BDAP

WHARTON BLOCKCHAIN AND DIGITAL ASSET PROJECT

Restoring Trust & Managing Risks

June 2023

The Ninth Reg@Tech Roundtable On Digital Assets

Wharton
University of Pennsylvania

Foreword

The emergence and proliferation of digital assets have sparked global interest. Digital assets, non-fungible tokens (NFTs), decentralized finance (DeFi), and decentralized autonomous organizations (DAOs) have introduced both major opportunities and unique challenges. It is in this context that the Reg@Tech Roundtable serves as a platform for dialogue and collaboration among industry stakeholders, regulators, and policymakers.

This report provides an overview of the discussions and insights shared during the 9th Reg@Tech roundtable, capturing the collective wisdom and perspectives of thought leaders, academics, experts, and practitioners from diverse backgrounds. Our aim is to foster a deeper understanding of the digital asset landscape and to inspire ongoing dialogue and collaboration among all stakeholders involved in shaping the future of digital asset regulation.

Kevin Werbach

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

This report summarizes discussions at Reg@Tech 9, which took place March 23-25, 2023 at The Wharton School in Philadelphia. Reg@Tech is conducted in accordance with the Chatham House Rules. Participants include government representatives who do not represent the official positions of their agencies. There is no consensus on many topics. While this summary attempts to reflect the spirit of the meeting, the conclusions are those of the author. It should not be taken as an embodiment of the views of any participants or their organizations.

Image Credits

Image on p. 21 created by Bianca Kremer & DALL-E2.
Image on p. 22 created by the working group & Midjourney.
All other images, including cover image, created by Bianca Kremer & Midjourney.

State of Digital Asset Regulation

The Ninth Reg@Tech Roundtable on Digital Assets brought together industry leaders, academics, regulators, and stakeholders to discuss the rapidly evolving landscape of digital assets and the challenges and opportunities that lie ahead.

The three-day workshop delved into critical aspects of digital asset regulation, including the need for global coordination, the development of risk management frameworks, and the importance of consumer protection. The discussions emphasized the complexities of regulating digital assets and the significance of collaboration between different stakeholders to create effective risk management practices tailored to blockchain-related projects and platforms. Moreover, the report sheds light on the challenges of ensuring market integrity and investor protection in the digital asset space. It also highlights the importance of a decentralized digital identity system, privacy-protecting technologies, and risk education in addressing the unique challenges of the digital asset industry.

During the first day of Reg@Tech 9, a roundtable session was held to discuss various topics related to digital asset regulation. The European Union's Markets in Crypto Assets (MiCA) regulation was a central topic of conversation, as - at the time of the conference - it was awaiting approval by the European Parliament.[1] Participants emphasized the importance of staying close to the market and adapting national legislation to keep pace with the rapid development of the crypto market. They also noted that discussions about MiCA 2.0 are underway to address the gaps in the current legislation.

