



WHARTON BLOCKCHAIN
AND DIGITAL ASSET PROJECT

Finding Common Ground

*Navigating Tornadoes, Algorithmic Collapses,
And Novel Kinds of Organisms*

January 2023

The Eighth Reg@Tech Roundtable On Digital Assets

Foreword

At our biannual Reg@Tech roundtable, participants share their views on recent developments and discuss ongoing regulatory efforts. Reg@Tech 8, held October 7-8, 2022 in Philadelphia, followed an eventful period in the crypto world. Little did we know, however, that a month later, the crypto industry would experience one of its most dramatic meltdowns with FTX's collapse, substantially raising the profile of regulatory and other public policy debates.

A common phrase reiterated in blockchain communities is “do not trust, verify”. The reality, though, is more complicated. Policy-makers and regulators need to understand both the technology and the realities of the market. Although every Reg@Tech meeting is different, there are common threads throughout all our sessions since our first meeting in 2017. One of these, which we highlight in this report, is the surprisingly complex concept of decentralization.

At Reg@Tech, we build bridges among industry, academia, and government, facilitate important discussions, and develop pathways forward. Regulation and innovation need not be in conflict. Recent events show that these meetings to find common ground are more important than ever.

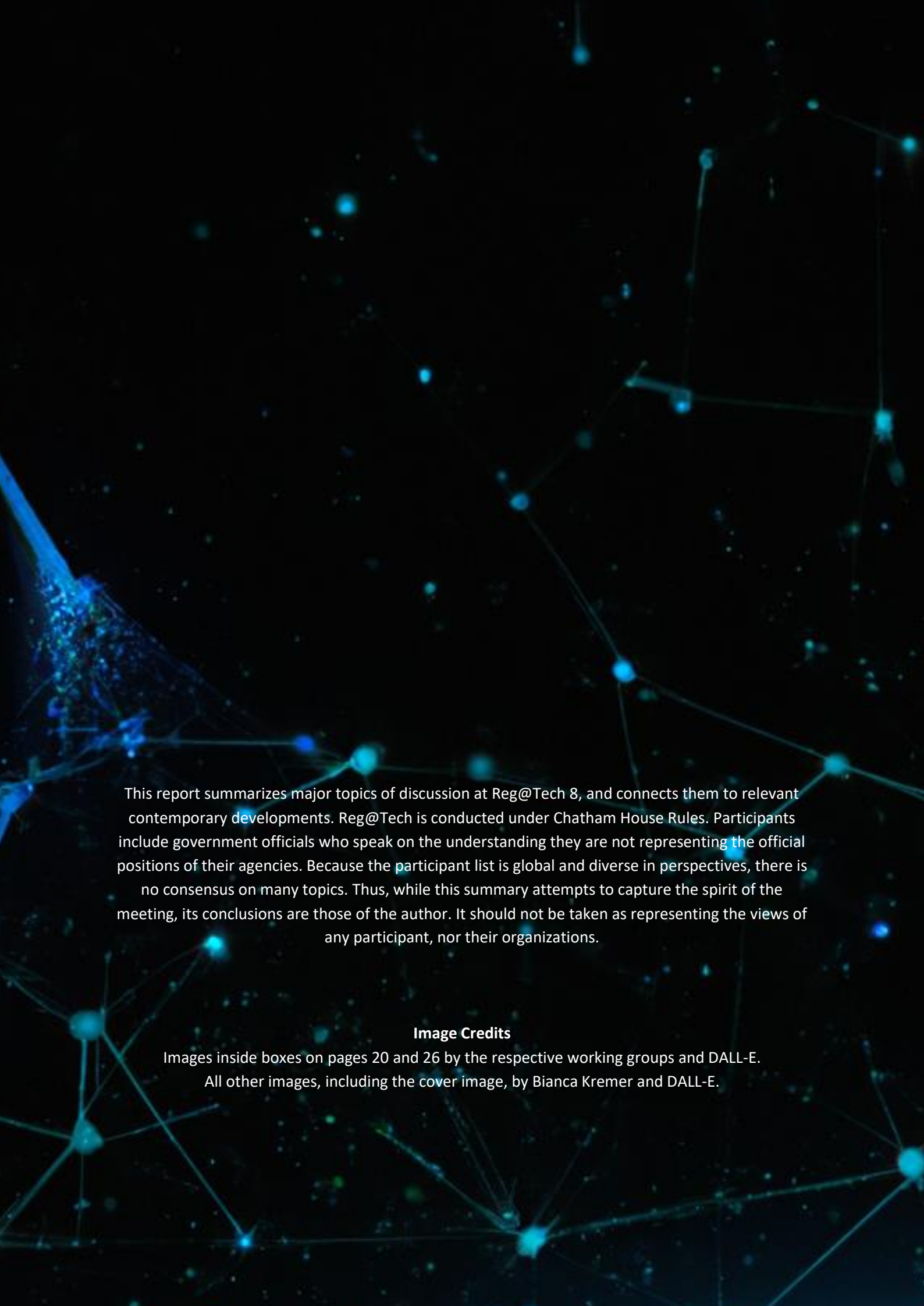


Kevin Werbach is the Liem Sioe Liong/First Pacific Company Professor, and Chair of the Department of Legal Studies & Business Ethics at The Wharton School, University of Pennsylvania. He is the director and founder of the Wharton Blockchain and Digital Asset Project. A world-renowned expert on emerging technology, he examines business and policy implications of developments such as broadband, big data, gamification, and blockchain.

werbach@wharton.upenn.edu

Table of Contents

INTRODUCTION	5
RECENT DEVELOPMENTS	6
BEYOND CENTRALIZED SERVICES: ADDRESSING AN EVER-CHANGING LANDSCAPE	8
From Earth to the Moon and Back: Extraordinary Rise and Spectacular Fall of Terra Luna	8
Targeting Who, Targeting What? Charges Against Ooki DAO	10
Stopping the Unstoppable: Inside the Eye of Tornado Cash	11
The Privacy Dilemma	12
Is Tornado Cash an Entity?	14
A Better Way Forward	16
To Decentralize, or not to Decentralize, that is the Question	21
EXPLORING POSSIBLE PATHWAYS FOR THE REGULATORY ENDGAME	23
Learn, Understand, and Use	24
The Fundamentals of the Technology	24
Categories of Crypto Assets	24
Courage to Experiment	25
Flexibility	25
Encourage Innovation	26
Recall Principles, Reinvent Methods	26
Consumer Protection Goal	26
Same Risks, Same Rules vs New Rules for New Tools	27
CONCLUSION	28



This report summarizes major topics of discussion at Reg@Tech 8, and connects them to relevant contemporary developments. Reg@Tech is conducted under Chatham House Rules. Participants include government officials who speak on the understanding they are not representing the official positions of their agencies. Because the participant list is global and diverse in perspectives, there is no consensus on many topics. Thus, while this summary attempts to capture the spirit of the meeting, its conclusions are those of the author. It should not be taken as representing the views of any participant, nor their organizations.

Image Credits

Images inside boxes on pages 20 and 26 by the respective working groups and DALL-E.
All other images, including the cover image, by Bianca Kremer and DALL-E.

Introduction

The topic of Reg@Tech 8 was “Digital Assets and Decentralized Systems”. Points in the agenda included the state of digital asset regulation, recent policy and near-term prospects around the world, as well as major events that happened since our last Reg@Tech meeting in March 2022.

We also looked forward, to what we termed, "The Regulatory Endgame." Participants discussed how public policy and regulation can be reconciled with ownerless, borderless, and unstoppable decentralized protocols. The notion of decentralization more specifically underlies many Reg@Tech discussions and was one of the major focal points in this roundtable. We considered such enduring concepts in light of contemporary events, such as the Terra Luna collapse,¹ the sanctioning of Tornado Cash,² and the CFTC’s penalty against Ooki DAO.³

Working Group Summaries

At Reg@Tech 8, participants were divided into four working groups, which focused on the following topics and questions:

- 1. Identity:** Many current regulatory issues for digital assets depend on representations of identity. Examples include AML/KYC, DeFi regulation, and treatment of DAOs. What are the options, technically and in policy design, for identifying relevant actors in ways that protect privacy yet facilitate appropriate (possibly embedded) supervision?
- 2. Global Implementation:** Digital assets are a global phenomenon being tackled by governments constrained by their specific jurisdictions. How can we design regulatory approaches, coordination mechanisms, and industry best practices that encourage a "race to the top" rather than regulatory arbitrage and uncertainty?
- 3. Non-Financial Regulation:** What legal or regulatory developments in areas such as consumer protection, intellectual property, speech, antitrust, contracts, insolvency, and ESG are important to the development of digital assets, with potential impacts on financial regulatory debates?
- 4. Institutional Design:** If there were no legal or political constraints, what would the attributes of an ideal digital asset regulator, resilient to the rapid technological change in this area, be?

Throughout this report, in boxes such as this one, we provide summaries of the ideas the working groups developed.

Recent Developments

Since the Biden Administration's Executive Order (EO) on Ensuring Responsible Development of Digital Assets was released in March 2022, agencies across the government prepared reports and policy recommendations. Significant progress has been made, such as the First-Ever Comprehensive Framework for Responsible Development of Digital Assets in the United States.⁴ Across the pond, an agreement has been reached on the Markets in Crypto-Assets regulation (MiCA) in the European Union.⁵

Among some other recent developments in discussion were the Basel Committee on Banking Supervision (BCBS)'s work to develop a framework on capital requirements for bank exposures to crypto assets. Recently, it published its second consultation on prudential treatment of crypto asset exposures.⁶ In other under-the-radar regulatory news, the United States Office of Government Ethics (OGE) issued a legal advisory on July 5, 2022 stating that government employees who hold any amount of cryptocurrency or stablecoin may not be involved in working on regulations and policies of such assets.⁷ Since the OGE's interpretation may have a massive systemic impact across every agency, it became one of the points of discussion. One participant sarcastically remarked that, "this is like saying that if you regulate a bank, you can't have a bank account".

