management at the *outer* layer of the intermediated market structure exposes the *inner* layer to consequent risks. This is so because those intermediaries are members of the trading platform as well, and the effects of a risk-management breakdown can be transferred to the trading platform as well as to the other members of the trading platform. Policy makers refer to this concept as interconnection risk. Arguably, the existence of this outer layer created through intermediation increases the opportunities for risk-management failure because there are so many more points of potential lapses or failure. Many of these can be inconsequential to the overall ecosystem, but some or many can be consequential.

The simplified market structure native to the digital-asset ecosystem poses fewer interconnection risks within the system because the outer layer of participants is folded into the inner layer—investors access the digital-asset platform directly. Likewise, without intermediaries bringing their customers to the trading platform, the trading platform is not exposed to risk-management failures by an intermediary, and can focus instead on its own risk-management program. This in turn simplifies the role of the supervisory community overseeing such platforms, who by focusing on the risk management of the platform operator can dispense with concerns about the platform's members who are not intermediaries. Again, this concept is key to FTX's view that the market structure for our platforms is ***risk reducing*** compared to those found in traditional markets.

One corollary to this concept is that involving intermediaries in the market structure ***does not*** by definition lead to greater investor protections, as some have argued. Instead, greater protections would depend entirely on the risk-management resources and capabilities (operational and financial) of the intermediary and whether they are delivering on other key investor protections, which in part depends on the level of supervision of the intermediary *vis à vis* the level of supervision of the platform. As a general matter, the supervision of clearinghouses as it relates to risk management in particular is equal to or greater than that for intermediaries, with heightened financial integrity and reporting standards. And as explained above, FTX risk management is designed and has been implemented to improve upon those standards in multiple ways.

Fewer interconnections, combined with superior risk-management practices at the platform level, while delivering on core investor protections, leads to a superior and risk-reducing market structure that better protects investors.

5. Avoiding Conflicts of Interest

The final principle is that in order to ensure the investor's interests are protected, conflicts of interest between the investor and the entity offering the products should be eliminated, mitigated and/or managed appropriately. Once again, in traditional capital markets the policy focus has been on intermediaries who offer access to investment products or otherwise sell the products to their customers directly, and today there are considerable requirements directed at intermediaries. Although not all existing regulations related to conflicts will apply, to the extent that policy makers wish to apply the relevant measures to the digital-asset space, this could be accomplished rather smoothly by shifting the burden of those measures from intermediaries to the platform operator as needed.

Policy governing traditional markets generally takes two approaches to addressing conflicts of interest: expressly prohibiting certain types of conduct, and requiring

policies and procedures that involve affirmative steps to identify areas of risk for conflicts, and measures to mitigate or eliminate those conflicts. As an example of the former, most securities regimes, including in the U.S., expressly prohibit misstatements or misleading omissions of material facts, and fraudulent or manipulative acts and practices, related to the purchase or sale of investment products.[32]

An example of the latter approach is a "best interest" or "suitability" requirement for entities offering investment products to their customers, again typically intermediaries in the case of traditional markets. This type of policy seeks to discourage entities from offering or recommending products that the investor does not sufficiently understand or possess the resources to use properly.[33] Other regimes are less prescriptive and generally focus on the financial wherewithal of a customer seeking access to a trading market, on the premise of ensuring creditworthiness and an ability to meet financial obligations on the platform,[34] along with risk-related disclosures.[35]

FTX favors an approach that provides equal access to all investors, and follows sufficiently robust listing standards that ensure adequate information about the listing is provided to the customer. But if policy makers preferred to impose a heightened standard more similar to what is found in securities markets, for example, they would need to impose that responsibility on the platform operator, which again could easily be accomplished.

In any case, whether intermediaries are involved in the market or not, conflicts inevitably arise when each actor is pursuing its commercial or economic interests. The key point for this particular principle is that when they do, there are familiar methods for eliminating or mitigating those conflicts, even as they apply to platform operators. FTX conducts its business with a goal of maximizing our customer's interest, but supports reasonable policy measures to eliminate or mitigate conflicts that impose those responsibilities directly on the platform.