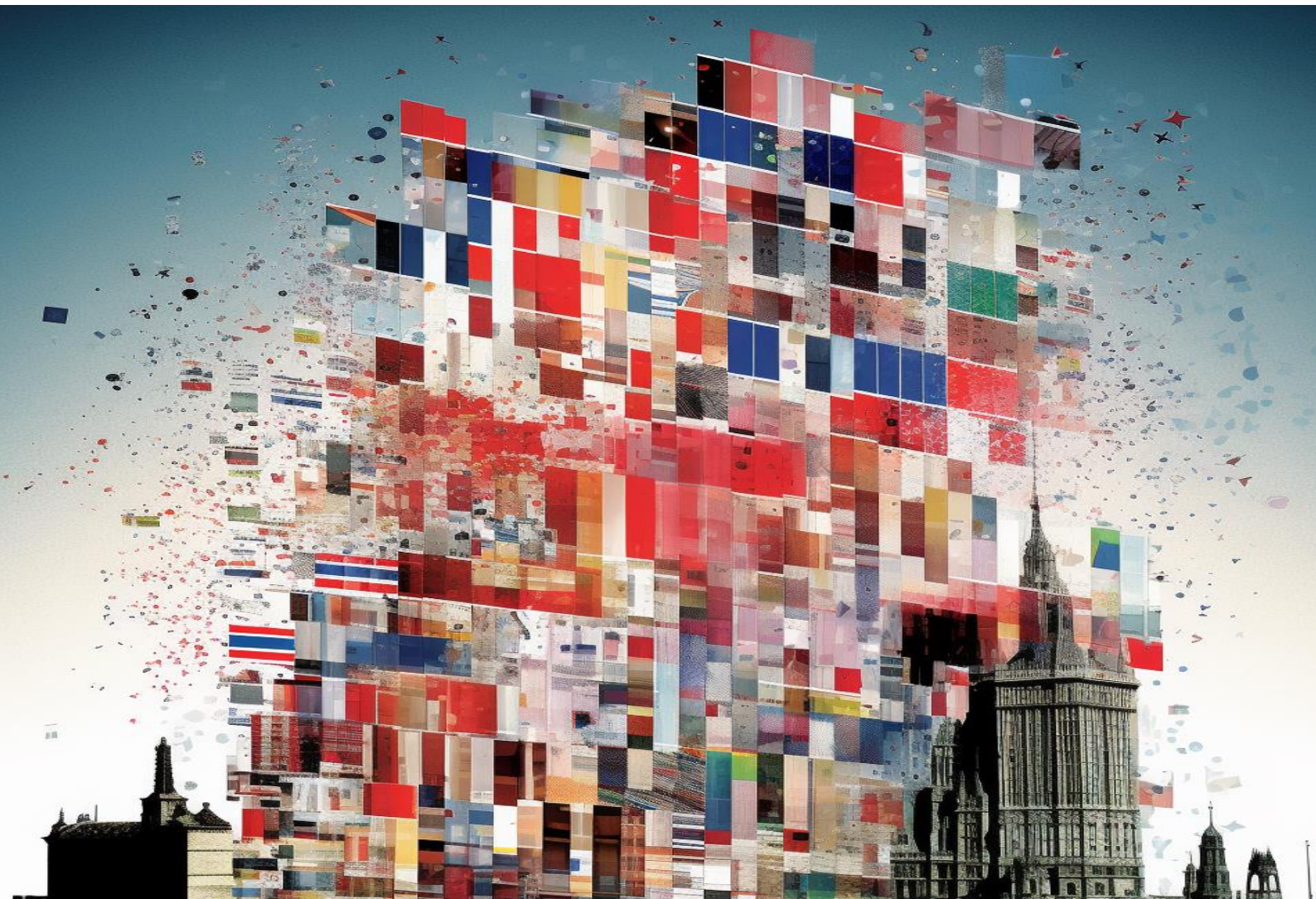
Level two regulations were also discussed. Some participants highlighted the defensive nature of the MiCA regulation as it was initiated in response to the possibility of a private company taking over the public good of money (the Libra/Diem project). The journey towards developing MiCA has revealed the "law of unintended consequences" at play. A striking example is the lack of synchronization between policy branches. During the simultaneous updates to the Transfer of Funds Regulation (TFR) and MiCA discussions, the teams managing risks for each policy were isolated from each other. Consequently, fiat and cryptocurrency transactions may be treated differently in Europe, resulting in regulations that lack technology neutrality.

Balancing policy-making with technical considerations and understanding the risks involved in cryptocurrency transactions were underscored as crucial. The session also touched upon the challenges faced by various jurisdictions in complying with AML regulations, the complexities surrounding the global digital economy, and the importance of supervising and providing support for compliance. Regulatory arbitrage, interpretation issues, and proportionality concerns are significant issues. Regulation of stablecoin issuance, money transmitter licensing, wallet management, NFTs, and crypto assets were discussed. The conversation revolved around finding the right balance between managing risk and enforcing regulations.

The fragmented international banking regulatory landscape was also a topic of conversation, highlighting the difficulties faced by banks and financial institutions in complying with different jurisdictions and regulatory regimes. The lack of global standards and harmonization, as well as the implementation of new technologies and financial products, were cited as complicating factors in the regulatory environment.

The complexity of regulating crypto assets was a central theme, emphasizing the need for a taxonomy and a conversation on how to regulate such diverse assets. The session also delved into the nature of digital assets and property law, and the challenges of regulating digital assets generally.

Overall, the roundtable session provided a comprehensive overview of the challenges and complexities faced in regulating digital assets and the ongoing efforts to find a balance between risk management, innovation, and competition in the rapidly evolving crypto market.