In June 2022, the Financial Action Task Force (FATF) published a targeted update on the implementation of FATF standards on virtual assets (VAs) and virtual asset service providers (VASPs).⁸ Some noted that jurisdictions can have staggeringly different virtual asset service providers (VASPs) interpretations, which leads to regulatory arbitrage, depending on how the FATF wording is transposed into national legislation. A suggestion voiced was that regulatory arbitrage may be deliberate. Since the FATF guidance's release in 2018, only 43% of responding jurisdictions around the world have adopted a regulatory regime for licensing or registering VAs and VASPs. The remaining countries are taking longer than expected to implement the rules, which leads to the question of whether being the last to adopt such rules might actually constitute an advantage. From a US perspective, a participant questioned whether the FATF guidance matches US policy, which tends to be more focused on actual custody rather than a facilitator for Bank Secrecy Act purposes.

Regarding the present state of affairs, some participants argued that the existing regulatory regime for traditional financial services providers is far from perfect. Regulators should not take for granted that everything was fine before crypto came along. Tomicah Tillemann, for example, said that "spending \$30 billion dollars on an AML framework that has a 99% failure rate is far from optimal. In addition, between \$70 and \$400 billion are missing from the US government's pandemic relief funds because of failures in the present infrastructure. Millions of people in the US and billions around the world do not have access to financial services. Realizing that the *status quo* has profound deficiencies is the first step to then being able to work through these very substantial problems." Navigating novel problems in the digital asset space in addition to already existing ones in the traditional financial system, only adds complexity. For example, the May 2022 TerraUSD stablecoin crash resulted in a wave of insolvencies, which saw hundreds of billions of funds evaporate.

Working Group: Global Implementations

Regulation of digital assets is diverse globally. In a working group on this topic, participants delved into the issue of regulatory competition and examined ways for global activities to thrive. Six regulatory approaches were guiding elements in the discussion: financial inclusion, consumer protection, market integrity, cybersecurity, market competitiveness, AML and CFT.

Because digital assets can have various types of risks, this working group suggested that the principle of “same risks, same rules” should be changed to “same risks, same regulatory outcome”. Coordination and exchange of knowledge between jurisdictions were identified as particularly important actions, especially in creating standardized procedures and making them “passportable”. An idea this working group came up with was to have a “Ministry of the Future” in each jurisdiction that coordinates on these important global questions, and is in charge of promoting innovation, while overseeing the agencies and making sure that coordination happens.

Another one was to create a data rich privacy preserving environment for open source development and critical technology, especially around the following four areas:
(1) AI, (2) homomorphic encryption, (3) DLT, and
(4) federated learning.

This working group highlighted the need to implement processes to make demonstrable use cases available, and the usefulness of having solid data and demonstration around these use cases to give policymakers and regulators a more hands-on experience of where things are going and why these innovations are useful. Participants also debated on how to incentivize a race to the top rather than the lowest common denominator across countries.



Beyond Centralized Services: Addressing An Ever-Changing Landscape

**From Earth to the Moon and Back:
Extraordinary Rise and
Spectacular Fall of Terra Luna**

Terra LUNA

In 2018, South Korean software developer Do Kwon together with Daniel Shin co-founded the Terra network, launching the network's native token, LUNA a year later.⁹ Late 2020, Do Kwon announced the launch of TerraUSD (UST) and described it as "an algorithmic stablecoin, where the cost of minting is equal to the face value of the stablecoins minted — in order to mint 1 TerraUSD, only \$1 worth of the reserve asset (\$LUNA) must be burned. TerraUSD monetary policy is infinitely scalable — helping DeFi apps and protocols achieve their full potential without restrictions."¹⁰ By April 2022, it had become the third-largest stablecoin,¹¹ seeing its value rise to \$40 billion,¹² only to come tumbling down a month later in what would be considered the largest stablecoin failure in cryptocurrency history. In May 2022, UST lost its dollar peg and the Terra network went into a death spiral, along with a hyperinflation in the Luna token. \$40 billion evaporated and triggered a domino effect across the wider crypto ecosystem.

One participant described the Terra Luna incident as a "sonic boom across the regulatory space", which resulted in a "sigh of relief" from regulators internationally when it became obvious that the "interconnectedness within the crypto space did not bleed into the traditional financial institutions". It can thus be expected that there will not be unbounded willingness to let those interactions increase until there is some maturity. However, significant losses have still occurred, particularly because of the contagion effects of insolvencies throughout the industry. This includes several platforms that were interconnected in some way with Terra Luna, going into bankruptcy and suspending withdrawals. The list continues, while the domino effect is still being felt.

Participants pondered the learnings that could be derived from the Terra Luna collapse, a sort of "post mortem", and deliberated on what could have been done differently from a regulatory perspective or from an industry perspective. One participant criticized policymakers and regulators and argued that they were partly to blame because they had already identified the very risks people have lost money on years ago. It was thus argued that when risks are identified in a fast-moving sector, action must be taken immediately, otherwise, this could be interpreted as tantamount to a positive decision not to do anything at the moment, which costs people a fortune. There was general agreement that protections have to start being built into the technology.

The question arose whether regulators can incentivize the idea of in-built safety nets in such systems. In this context, discussions were held on the benefits of market-driven decisions. Market dynamics that create incentives for such protections are much

needed for digital assets to become real options. Only if this happens, can the industry truly grow.

VCs are investing substantial amounts into companies that are building out the trust layer, and the infrastructure in all kinds of ways. Some were of the opinion that in the long run, these systems will do much better than the existing banking system in mitigating risk.

Debates were held about what the role of developers and the founding teams should be. Some participants pointed out that while many projects claim to have decentralized governance, upon closer examination, this is not always the case. Taking Terra as an example, they argued that despite having open-source software, its centralized intermediaries were identifiable and could be held liable, thus failing to be truly decentralized.

The question then arose of how to better protect consumers and who should bear the responsibility when such massive failures happen. Some roundtable participants voiced their concern that regulators may start to use the idea of secondary liability. The worry expressed was that from a longer-term perspective, even if there is no primary liability in decentralized systems, the concept of secondary liability would be applied more aggressively for software development in the US.

Joshua Klayman noted that "although Terra Luna was a centralized situation, it cannot be totally decoupled from Decentralized Finance (DeFi) since the whole idea of stablecoins is to provide a foundation to incorporate some stability in an otherwise unstable and highly volatile market."

Targeting Who, Targeting What?