SUBMITTED QUESTIONS

Response from Vincent "Vince" McGonagle, J.D., Director, Division of Market Oversight, Commodity Futures Trading Commission

Questions Submitted by Hon. Ann M. Kuster, a Representative in Congress from New Hampshire

Question 1. Director McGonagle, you mentioned in your testimony that since 2014 CFTC has brought more than 50 enforcement actions against digital asset markets for issues like fraud, manipulation, and false reporting.

Could you speak to how the investigation process works at CFTC, and do you feel there is more authority or support you need from Congress to strengthen CFTC's enforcement role?

Answer. The CFTC's Division of Enforcements ("DOE") receives information concerning possible enforcement matters from many different sources.[1] As part of DOE's process of assessing potential violations of the Commodity Exchange Act and CFTC regulations, DOE identifies: the necessary documents and information; the means available to obtain such documents and information (and the timing thereof); and any legal issues, including any statute of limitations issues. Generally, sources of information used by the CFTC to investigate include testimony and documents the CFTC may subpoena[2]* as well as books, records, and other information on the

---

[32] *See, e.g.,* Section 15(c) of the Exchange Act.

[33] *See, e.g.,* SEC Regulation Best Interest (BI), FINRA Rule 2111. This type of policy seeks to discourage entities from offering or recommending products that the investor does not sufficiently understand or possess the resources to use properly. To accomplish this, some policy regimes require the intermediary to collect relevant information about the customer/investor in order to ascertain the customer's investment profile, and then have policies and procedures for assessing suitability based on that information.

[34] *See, e.g.,* CFTC Rule 38.602, Rule 38.604, Rule 39.12, all of which speak to financial fitness and wherewithal.

[35] *See, e.g.,* CFTC Rule 1.55 and 33.7.

[1] These sources include customer complaints, market surveillance, Bank Secrecy Act Information, whistleblowers, self-reports, other Federal, state, or local government agencies, our self-regulatory organizations, such as the National Futures Association, designated contract markets, and swap execution facilities.

[2] The CFTC's power to subpoena testimony and documents in connection with its investigatory proceedings derives from Section 6(c)(5) of the CEA, 7 U.S.C. § 9(5).†

* **Editor's note:** footnotes annotated with † are retained in Committee file.

commodity interest-related activities that registrants, registered entities, and reportable traders are required to keep and make readily available to DOE.

For entities that only offer so-called "spot" digital commodity transactions, the CFTC does not have similar regulatory authority to require maintenance and production or inspection of required records. As a result, the CFTC must rely on voluntary cooperation and use its subpoena authority to obtain testimony, information and records relating to "spot" digital commodities. Thus, in order to strengthen the CFTC's enforcement tools with respect to enforcement against fraud and manipulative activity involving spot digital commodity transactions, the CFTC would need more authority and support from Congress, which have been thoughtfully provided in many of the proposed bills.

To that end, the CFTC continues to provide technical assistance to Members of Congress in support of a comprehensive Federal regulatory regime that, among other things, strengthens the CFTC's enforcement role with respect to spot digital commodity transactions.

Question 2. Director McGonagle, you also noted a number of recent cases involving retail fraud of digital assets and illegal off-exchange trading.

Could you elaborate on how these crimes work and what you all have identified as emerging trends in illicit activity related to digital assets that you are on the lookout for?

I know there has been a lot of focus lately on fully decentralized blockchains, where there is no central association acting as a supervisor, and as such there is also less trust between actors within that market.

Answer. Illicit activity in digital asset markets has become more sophisticated. One current trend DOE has observed is for bad actors to direct customers to transfer their own fiat currency into digital assets and then contribute those digital assets directly to the scheme. For example, a fraudster may ask a victim to open an account with a well-known cryptocurrency platform, convert his or her fiat currency into the platform to purchase digital assets, and then transfer those digital assets directly to the fraudster's digital asset wallet. Fraudsters then use a variety of tools and methods to move victim funds in ways that make it very difficult to track both the flow of funds and the identity of the responsible individuals, particularly because the fraudster's illicit activity rarely flows through a traditional bank account or an account hosted by a reputable platform that has a robust customer identification program or know-your-customer program.

Another common category of fraudulent and manipulative activity involving digital assets—known as the "rug pull"—typically involves enticing victims to purchase what is held out as a soon-to-be listed digital asset token by misrepresenting its potential value and failing to disclose the fraudsters' own interest. Then, after the digital asset's price increases, the fraudsters sell their holdings at the inflated price, abscond with the purchasers' funds, and disappear.