Diverse Interpretations of Crypto Assets and Challenges for Trading Venues

Some participants argued that we have yet to establish a universally accepted definition of crypto assets. The understanding of what constitutes a crypto asset varies significantly from one jurisdiction to another. The US perspective, for instance, differs from those held in Australia, the European Union's Markets in Crypto-Assets (MiCA), and the UK.

This disparity poses a considerable policy challenge as each region's crypto asset framework embodies a distinct understanding. These differences can pose significant risks from a policy perspective, with potential complications in risk management due to inconsistent global definitions.

There was an understanding among some participants that trading platforms could host a wide array of assets, each with its unique characteristics and requirements. The potential challenges that trading venues could face when dealing with different types of assets could be particularly cumbersome. Some participants viewed that from a market integrity perspective, these venues need to manage various regulations, especially when different assets are traded on the same platform. Therefore, the need for comprehensive trading rules encompassing transparency, accessibility, and prohibitions against insider and manipulative trading was underscored by these discussants.

However, the view was not universally accepted that regulations should be uniformly applied. Some participants emphasized that the protections needed for trading various assets, be they cars or securities, should differ significantly, questioning the tendency to apply a single regulatory framework to all assets. These contributors suggested that a more nuanced approach might be necessary, taking into account both the trading market dynamics and the unique attributes of the assets being traded.

Several participants also touched upon the varying meaning of the term "security" in different jurisdictions, each free to regulate any instrument they categorize as a security. While this situation has always posed a challenge, the advent of a global trading environment has amplified these issues, leading to cross-jurisdictional complications.

In Europe, a security, as a financial instrument under the existing MiFID 2 regime, triggers a certain level of regulation when traded, as observed by some discussants. However, in the US, the trading aspect of an asset does not necessarily influence its classification as a security under securities laws. In addition, there are slight variations in the definitions of "securities" across U.S. securities laws, the Uniform Commercial Code, and different state laws. Further, a senior advisor employed by the Federal Government noted that the U.S. system of federalism results in the presence of multiple regulatory bodies including securities regulators, commodity regulators, and their state counterparts.

However, this diversity, while presenting challenges, can also be seen as an

avenue for innovation. The U.S. encourages states to be “laboratories of innovation,” allowing them to take calculated risks and potentially attract certain industries or enhance consumer protections through unique applications of their laws. A notable example of this is California's adoption of a data privacy law modeled after the European Union's General Data Protection Regulation (GDPR).

Some participants noted that the ongoing debates surrounding digital assets in the U.S. not only revolve around the risks and opportunities of these assets but also mirror long-standing debates on financial services regulation. While the U.S. maintains a dual system of state and federal regulation, further complexity is added by the presence of multiple federal bank regulators.

It was argued that despite the challenges and the seemingly slow pace of progress, the U.S. will eventually reach a resolution. However, predicting a timeline for this remains elusive. This perspective resonates with the timeless adage, “the more things change, the more they stay the same,” reflecting the recurring nature of these debates whenever a paradigm shift in financial services regulation is considered.

Finally, a few participants highlighted the increasing complexity that tokenized real-world assets bring to the mix. They speculated on the possibility of diverse tokenized assets, such as body organs or automobiles, being traded against cryptocurrencies on the same platform. From these discussants’ viewpoint, the regulatory challenges stemming from these scenarios were identified as one of the most pressing issues to address in the future.

The Nature of the Assets

Some participants stressed that crypto assets should not be seen as a single asset class due to their diverse natures. The roundtable discussion thus explored the following question: does the nature of the asset matter?[2] While there was speculation about a future where the nature of the asset might not hold significance due to the ubiquity of internet trading, some participants acknowledged that this perspective deviates from traditional legal interpretations in most jurisdictions.

While some participants emphasized the importance of discussing the nature of different assets and considering the associated challenges, such as market integrity, custody, disclosure, and privacy, others saw the activity occurring on the blockchain as more relevant than the nature of the digital asset itself. However, there was acknowledgment of the challenges involved in defining activities and the difficulty in applying regulation to newly emerging activities.

Lee Schneider drew attention to the distinction between real estate law (real property law) and other areas of law, such as contract law or securities law. The development of Real Property Law in common law jurisdictions has been marked by a unique trajectory, driven by historical factors. In agrarian societies, owning real property was a primary mode of wealth accumulation and livelihood, which significantly influenced the evolution of the related law.