Charges Against Ooki DAO

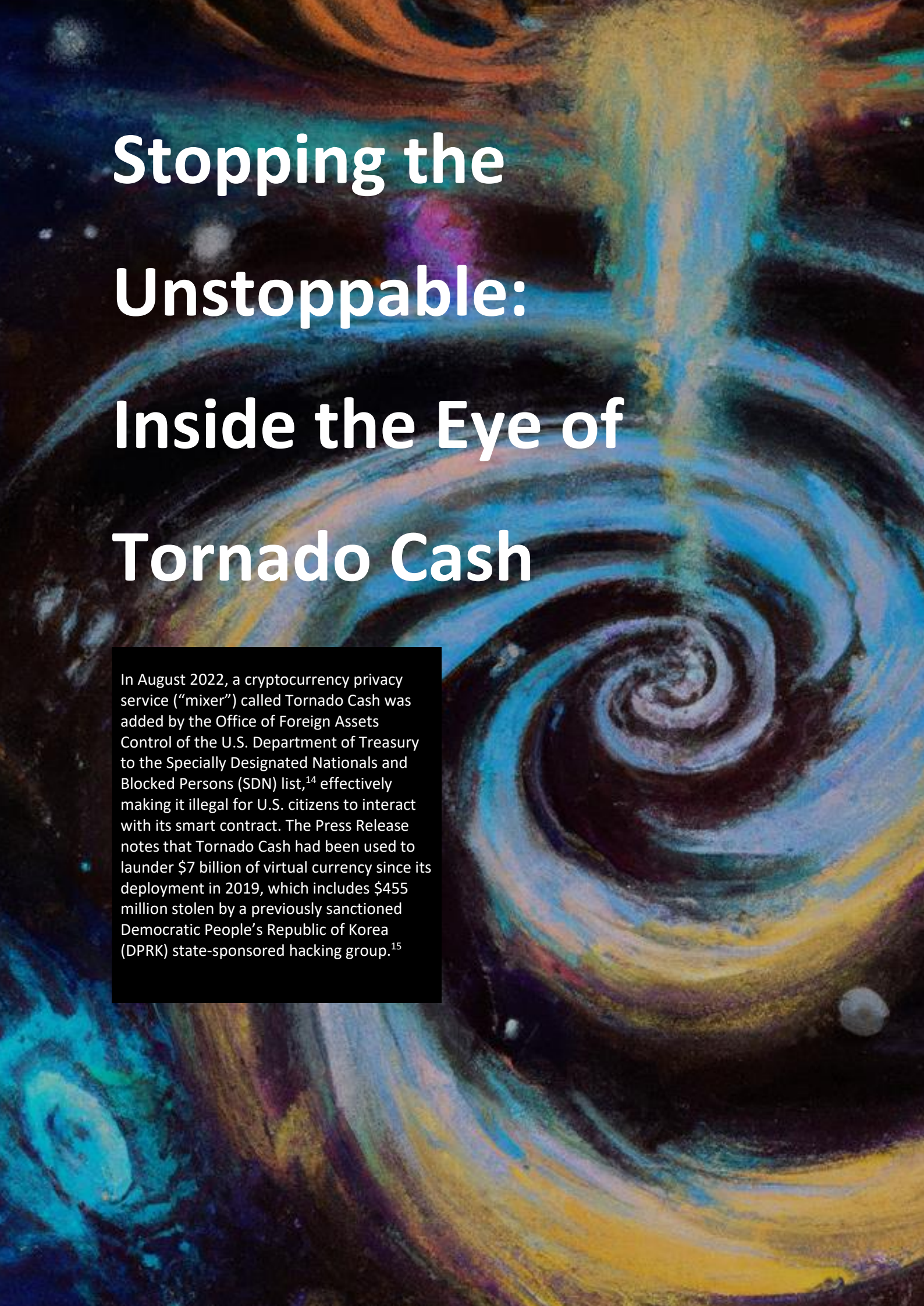
Ooki DAO

On September 22, 2022, the CFTC took action and settled charges against bZeroX, LLC (bZerox) and two of its co-founders, Tom Bean and Kyle Kistner, for illegally offering retail commodity transactions in digital assets in breach of the Commodity Exchange Act (CEA), the so-called bZx protocol, which functions like a trading platform. The bZx LLC entity settled the charges for \$250,000.¹³

The CFTC also filed suit against Ooki DAO for being the successor of bZeroX and operating the same bZx protocol in violation of the CEA, CFTC regulations and Bank Secrecy Act.

Aside the difficulty of determining responsibility in quasi decentralized systems, when DAOs get sued, this opens up a whole other complicated set of questions. Attention was drawn to the danger of not having a clear path for the decentralized ecosystem to enter the regulatory perimeter. In that vacuum, regulators are likely to use existing tools, existing legal theories, and existing regulatory structures to try to impose order on the ecosystem. Some thus voiced their opinion that the Ooki DAO case represents legal theories of how to impose centralized exchange requirements and centralized intermediary requirements on a decentralized protocol.





Stopping the Unstoppable: Inside the Eye of Tornado Cash

In August 2022, a cryptocurrency privacy service (“mixer”) called Tornado Cash was added by the Office of Foreign Assets Control of the U.S. Department of Treasury to the Specially Designated Nationals and Blocked Persons (SDN) list,¹⁴ effectively making it illegal for U.S. citizens to interact with its smart contract. The Press Release notes that Tornado Cash had been used to launder \$7 billion of virtual currency since its deployment in 2019, which includes \$455 million stolen by a previously sanctioned Democratic People’s Republic of Korea (DPRK) state-sponsored hacking group.¹⁵

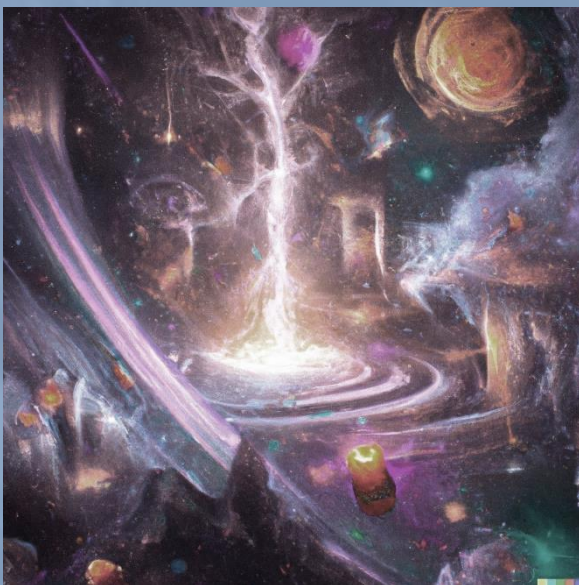
Tornado Cash is a crypto mixer that can obfuscate the origins of cryptocurrencies deposited into any of its pools once they are withdrawn. Fees are collected for the service of randomly shuffling and blending funds of users.¹⁶ The U.S. Treasury sanctioned Tornado Cash for its role in facilitating money laundering from several hacks, such as e.g., the hack on Axie Infinity's Ronin Bridge protocol, performed by a hacking group called Lazarus Group, which has ties to North Korea.¹⁷

Adding blockchain addresses to the SDN list is nothing new. In 2018, the Office of Foreign Assets Control (OFAC) added Bitcoin addresses for the first time to the SDN list, which belonged to two Iranians who were using ransomware to attack US infrastructure and collect bitcoin at those addresses.¹⁸ In May 2022, OFAC added blender.io, a custodial or centralized Bitcoin mixer, to the SDN list.¹⁹ Sanctions determinations in the US are done trying to avoid harming innocent people.

Coinbase and the crypto think tank Coin Center filed lawsuits against the Treasury Department and the OFAC, criticizing the sanctioning of an open-source software project.²⁰ Some participants debated the OFAC action on the basis that Tornado Cash is a piece of software. There was some confusion as to whether Tornado Cash was even a regulatable entity. The issues being raised here are not just issues in a blockchain context but concern autonomously functioning code more generally, i.e., code that human beings can't stop or change. There was a suggestion that we would be seeing more and more autonomous code in the world.


Autonomous code and immutable software that cybercriminals can abuse present new and difficult challenges. According to a Chainalysis report at least 25% of mixed cryptocurrencies originate from illicit addresses and hackers with connections to hostile governments are among those who benefit the most.²¹ However, Tornado Cash is used for a number of legitimate purposes as well, for example, by individuals who value their privacy, by famous people who want to make donations to political causes in a manner to avoid attracting publicity,²² and wealthy individuals who are concerned about their privacy and safety.²³

The Privacy Dilemma



Balancing privacy with national security is difficult. Some participants debated ways to support privacy, expressed their wish for more privacy, and their concern about continued privacy erosion.

Tomicah Tillemann explained that there are projects that exist on either extreme of the privacy continuum: "either there is total opacity or attempted total opacity, such as in the case of Tornado Cash, or on the other extreme, there is Bitcoin and Ethereum, which are totally transparent to anyone who has access to a sophisticated analytics package."



Tillemann further explained that "most do not want to operate at either end of that spectrum. Thus, there is an opportunity to create some third-party solutions that are a compromise between total opacity on the one hand and total transparency on the other." Some roundtable participants expressed the view that this is where the vast majority of consumers and commercial activity will end up taking place.

The technology is catching up and there is a lot of promising research in the area of zero-knowledge proofs being conducted. There are systems being built that offer interesting solutions that will provide the average user of these systems with a much higher degree of confidence that their information is being protected while still having some accountability assurance.

Some participants highlighted the need for constructive dialogue between the public and private sectors to demonstrate how these tools work, what the potential pathways are, and how to balance compliance and privacy. One example discussed was Tornado Cash's software-based compliance tool that generates a printable PDF to prove the source of funds. This method of selective disclosure allows individuals to re-identify themselves to an exchange and is also available in Zcash and Monero, which are privacy-preserving blockchains.

Such tools provide computational privacy in addition to asset transfer privacy. However, these compliance tools are not "the silver bullet solution". This solution does not enable the regulator to selectively disclose anyone's transactions in a top-down manner, the network just empowers individuals to have control over their own privacy. This means that if one goes to an individual who is not regulated, one may persuade them with a warrant or a subpoena to use their selective disclosure powers and share a public key in order to reveal the transactions.

A comparison that was drawn was that this was reminiscent of an era before transactions started happening through intermediaries, a time when people kept their records at home and the only way for authorities to have insight into cases such as criminal activity or fraud, was to get a warrant to search the premises and open the file cabinet and take the records.

The full transparency of Bitcoin and Ethereum was seen by some as a bug and not a feature. However, in privacy-preserving systems, selective disclosure and the ability to prove to a regulator that one has engaged in licit activity rather than illicit activity is a feature that can be harnessed. These systems can thus accommodate compliance and are not absolutely opaque.

Is Tornado Cash an Entity?

Some expressed their concern that there was a disconnect between industry and government, that nobody on either side really knows what was sanctioned, and that there is a lot of uncertainty and confusion.

It was thus suggested that the best way to address these problems in really meaningful ways is for the public sector and the private sector to sit in the same room and try to find solutions.