Additionally, DOE has observed the continuing trend of "pump and dump" activities where promoters of certain digital assets use social platforms to quickly and artificially "pump up" the value of a digital asset they hold and then sell off their (often undisclosed) ownership of those assets at increasingly higher prices, often with a correlating "dump" of the assets once their artificially inflated price becomes known.

Finally, traditional Ponzi schemes are common in digital asset fraud cases, where fraudster often promise large returns to be derived from digital asset trading activity.

Question 3. Director McGonagle, could you talk about how you see consumer protections being enforced in decentralized environments like that, and as a precursor, what factors you believe are most critical to objectively determining when a digital asset or token is indeed "fully decentralized"?

Answer. From the CFTC's vantage point, we evaluate whether persons are engaged in activity that falls within the jurisdiction of the Commodity Exchange Act or CFTC regulations or are otherwise engaging in activity that violates those provisions (including our anti-fraud and anti-manipulation requirements).

Even under the CFTC's current limited jurisdiction over the digital commodity markets, the CFTC has been committed to protecting customers. For example, the Commission recently filed an enforcement action against a decentralized autonomous organization, for illegally offering leveraged and margined retail commodity transactions in digital assets; engaging in activities only registered futures commission merchants ("FCMs") (which are subject to various customer protection require-

ments) can perform; and failing to adopt a customer identification program as part of a Bank Secrecy Act compliance program, as required of FCMs.[3]

However, to best address consumer and investor protections, digital asset spot markets must be subject to a comprehensive Federal regulatory regime similar to those financial markets currently regulated by the CFTC. By way of example, in the futures markets that are currently under CFTC jurisdiction, the Commodity Exchange Act provides for a regulatory framework that applies to any trading facility that lists and offers futures contracts for trading to retail customers on commodities, including futures contracts on digital assets. Under this framework, the trading facility must apply to the CFTC to be designated as a contract market and then comply with 23 statutory core principles. Those core principles require the designated contract market ("DCM") to, among other things: ensure the protection of customer funds;[4] protect market participants and the markets from abusive practices;[5] and promote fair and equitable trading in the DCM.[6] Furthermore, the core principles also require that the DCM: only list products for trading that are not readily susceptible to manipulation;[7] be able to detect and prevent manipulation, price distortion, and disruption of the contract's settlement process;[8] and establish system safeguards, which include cybersecurity protections and disaster recovery.[9]

In addition, under the current regulatory regime for futures markets, DCMs also have the responsibility, on a self-regulatory basis, to make sure their market participants are complying with the rules.[10] Additionally, the CFTC has broad enforcement authority to make sure those market participants comply with the Commodity Exchange Act and CFTC regulations.

The Commodity Exchange Act and CFTC regulations also provide for a system of intermediary oversight that focuses on retail market participants, which includes a disclosure regime that ensures those market participants are informed of the risks of trading strategies and fees involved for their trades.[11] These market participants are also informed of how their funds are being segregated and protected in the event of bankruptcy, as well as how such funds may be utilized.[12]

The CFTC would be well positioned to adopt a similar regulatory framework for spot digital commodity markets if Congress were to direct the CFTC to do so.

Questions Submitted by Hon. Stacey E. Plaskett, a Delegate in Congress from Virgin Islands

Question 1. Some observers have questioned how consumer protections will be enforced against a fully decentralized blockchain.

Do you believe adequate consumer protections could be achieved by regulating the exchanges and platforms on which most digital assets are bought and sold under the Commodity Exchange Act?

Answer. Yes. By way of example, in the futures markets that are currently under CFTC jurisdiction, the Commodity Exchange Act provides for a regulatory framework that applies to any trading facility that lists and offers futures contracts for trading to retail customers on commodities, including futures contracts on digital assets. Under this framework, the trading facility must apply to the CFTC to be designated as a contract market and then comply with 23 statutory core principles. Those core principles require the designated contract market ("DCM") to, among other things: ensure the protection of customer funds;[13] protect market participants and the markets from abusive practices;[14] and promote fair and equitable trading in the DCM.[15] Furthermore, the core principles also require that the DCM: only list products for trading that are not readily susceptible to manipulation;[16] be able to detect and prevent manipulation, price distortion, and disruption of the contract's

---

[3] *CFTC Imposes $250,000 Penalty Against bZeroX, LLC and Its Founders and Charges Successor Ooki DAO for Offering Illegal, Off-Exchange Digital-Asset Trading, Registration Violations, and Failing to Comply with Bank Secrecy Act,*† available at *https://www.cftc.gov/PressRoom/PressReleases/8590-22*.