Schneider also highlighted a recent development, in which the Treasury Department and the IRS, through Notice 2023-27, unveiled their intention to classify certain NFTs as Section 408(m) collectibles.[3] He interpreted the guidance to mean that the IRS may eventually treat a token representing a gemstone, for example, as the gemstone itself.

The notion was that tokenization, at its simplest level, is equivalent to writing an entitlement on a piece of paper, such as "Person A gets one gemstone". While acknowledging the additional complexity that may layer onto this fundamental principle, Schneider suggested that this understanding of tokenization could guide future legal and regulatory perspectives. In general, the discussion emphasized the importance of collaboration between industry and regulators to standardize legal terms and understand the nature of assets.

Measured Policymaking

The roundtable discussion also brought to the fore the importance of measured policymaking. An instance was shared where the European Parliament almost rejected MiCA due to a hastily introduced proposal to ban proof of work. This proposition appeared to be a reactionary defense strategy, with insufficient discussion and consideration.
A similar issue was raised with the last-minute introduction of NFTs at the council level. This move lacked technical discourse, consultation with the private sector, and due risk consideration. Policymaking without adequate understanding was identified as a significant risk.

As anticipation builds for MiCA 2.0, the lessons from the past year were underscored. The discussion stressed the need for policymakers to avoid making hasty decisions without sufficient evidence and a thorough examination of the potential implications. The importance of dialogue, deep understanding, and a measured response cannot be overstated in the realm of policymaking.

The Quest to Measure Decentralization

JP Vergne of UCL School of Management presented an innovative perspective on how to measure decentralization, introducing a new measurement approach that identifies two key aspects: information dispersion and decision-making dispersion, collectively referred to as “dispersion of authority”. This approach aims to quantify the distribution of access and decision-making power among different types of agents, enabling the comparison of decentralization across various blockchain platforms over time.

Vergne juxtaposed traditional hierarchical authority structures with those of Bitcoin's blockchain platform. Within Bitcoin, different levels of information access exist among wallet users, miners, and nodes. Similarly, decision-making dispersion is observable among these

agents with varying degrees of authority, from signing transactions to accepting or rejecting blocks, and the ordering of pending transactions.

Such metrics could inspire new regulatory frameworks and enhance transparency for consumers and investors. Though the speaker shared sample data comparing Ethereum, Bitcoin and other blockchains, he emphasized that the responsibility of defining and setting thresholds for decentralization falls within the remit of regulators, not researchers.

The discussion further delved into the intricacies of decision-making authority in decentralized networks. The potential for assigning weights to different decision categories was proposed, though the exact basis for such weighting remains undetermined.

Governance under a Magnifying Glass

Some participants addressed concerns about potential malicious activities and obfuscation of control within blockchain networks and decentralized autonomous organizations (DAOs). While DAOs may claim decentralization in theory (and may be decentralized in name only, “DINO”), there is often a practical reality where decision-making control lies in the hands of a select few. This discrepancy raises questions about the true extent of decentralization within such systems and poses potential regulatory challenges.

From a regulatory standpoint, governance decisions were singled out as of utmost importance. The significance of understanding the number of individuals with the authority to alter the core protocol of a blockchain system was highlighted. In particular, regulators may want to identify the agents capable of initially setting the parameters that could enable such alterations. The existence of such an agent, potentially wielding a so-called “God key,” raises pertinent questions about the centralization of power within a supposedly decentralized system.

This focus on governance and protocol alteration is crucial because the degree of centralization within a system can have significant implications for regulatory enforcement. As such, a deeper understanding of the practical implementation of decentralization, especially in terms of governance within blockchain platforms, is key to developing appropriate and effective regulatory measures.

The session included a discussion on the challenges encountered while gathering data on various blockchain networks and improving transparency. The speaker highlighted the difficulty in obtaining historical data and information on individual miners, resorting to interpolation and inference to fill gaps. A collaborative approach with industry participants was deemed crucial to acquiring reliable data.

Towards a Decentralization Index

Various dialogues covered a range of topics, including the importance of rigorous metrics for decentralization, information access in decentralized networks, challenges in identifying joint control behind nodes, the relationship between permissions and decentralization in blockchain networks, censorship, and factors influencing decentralization in blockchain technology.