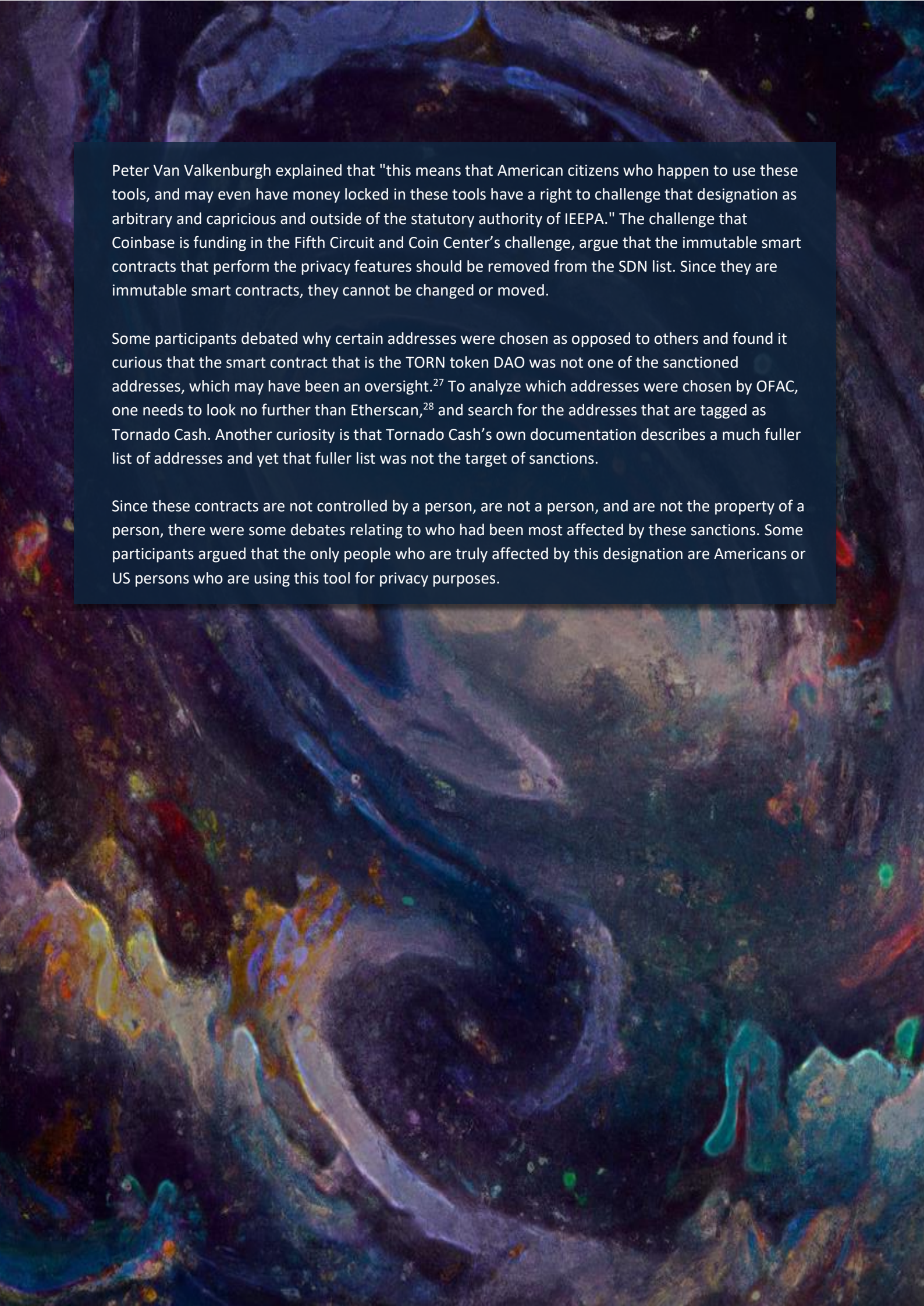
In the industry, Tornado Cash itself is largely not seen as an “entity”. Some questioned whether there was a lack of understanding at the OFAC in sanctioning these smart contract addresses.²⁴ Some participants asked whether that was done by mistake. In the sanctions list, the OFAC also refers to an “Organization Established Date 2019”,²⁵ which some participants pointed out as incorrect since there was no organization or software development company relating to Tornado Cash established in 2019.

Some participants urged that it is important to note that North Korea continues to pose a real security threat as it ramps up its ballistic missiles program and that the agencies are trying their best to mitigate those threats and solve these highly complex problems. Whether they did that in the right way here might be a completely different question. When it comes to security threats, the U.S. President has broad powers. The IEEPA (International Emergency Economic Powers Act, 50 U.S.C. 1701 et seq.) or the executive order,²⁶ which is based on IEEPA, gives the President broad authority, which ranges from banning TikTok to cutting off the Iranian oil energy sector. It even gives the President,

through the agencies, the ability to construct an executive order that allows an agency to sanction somebody just by virtue of the fact that they happen to be the family member of a bad actor.

During the discussions, the topic of responsibility, first addressed in the context of Terra Luna, emerged again. The question posed was: If DeFi is truly autonomous, should regulators meet in the middle and think about regulating the software code or still regulating the developer or the person behind it? In other words, how can our regulatory regime and our current legal system assign responsibilities regarding such software programs? Fundamentally, the law always seeks to place responsibility somewhere, on a legal entity, be it a person or a corporation. But in the case of Tornado Cash a software program is being sanctioned.

Nevertheless, it will still be necessary to identify the central person or the regulatory hooks that can be held responsible. Some then pondered the question of placing responsibility on the software developer, which others disagreed with, stating that to turn software developers into financial intermediaries would definitely stifle innovation, regardless of where in the world the software developers were located. Typically, the party that has been sanctioned has the capability to challenge the sanction and then go into discovery and litigation. The bizarre situation here is: who would be the person to do that? Normally the person would petition to be removed from the SDN list. However, in this case, there are no targeted persons.

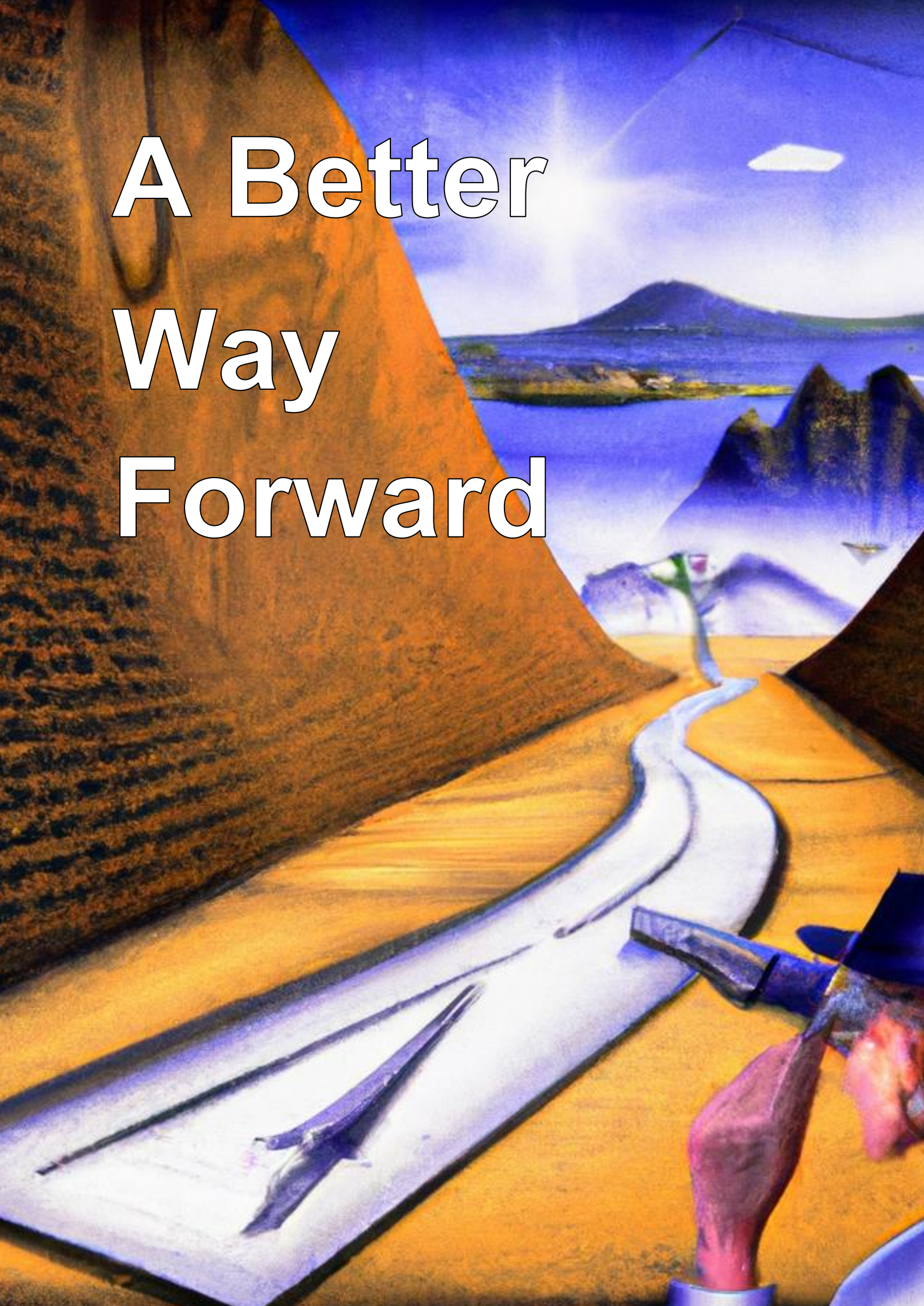


Peter Van Valkenburgh explained that "this means that American citizens who happen to use these tools, and may even have money locked in these tools have a right to challenge that designation as arbitrary and capricious and outside of the statutory authority of IEEPA." The challenge that Coinbase is funding in the Fifth Circuit and Coin Center's challenge, argue that the immutable smart contracts that perform the privacy features should be removed from the SDN list. Since they are immutable smart contracts, they cannot be changed or moved.

Some participants debated why certain addresses were chosen as opposed to others and found it curious that the smart contract that is the TORN token DAO was not one of the sanctioned addresses, which may have been an oversight.²⁷ To analyze which addresses were chosen by OFAC, one needs to look no further than Etherscan,²⁸ and search for the addresses that are tagged as Tornado Cash. Another curiosity is that Tornado Cash's own documentation describes a much fuller list of addresses and yet that fuller list was not the target of sanctions.

Since these contracts are not controlled by a person, are not a person, and are not the property of a person, there were some debates relating to who had been most affected by these sanctions. Some participants argued that the only people who are truly affected by this designation are Americans or US persons who are using this tool for privacy purposes.