[4] 7 U.S.C. § 7(d)(11).†

[5] 7 U.S.C. § 7(d)(12).†

[6] *Id.*

[7] U.S.C. § 7(d)(3).†

[8] 7 U.S.C. § 7(d)(4).†

[9] 7 U.S.C. § 7(d)(20) and 17 CFR § 38.1051.†

[10] 7 U.S.C. § 7(d)(2).†

[11] *E.g.,* 17 CFR § 4.24 and 4.34.†

[12] *E.g.,* 17 CFR § 1.55.†

[13] 7 U.S.C. § 7(d)(11).†

[14] 7 U.S.C. § 7(d)(12).†

[15] *Id.*

[16] 7 U.S.C. § 7(d)(3).†

settlement process;[17] and establish system safeguards, which include cybersecurity protections and disaster recovery.[18]

In addition, under the current regulatory regime for futures markets, DCMs also have the responsibility, on a self-regulatory basis, to make sure their market participants are complying with the rules.[19] Additionally, the CFTC has broad enforcement authority to make sure those market participants comply with the Commodity Exchange Act and CFTC regulations.

The Commodity Exchange Act and CFTC regulations also provide for a system of intermediary oversight that focuses on retail market participants, which includes a disclosure regime that ensures those market participants are informed of the risks of trading strategies and fees involved for their trades.[20] These market participants are also informed of how their funds are being segregated and protected in the event of bankruptcy, as well as how such funds may be utilized.[21]

The CFTC would be well positioned to adopt a similar regulatory framework for spot digital commodity markets if Congress were to direct the CFTC to do so.

Question 2. Could regulation of platforms under the Commodity Exchange Act in this manner achieve price and volume transparency, order flow, segregation of client assets, bankruptcy protections, cybersecurity, and Know Your Customer and Anti-Money Laundering requirements?

Answer. Yes. The Commodity Exchange Act grants the CFTC the authority to address all of the topics identified in your question through our core principles framework applicable to designated contract markets today. For example, DCMs provide centralized marketplaces that provide market participants with price transparency and the ability to trade these products in a safe and secure manner, with their assets segregated[22] and with bankruptcy protections[23] built into the system. There are also cybersecurity,[24] know-your-customer,[25] and anti-money laundering requirements[26] built into this regulatory framework. The CFTC would be well positioned to oversee spot platforms through a similar regulatory framework and achieve similar protections if Congress were to direct the CFTC to do so.

Question 3. What other protections could Commodity Exchange Act "principles based" regulation provide?

Answer. The CFTC is considered a principles-based regulator that issues prescriptive rules, when appropriate, in implementing the Commodity Exchange Act. For example, the Commission has issued rules that elaborate on the core principles applicable to DCMs,[27] as well as rules that mandate disclosures that commodity pool operators and commodity trading advisors must make to their retail participants and customers, respectively, which include, among other things, information about past performance, conflicts of interest, and risk factors.[28]

Ultimately, the type of regulatory regime provided in the Commodity Exchange Act will enable the CFTC to implement effective customer protections, while ensuring that the digital asset markets can continue to innovate in a responsible manner.

○

[17] 7 U.S.C. § 7(d)(4).†
[18] 7 U.S.C. § 7(d)(20) and 17 CFR § 38.1051.†
[19] 7 U.S.C. § 7(d)(2).†
[20] *E.g.,* 17 CFR § 4.24 and 4.34.†
[21] *E.g.,* 17 CFR § 1.55.†
[22] *E.g.,* 7 U.S.C. § 6d(a)(2).†
[23] *See* 17 CFR Part 190.†
[24] 7 U.S.C. § 7(d)(20) and 17 CFR § 38.1051.†
[25] 17 CFR § 42.2.†
[26] *Id.*
[27] *See* 17 CFR § 38.150–160.†
[28] 17 CFR § 4.24 and 4.34.†