A Better Way Forward



In the context of discussing the regulatory endgame, a question arose as to how agencies could have responded differently to Tornado Cash. While criticizing the approach that was taken in sanctioning Tornado Cash is easy, it is much harder to come up with an alternative solution in terms of national security concerns that could have the intended impact on North Korea.

When trying to implement a national security strategy, a holistic approach is generally strived for, which brings together different tools to get the ultimate desired impact, such as a change of behavior, deterrence, cutting off money from bad actors, etc. on the one hand. There are a lot of cyber risks and security risks, on the other hand. This needs to be solved and mitigated because North Korea should not be able to just hack a DeFi protocol or a bank, engage in trade-based money laundering or anything similar where they can get access to these funds. It was repeated time and time again throughout the roundtable discussions how important it is for regulatory agencies to engage in that conversation, do that analysis, understand the consequences, and understand the technology.

Among some of the ideas discussed in tackling this issue are employing blockchain analytics, setting standards, applying security audits, and increasing public-private sector collaboration, which will be addressed in turn.

Blockchain Analytics

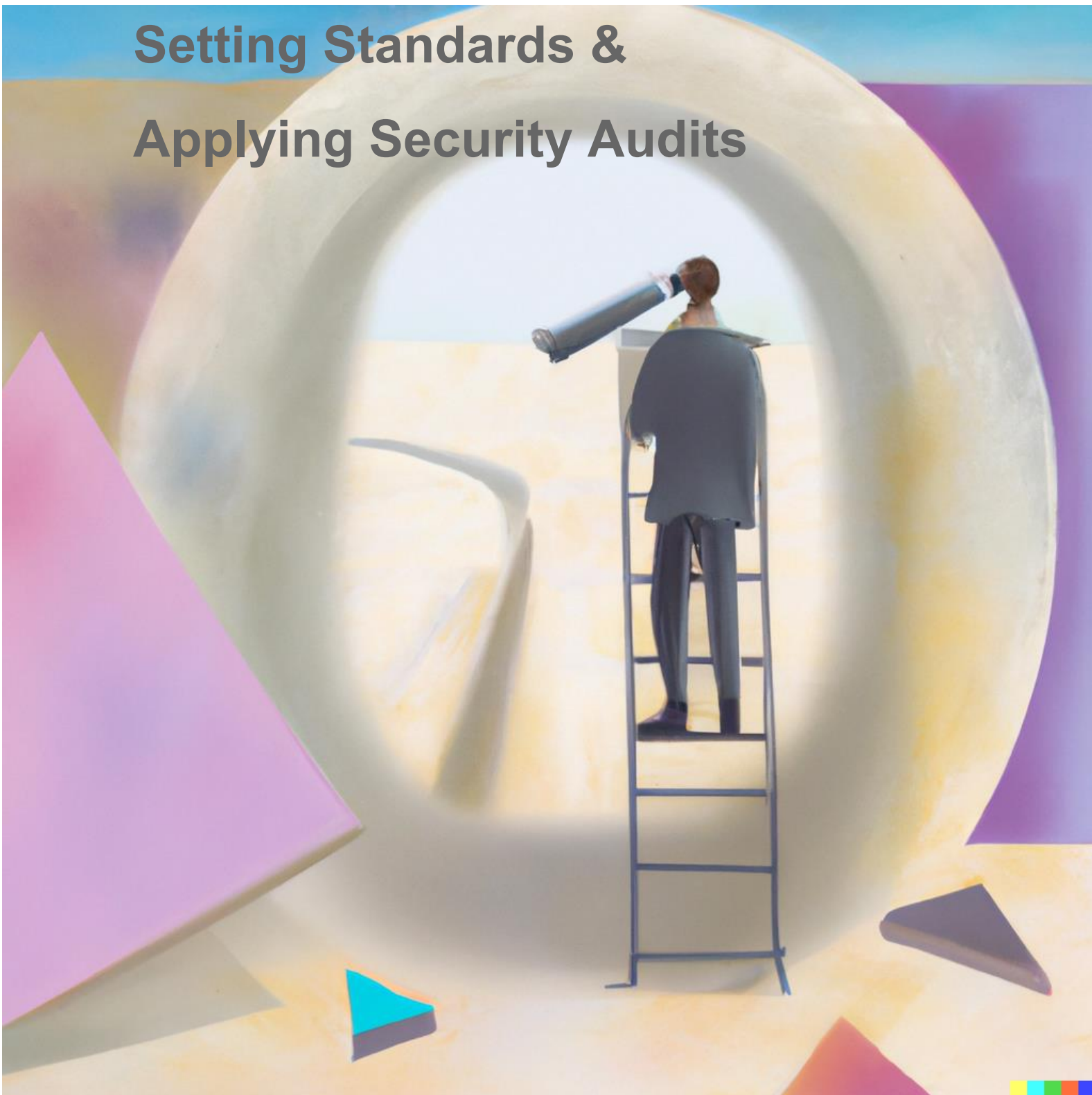
During the discussion, a wide variety of tools that could be used to track, trace, and disrupt North Korea's access to the resources they need to develop their weapons of mass destruction program, were considered. Blockchain analytics tools like those created by Chainalysis, TRM labs and others, have advanced technical capabilities for identifying suspicious transactions.

Most of the illicit transactions went through the 100 ETH pool on Tornado Cash,²⁹ which is true for the significant majority since it would have been inefficient doing 0.1 ETH transactions for an amount as large as \$600 million. Besides taking longer it would have required more resources to go through smaller pools. Cryptocurrency transactions on open permissionless blockchains without privacy features such as Ethereum or Bitcoin are traceable. It is entirely possible to see where transactions ultimately land and in which exchanges they are being cashed out.

However, when investigating these transactions, it is often found that they are being processed by centralized exchanges located outside of the United States. Imposing sanctions on these truly centralized entities in other jurisdictions is similar to how OFAC sanctions foreign banks that process illicit transactions. While targeting centralized exchanges as a means of enforcement is not a failsafe, as one participant stated, "DPRK could trade crypto for nuclear weapons just as they trade cigarettes for nuclear weapons", it could still be the most effective method or closest to traditional sanctions.

A daunting realization is that the problem is not solved by sanctioning Tornado Cash, because the tool can still be used by criminals, who can continue to exchange crypto in real life or send it to some centralized exchanges to which they have better access.

Setting Standards & Applying Security Audits



Another idea suggested was to implement a set of standards where code could only be deployed if certain types of restrictions were met, which make the code compliant. A debate on the regulatory mantra of “same activities, same risks, same rules” ensued.³⁰ One participant questioned the legitimacy of having the focus be on “activities” and “risks”, rather than solely on regulatory outcome, because in their mind, neither activities nor risks make any difference. They argued that by qualifying risks and activities, it could lead to regulatory capture, favoring the incumbent because the comparison would always be drawn to that which came before.

One viewpoint was that crypto poses additional risks compared to the traditional financial system. This was contested by an opposing view that the risks are fundamentally the same, with the main difference being variations in IT risks, consumer protection risks, and other known risks.

Risks provide a justification for regulatory action. Restricting the principle of free markets requires a valid reason, and risks serve as that basis. Historically, financial market regulation did not exist 200 years ago, but it has become clear over time that an unregulated free market can lead to negative externalities. Lessons learned from past crises led to new regulations, and whenever new risks were uncovered, they were addressed. Without the presence of risks, there is no reason for the regulator to act, as it would be considered excessive and an unlawful restriction on people's freedoms.

In a DeFi setting, the risks mostly relate to cybersecurity and are risks that could affect the goals of consumer protection or market integrity. A good way to mitigate these risks would be to implement security audits. One possibility would be licensed auditors who have to file certain types of reports as well as companies that are required to file disclosures and reports on their audits. There are also crypto-native insurance mechanisms that require software developers to have "skin in the game". These crypto-native ways to meet all regulatory goals would allow truly decentralized systems to continue to thrive while strengthening the market infrastructure.

Public and Private Sector Collaboration

An often-reiterated opinion was that we need to have 24/7 real-time interaction between the public sector and private sector, so that particular movements of value can be targeted in real-time. In addition, there needs to be a better understanding of what the best tools are that can be used to prevent access quickly, which is no different than what is done with trade-based money laundering.

There are serious cyber risks, which need to be addressed as well. This should happen through real public-private sector collaborations. Some participants agreed that more could be done proactively. There were some discussions about whether and how the private sector and the public sector should and could come together more frequently to create this regulatory regime for DeFi in a collaborative manner with ongoing knowledge exchange.



Attention was drawn to the question of "the Who?": In a decentralized DeFi world, who should the regulators be talking to? Regulators cannot talk to the software program, they can talk to the developers, who in turn would respond by saying that what they are doing is not a regulated

financial activity, "I'm just the provider of code", and in the US that would fall under First Amendment considerations of free speech. Regulators may seek out governance token holders and talk to them. However, some, if not most of them are anonymous, many may even be dispersed in several jurisdictions. Based on this realization, it becomes hard to think about what dialogue to conduct. It was suggested that instead of thinking about how to arrive at the regulatory endgame, we should be thinking about how to even arrive at the regulatory middle game.

Working Group: Identity and Self-Hosted Wallets

The question about "the who", which comes up in Decentralized Autonomous Organizations (DAOs) conversations as well, was discussed more thoroughly in a working group setting on identities.

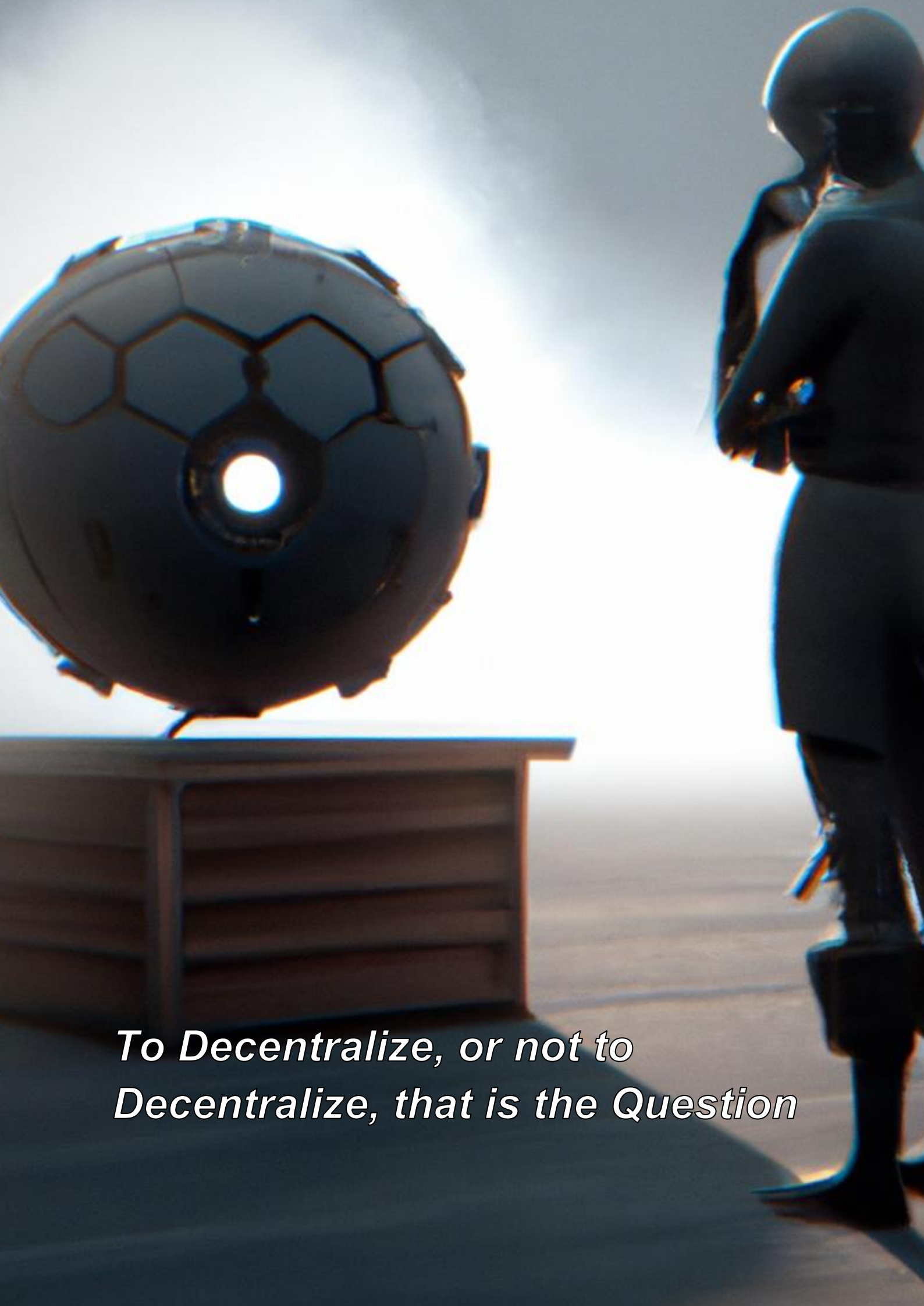
This working group presented some solutions to the personal (self-hosted) wallet problem such as the "Swiss Rule" (soon all EU/TFR) and Secretary Mnuchin's "unhosted wallet" rulemaking. These solutions usually propose that the VASP must obtain and/or verify the credentials of their customers' counterparts. However, this means that exchanges will need to collect personal identifiable information (PII) about people who are not their customers, to whom they have no contractual obligation. Other issues include constitutional privacy rights problems and GDPR and it does not improve financial inclusion because it creates the same barriers that exist in traditional banking. Furthermore, having the financial intermediary be the identity provider creates customer lock-in.



Crypto enables alternative self-sovereign identities, such as the concept of Soulbound tokens developed by Glen Weyl, Puja Ohlhaber, and Vitalik Buterin.³¹ VASPs would not do the actual PII collection or verification for anyone but their own customers, rather other "attestors" (VASPs, businesses, governments, NGOs, or even autonomous software) would do the collection, verification, and attestation of identity attributes to create a tokenized zero-knowledge proof of identity or attributes. This results in a series of benefits, such as more ID providers competing on ID quality rather than financial institutions with customer lock-in, which in turn means fewer single points of failure. Using zero-knowledge proofs helps to minimize the data that is shared or made public for compliance reasons.

In addition, constitutional and privacy laws, including GDPR, are preserved because PII is not collected by third parties on a non-contractual basis. It also opens the pathway to non-human identification for smart contracts, DAOs, and other entities. In terms of financial inclusion, such a system may also provide benefits because with a variety of attestors, some could be available for underserved populations. Persons with no viable third-party attestors may be able to use autonomous software tools that create a level of identification without third-party validation, such as biometrics or social graphs. This working group proposed that in general, identity should be tiered rather than "all or nothing" because fake IDs are still abundant. Smaller transactions may not require as much personal information as bigger ones, and p2p transactions are possible without identification between the consenting parties but they may not have access to regulated activities. There are of course a lot of questions that need to be resolved, such as how should the tiers be determined, what level of attestation should be required in each one, and will self-sovereign IDs be enough?





*To Decentralize, or not to
Decentralize, that is the Question*

When it comes to the regulatory debate concerning decentralization, the discussion often leads to addressing a widespread perception that projects structure themselves as “decentralized” to avoid regulation. Some called this “a lack of curiosity for the technology” by several agencies globally that imply in their reports that no further investigation is needed into DeFi because most protocols are centralized upon closer inspection anyway.

Some participants argued that people are racing to decentralize in this space precisely to avoid a heavy enforcement action from coming on top of them. However, if this is true then it might be a policy failure because if there were clearer pathways for conducting this type of activity in a safe way, then people would do that. Patrick Murck highlighted that “the challenge of decentralization is not from a technology perspective, being able to build decentralized tools because the technology is further along on that point than anyone could have imagined, the real challenge is bringing the business model into these kinds of new settings.”

Murck explained that “tools that are more decentralized, such as Tornado Cash, lack an effective business model if they are not

altruistic. A space of quasi-decentralized products, however, becomes a real challenge for building real businesses.” He then voiced a critique: “It’s as if there is an ongoing attempt to have the best of both worlds: to have a decentralized solution, in which liability cannot be attached to developers because they are publishing open-source software, while at the same time retaining the economic benefit of running a product or service in the financial world.”

The discussions concerning decentralization brought the roundtable back to the broader policy question of what the regulatory endgame is and whether the endgame should be how to move the regulatory conversation forward in a way that draws a distinction between acceptable and unacceptable business models and practices.

Some Reg@Tech participants noted that since the inaugural Reg@Tech in 2017, this tension and challenge appears again and again, which prompted the question: How can we “unstick” the conversation? Some suggested that “unsticking the conversation” requires regulators and policymakers to work together, taking some risks about doing new regulations, and exploring new pathways.



Exploring Possible Pathways for the Regulatory Endgame

Learn, Understand, and Use

The Fundamentals of the Technology

A widespread concern was that regulatory bodies usually do not have good technical knowledge about blockchains or crypto assets. The private sector can more easily attract this kind of competence. However, some considered it important to interact with the technology in order to make smart policy choices. At some point in the discussion, the narrative that regulators do not sufficiently understand and use the technology was challenged based on the argument that regulatory agencies have been publishing reports on these subjects for years, which means that they already have and if needed, can get more competent people to join their efforts. This view was not widely supported since resources continue to be a problem.

A criticism voiced was that extraordinarily important decisions are made by people globally that have never even interacted with the technology or know anything about blockchains besides using blockchain analytics tools. An idea was put forth that regulators could potentially explore blockchains to regulate, and possibly run a node on a blockchain so they can deeply understand these technologies and how they work.

Regulators being well versed in the technology, and speaking the same language so to say, could be a helpful pathway for meaningful regulation.

Categories of Crypto Assets

It was pointed out that not enough attention is paid to the differences that exist between crypto assets, virtual assets, digital assets, and digital commodities, as they are not all the same thing, although these terms are often used interchangeably. An NFT, for example, is not the same as Bitcoin, a governance token is not the same thing as a Bored Ape, or the same thing as Ethereum, and the list of different categories of tokens goes on. And when realizing the potential for further tokenization, there might be even more classes of assets that humans create.

Financial regulators usually only regulate products that are financial in nature. It was suggested that investing in a work of art is not financial in nature. However, what if it is not investing in a work of art but rather in an early-stage venture, or if it is token-based early-stage funding of some sort?

Working Group: Non-Financial Regulation

Although the digital asset space has matured as an industry, with lots of players, established foundations, and moving dynamic parts, a foundational piece that is missing is the regulatory or statutory clarity on what these products precisely are. A working group tackled the topic of non-financial regulation and suggested that one way to construct an efficient regulatory regime for a set of assets whose setup might change with time is to create market-driven solutions based on the assumption that there is a sufficient level of access to justice. There needs to be statutory clarity on what constitutes a financial instrument based on a clear taxonomy.

In terms of consumer and investor protection, the participants of this working group discussed asset-related information asymmetries and fraud. Questions related to enforcement in that context are important. From a private law perspective, many jurisdictions do not have clear rules on how ownership and title are associated with NFTs or other digital assets. Recognizing the cross-border phenomenon, jurisdictional questions from an enforcement perspective arise as well.

In the context of (DAO) governance, identity also becomes an important issue. The example given in this context was to imagine a person sitting on the boards of Exxon, Chevron, and BP and having three of their friends also serving on the same boards. What would that mean? And what if no one else realized they were all sitting on the same boards? Another issue discussed in this working group was the fact that shareholder activism could represent an opportunity for decentralized governance.

Courage to Experiment

Flexibility

Due to this field's rapid-paced development and dynamics, some were of the opinion that flexibility was needed on the part of regulators to adapt to change. What could be viable incentives for regulators to take that course of action? Some suggested it requires a change in approach and a new way of thinking about regulation. Others, however, suggested that maybe we should not be fundamentally transforming the way regulations or regulatory regimes work.

Another suggestion was the creation of sandboxes to consider new developments in the context of the already known. Stepping outside of the already known involves taking risks, which in the public sector cannot be done in quite the same way as in the private sector. Others disagreed, arguing that regulators do take risks, although this might not be their *modus operandi*, it was argued that they still do. However, some cautioned against a radical departure for radical departure's sake, arguing that it is important to have a familiar analog to inform and educate policymakers.

When policymakers are confronted with many new concepts, they can quickly become unfamiliar and uncomfortable. That is when analogies are helpful, such as borrowing an existing framework or some existing precedent. In the words of a participant, "this is a much better approach than trying to draw a whole new picture." Moreover, being able to draw on analogies is often necessary to resolve disagreements between the parties in order to facilitate and increase understanding.

Working Group: The Ideal Regulator

In a working group, participants came together to discuss the attributes of a regulatory institution that is resilient, adaptable to change and can be competent not only today but also in the future. The general consensus was that an ideal regulator would adopt a principles-based approach, be technologically neutral and adopt the principle of proportionality, allowing for different levels of rulemaking based on risks identified. Its mandate would be market integrity and consumer protection.



Regulation should be based on activity, such as issuance, trading, custody, banking, brokerage, advisory, collective investments, infrastructure services, etc. It would encompass all digital assets and related activities, where one would distinguish between those that are financial in nature and those that are not and can thus be excluded from the mandate. An ideal regulator would operate both globally and locally, with local minimum standards coordinated at a global level. Since in the blockchain space, the infrastructure looks different than in traditional financial markets, prudential supervision and regulation are important for the functioning of the entire market, especially for aspects, which can be systemically important.

Encourage Innovation

At Reg@Tech, some commented on the need to encourage innovation: If the regulatory hammer had been thrown at the early Internet in the 90s, we would not be here today with all the marvelous technology of videoconferencing and 24/7 connectivity. However, there is always a balance to be struck on how quickly regulation should intervene rather than letting the technology evolve. There was some discussion about setting up experimental labs and how to build expertise despite restrictions.

Recall Principles, Reinvent Methods

Consumer Protection Goal

The topic of consumer protection came up at various points in the discussions. In this innovative space, there can be some successes but there can also be large failures with no safety nets, which makes retail investor participation in this area particularly unsafe. It was argued that retail investors need to have sufficient awareness and knowledge of the risks, without which they should not be allowed to participate in a particular protocol and that service providers should not promote their services to entice the general public to participate.

The way consumer protection can happen is by providing appropriate information about the crypto asset. In light of the fact that there are many different aspects to crypto, which are not the same, do not function the same, and do not serve the same purpose, a question was posed on how to come up with an approach in a way that protects consumers without having to label something as a security or commodity, followed by more questions, such as: Is there a different approach that we could collectively take that would pursue the right level of regulation, particularly protecting consumers without having to worry about which of those buckets it falls into? And if so, what might be an alternative approach?

Same Risks, Same Rules vs New Rules for New Tools

Some participants noted that there is a lot of talk among regulators on the topic of "same risks, same rules". There are many points of disconnect between the traditional financial system and the risks and opportunities of the digital asset ecosystem. Some Reg@Tech participants highlighted that when it comes to DeFi, the risks are different, no matter how similar these transactions may look to what is known in intermediated services in the Traditional Finance (TradFi) sense, they still happen in a different way. Therefore, mitigating the risks needs to be done in alignment with the technology.

Some claimed that all of the different types of regulatory goals, such as consumer protection, market integrity, cybersecurity, could be addressed in this context. The difference lies in the way one would go about addressing these risks, which must be different from how risks are mitigated in intermediated services, unless one starts qualifying software developers as centralized entities, in which case one has gotten rid of DeFi. There was widespread agreement that DeFi is one of the most interesting use cases for crypto other than digital asset transfer of value, and that enabling rather than stifling innovation in this area is particularly important.

Tomicah Tillemann, for example, at one point said "these are new tools and we will need new rules for these new tools". A debate followed whether this was really the case. Some claimed we would end up in the wrong place if we try to shoehorn this new, very vast universe of web3 tools into regulatory frameworks that were developed in most cases 70 or more years ago. Others disagreed and did not consider crypto to be new. They argued that it rather allows people to do the

same old activities. The difference is that it changes the cost of doing those activities at scale, or in a loose collaboration rather than some centralized organization.

Some expressed concern that in the Centralized Finance (CeFi) world (e.g., Terra Luna), some random person can go and get global markets for their investment contracts in what may seem like an instant. And in the DeFi space, 50 people can work collaboratively but none of them are actually really on point for the project. While they are all contributing, the software is its own thing. Peter Van Valkenburgh drew the conclusion that "crypto is not something brand new, rather it changed the cost of doing things, which in turn might mean that it changes the cost of regulation. The question then follows: Who is the least cost avoider to actually address investor harms by making disclosures to the investing public?" It was suggested that it might no longer be an issuer because there are too many of them and often they are too loosely associated with each other or the project that they have been working on. Other examples of who could fill that role might be found in a secondary market or it might be an interface.

Another concern raised was that solving this problem has become harder because of politics and that there might not be enough incentives to create a new regime that is focused on the new least cost avoiders. Some might want to use their political will to push the agencies to force old systems to work even in this new context where they become extraordinarily costly, both to the regulated parties and to the agencies themselves.

Conclusion

Regulating innovation and new disruptive technologies like digital assets puts regulators in a particularly difficult position of an observer who at some point knows it will need to act, but does not really know how, much less when. It is as if one were observing a strange new board game, where figures are involved in what seems to be a curious dance to music that only they seem to be able to hear. The regulator needs to find out the intrinsic rules of the game and learn the notes of the melody to which the players are dancing.

Inserting rules that completely change the logic of the game puts an end to the music, the players stop dancing, and everyone exits: The game is over. Now if the regulator is skillful in creating the right incentives by making additions to the logic of the game, let us tentatively call them safety nets, without ending the music, the players keep dancing, only now the vulnerable ones are protected. The playing field has been leveled for everyone. It has become a much better game.

At some point, the regulator will leave its spot as an observer, it will need to become comfortable with the logic, the rules, and the players. It will understand that on top of the logic of the game, there is music that needs to keep playing, and it will learn to dance too. All it needs is the private sector's hand. At Reg@Tech we invite you to this new game, which we will continue to explore together.



Author

Bianca Kremer is a postdoctoral research fellow at the Wharton Blockchain and Digital Asset Project at The Wharton School, University of Pennsylvania, USA. She obtained a Ph.D. in law from the University of St. Gallen, and her doctoral thesis focused on the topic of blockchains, smart contracts, and international arbitration law.

bkremer@wharton.upenn.edu

Reg@Tech 8 Participants

- **Salman Banaei** (Uniswap Labs)
- **Yaya Fanusie** (Center for a New American Security)
- **Joey Garcia** (Xapo)
- **Keisuke Hayashi** (Japan FSA)
- **Jorge Herrada** (Commodity Futures Trading Commission)
- **Nicolas Jacquemart** (Swiss FINMA)
- **Kavita Jain** (Federal Reserve Board)
- **Siân Jones** (xReg)
- **Josh Klayman** (Linklaters)
- **Michele Korver** (a16z Crypto)
- **Bianca Kremer** (Wharton BDAP)
- **Bill Laufer** (Wharton School)
- **Brynly Llyr** (World Economic Forum)
- **Alison Macdonald** (Office of the Comptroller of the Currency)
- **Caroline Malcolm** (Chainalysis)
- **Giovanna Massarotto** (Penn Carey Law)
- **Sigal Mandelker** (Ribbit Capital)
- **Peter Marton** (New York Department of Financial Services)
- **Patrick Murck** (Transparent Systems)
- **Aurelia Nick** (MME)
- **Michael Oh** (FINRA)
- **Alden Pelker** (Department of Justice)
- **Daniel Resas** (YPOG Law/Bubbles)
- **Rebecca Rettig** (Aave)
- **Marco Santori** (Kraken)
- **Lee Schneider** (Ava Labs)
- **Christoph Simmchen** (Safe Ecosystem Foundation)
- **Valerie Szczepanik** (Securities & Exchange Commission)
- **Joel Telpner** (IOHK/Sullivan & Worcester)
- **Tomicah Tillemann** (Haun Ventures)
- **Peter Van Valkenburgh** (Coin Center)
- **Kevin Werbach** (Wharton School)
- **Michael Wong** (Office of Senator Synema)
- **Selene Yoe** (Singapore MAS)
- **David Zaring** (Wharton School)
- **Landon Zinda** (Senate Banking Committee)

Endnotes

¹ Terra is a blockchain protocol for an algorithmic stablecoin called Terra, which is convertible into the network's native token LUNA. See chapter "From Earth to the Moon and Back: Extraordinary Rise and Spectacular Fall of Terra Luna", see also Binance Academy, What Is Terra (LUNA)?, <https://academy.binance.com/en/articles/what-is-terra-luna>.

² Tornado Cash is a transaction mixer on the Ethereum blockchain. See chapter "Stopping the Unstoppable: Inside the Eye of Tornado Cash". See also Milko Trajcevski, What Is Tornado Cash?, Alexandria at Coinmarketcap, 2021, <https://coinmarketcap.com/alexandria/article/what-is-tornado-cash>.

³ DAO stands for "Decentralized Autonomous Organizations". See Chapter "Targeting Who, Targeting What? Charges Against Ooki DAO". For more on DAOs, see David Gogel, Bianca Kremer, Aiden Slavin and Kevin Werbach, Decentralized Autonomous Organizations: Beyond the Hype, White Paper, June 2022, World Economic Forum and Wharton BDAP, https://www3.weforum.org/docs/WEF_Decentralized_Autonomous_Organizations_Beyond_the_Hype_2022.pdf.

⁴ The White House, Fact Sheet: White House Releases First-Ever Comprehensive Framework for Responsible Development of Digital Assets, Press Release, September 16, 2022, <https://www.whitehouse.gov/briefing-room/statements-releases/2022/09/16/fact-sheet-white-house-releases-first-ever-comprehensive-framework-for-responsible-development-of-digital-assets/>.

⁵ Council of the European Union, Digital finance: agreement reached on European crypto-assets regulation (MiCA), Press release, June 30, 2022, <https://www.consilium.europa.eu/en/press/press-releases/2022/06/30/digital-finance-agreement-reached-on-european-crypto-assets-regulation-mica/>.

⁶ Basel Committee on Banking Supervision, Consultative Document, Second consultation on the prudential treatment of cryptoasset exposures, September 2022, <https://www.bis.org/bcbs/publ/d533.pdf>.

⁷ See United States Office of Government Ethics, Legal Advisory, July 5, 2022, [https://www.oge.gov/web/oge.nsf/News+Releases/E116F1FD24F94BB3852588770058A0FA/\\$FILE/LA-22-04.pdf](https://www.oge.gov/web/oge.nsf/News+Releases/E116F1FD24F94BB3852588770058A0FA/$FILE/LA-22-04.pdf). See also Tom Mitchelhill, Crypto owners banned from working on US Government crypto policies, Cointelegraph, July 7, 2022, <https://cointelegraph.com/news/crypto-owners-banned-from-working-on-us-government-crypto-policies>.

⁸ FATF, Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers, June 2022, <https://www.fatf-gafi.org/media/fatf/documents/recommendations/Targeted-Update-Implementation-FATF%20Standards-Virtual%20Assets-VASPs.pdf>.

⁹ Krisztian Sandor and Ekin Genç, The Fall of Terra: A Timeline of the Meteoric Rise and Crash of UST and LUNA, CoinDesk, August 19, 2022, <https://www.coindesk.com/learn/the-fall-of-terra-a-timeline-of-the-meteoric-rise-and-crash-of-ust-and-luna/>.

¹⁰ Do Kwon, Announcing TerraUSD (UST)- the Interchain Stablecoin, Medium, September 21, 2020, <https://medium.com/terra-money/announcing-terrausd-ust-the-interchain-stablecoin-53eab0f8f0ac>. During Reg@Tech6 one of the discussions centered around stablecoins. In the report based on our only virtual roundtable, we discussed the types of stablecoins and made a distinction between asset-backed algorithmic and pure algorithmic stablecoins.

¹¹ Shaurya Malwa, Terra's LUNA surges 17% as UST Becomes Third-Largest Stablecoin, CoinDesk, April 19, 2022, <https://www.coindesk.com/markets/2022/04/19/terra-luna-surges-17-as-ust-becomes-third-largest-stablecoin/>.

¹² Krisztian Sandor and Ekin Genç, The Fall of Terra: A Timeline of the Meteoric Rise and Crash of UST and LUNA, CoinDesk, August 19, 2022, <https://www.coindesk.com/learn/the-fall-of-terra-a-timeline-of-the-meteoric-rise-and-crash-of-ust-and-luna/>.

¹³ CFTC, Release Number 8590-22, 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, September 22, 2022, <https://www.cftc.gov/PressRoom/PressReleases/8590-22>.

¹⁴ U.S. Department of Treasury, U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash, Press Release, August 8, 2022, <https://home.treasury.gov/news/press-releases/jy0916>. See also U.S. Department of Treasury, Specially Designated Nationals and Blocked Persons (SDN) Human Readable Lists, <https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists>.

- ¹⁵ U.S. Department of Treasury, U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash, Press Release, August 8, 2022, <https://home.treasury.gov/news/press-releases/jy0916>. See also Alia Shoaib, North Korea-linked hackers stole \$620 million in Axie Infinity cryptocurrency heist, FBI says, Businessinsider, April 15, 2022, <https://markets.businessinsider.com/news/currencies/crypto-heist-axie-infinity-hackers-north-korea-stole-620-million-fbi-2022-4>. Profits from cyberattacks are reportedly used to fund North Korea's nuclear and missiles program, see Michelle Nicholas, EXCLUSIVE North Korea grows nuclear, missiles programs, profits from cyberattacks - U.N. report, Reuters, February 7, 2022, <https://www.reuters.com/world/asia-pacific/exclusive-nkorea-grows-nuclear-missiles-programs-profits-cyberattacks-un-report-2022-02-05/>.
- ¹⁶ Understanding Tornado Cash, Its Sanctions Implications, and Key Compliance Questions - Chainalysis, <https://blog.chainalysis.com/reports/tornado-cash-sanctions-challenges/>.
- ¹⁷ Understanding Tornado Cash, Its Sanctions Implications, and Key Compliance Questions - Chainalysis, <https://blog.chainalysis.com/reports/tornado-cash-sanctions-challenges/>.
- ¹⁸ U.S. Department of the Treasury, Treasury Designates Iran-Based Financial Facilitators of Malicious Cyber Activity and for the First Time Identifies Associated Digital Currency Addresses, Press Release, November 28, 2018, <https://home.treasury.gov/news/press-releases/sm556>.
- ¹⁹ U.S. Department of the Treasury, U.S. Treasury Issues First-Ever Sanctions on a Virtual Currency Mixer, Targets DPRK Cyber Threats, Press Release, May 6, 2022, <https://home.treasury.gov/news/press-releases/jy0768>.
- ²⁰ Nikhilesh De, Crypto Think Tank Coin Center Sues US Treasury Over Tornado Cash Sanctions, CoinDesk, October 12, 2022, <https://www.coindesk.com/policy/2022/10/12/crypto-think-tank-coin-center-sues-us-treasury-over-tornado-cash-sanctions/>.
- ²¹ See Chainalysis, Mixer Usage Reaches All-time Highs in 2022, <https://blog.chainalysis.com/reports/crypto-mixer-criminal-volume-2022/>.
- ²² See Andre Beganski, Ethereum Co-founder Says He Used Now-Blacklisted Tornado Cash to Donate to Ukraine, Decrypt, August 9, 2022, <https://decrypt.co/107075/ethereum-cofounder-used-blacklisted-tornado-cash-donate-ukraine>.
- ²³ See Chainalysis, Mixer Usage Reaches All-time Highs in 2022, <https://blog.chainalysis.com/reports/crypto-mixer-criminal-volume-2022/>.
- ²⁴ For a list of the contracts sanctioned, see U.S. Department of the Treasury, Cyber-related Designation – Specially Designated Nationals List Update, August 8, 2022, <https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20220808>.
- ²⁵ U.S. Department of the Treasury, Cyber-related Designation, August 8, 2022, <https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20220808>.
- ²⁶ The White House, Executive Order -- "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities", April 01, 2015, <https://obamawhitehouse.archives.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m>.
- ²⁷ TORN is a governance token that was distributed to early adopters of Tornado Cash in an airdrop. See <https://etherscan.io/token/0x77777feddddfc19ff86db637967013e6c6a116c>. See also Tornado Cash, Tornado.Cash Governance Proposal, Medium, December 17, 2020, <https://tornado-cash.medium.com/tornado-cash-governance-proposal-a55c5c7d0703>.
- ²⁸ Etherscan, <https://etherscan.io/>.
- ²⁹ Etherscan, Tornado.Cash: 100 ETH, Address 0xA160cdAB225685dA1d56aa342Ad8841c3b53f291, <https://etherscan.io/address/0xA160cdAB225685dA1d56aa342Ad8841c3b53f291>. This pool allows for deposits and withdrawals in increments of 100 ETH. See also Alex Wade et al, How does Tornado Cash work?, Coin Center, August 25, 2022, <https://www.coincenter.org/education/advanced-topics/how-does-tornado-cash-work/>.
- ³⁰ There were variants of this mantra that some participants used in discussions, e.g., "same risks, same rules" or "same risk, same regulation".
- ³¹ E. Glen Weyl, Puja Ohlhaven, and Vitalik Buterin, Decentralized Society: Finding Web3's Soul, SSRN, May 10, 2022, https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID4105763_code1186331.pdf?abstractid=4105763&mirid=1&type=2.



WHARTON BLOCKCHAIN AND DIGITAL ASSET PROJECT

The work is licensed under the Creative Commons
Attribution-Noncommercial 4.0 License.

Published by the
Wharton Blockchain and Digital Asset Project.

Wharton Blockchain and Digital Asset Project
bdap.wharton.upenn.edu
whartonbdap@wharton.upenn.edu