A participant also highlighted the Cambridge Bitcoin Electricity Consumption Index,[4] which provides a geographical breakdown of Bitcoin mining activity. They suggested the creation of a similar distribution map regarding decentralization showing changes over time across different networks, which regulators could monitor closely. This kind of transparency and understanding of the distribution of authority in blockchain networks, they believe, would significantly aid their ongoing analysis and research.

Trust-Building in Digital Asset Markets

One of the central themes during the roundtable discussions was how to regain trust in digital assets, specifically in light of the key developments over the past year. The substantial influence of Luna, FTX in conjunction with Silvergate, Signature, and Silicon Valley Bank, cannot be overlooked. These entities play a key role in forming the context for contemporary regulatory discussions surrounding digital assets.

The initial aim of the discussion was to uncover potential advancements and necessary actions in this arena, given the noticeable shortcomings in transcending the initial framework. This conversation centered around bolstering trust and achieving regulatory harmony within the constantly evolving realm of digital assets.

Key steps to achieve trust include better risk management, industry accountability measures, and regulatory mechanisms. Separating operational risks from address-specific risks and following specific risk management principles were emphasized. The problem of custodians and counterparty risk was addressed, with a suggestion to create federal alternative-state money transmission licensing.[5]

Challenges in (Re)gaining Trust and the Need for Clarity

The digital asset industry faces challenges in building trust and obtaining government regulation due to political pressures and lack of unity. It was suggested that the industry needs to work with regulators to leverage technology for furthering anti-terrorism financing, financial crime prevention, and securities laws.

A clear vision for the industry and government regulations can help improve trust. Some argued that the crypto industry needs to change its approach and be more willing to work with regulators to achieve this trust. Education and engagement are crucial to bridge the gap between regulators and the industry.

The discussion also addressed conflicts of interest in the cryptocurrency industry when it comes to government regulation. The roundtable suggested that creating a functional separation within the industry, similar to the traditional financial industry, could help establish trust.

Need for Clearer Custodial Rules in the Digital Asset Space

One of the fundamental issues identified within the digital assets' ecosystem was on the role and regulation of custodians. These entities pose a significant counterparty risk due to their claim of owning assets on behalf of their customers through various structures such as licensed money transmitters, New York state chartered trust companies, or offshore entities with potentially diverse regulatory environments. However, the lack of unified federal guidelines in the US complicates the issue, putting consumers and investors at risk, despite the country's leading role in implementing certain policies like Anti-Money Laundering (AML).

It appears that the US has not taken a similar lead in regulating custodians for consumer and investor protection, instead leaving this responsibility to individual states, much like the approach to online money transmitters in the early 2000s. In fact, the existing regulatory framework has led to companies like PayPal, which function similar to banks, being regulated as money transmitters, an approach some would consider as a misstep. Peter Van Valkenburgh proposed that custodians of crypto should be treated similarly to custodians of traditional currencies like the dollar. Depending on their business model, they could potentially be classified as deposit takers, with appropriate regulatory guardrails ensuring their adequate capitalization.

While recognizing the unique features of the crypto space such as 24-hour settlement cycles, Van Valkenburgh suggested that these can be taken into account when designing a

suitable regulatory regime. This should not involve trying to fit the regulation of custodians into existing structures like money services businesses or money transmitter licenses, which were designed for different regulatory challenges.

Van Valkenburgh also noted that this is a pressing issue that should have been addressed years ago to prevent it from becoming a systemic problem in the digital assets space. He also highlighted that there is a need to differentiate between centralized finance (CeFi) and decentralized finance (DeFi). This distinction is crucial to avoid the pitfall of attempting to regulate all software developers and quasi-decentralized entities under one regulatory umbrella, when the more immediate task lies in ensuring a robust regulatory structure for entities claiming to hold customer funds. Schneider argued that trust must be built using broader markers beyond KYC requirements, and that it is essential to trust the code in DeFi and other decentralized systems.

The Markers of Trust

Some participants highlighted the importance of understanding the markers people use to determine whether or not to trust a counterparty in the blockchain ecosystem. Traditionally, Know Your Customer (KYC) requirements have been fundamental in establishing trust. However, some in the group argued that this is often interpreted too narrowly, focusing solely on concrete identifications like a driver's license.

The discussion suggested a need for broader markers to create trust, looking beyond the immediate "customer" to include all counterparties involved. These markers could include the reputation of investors in a blockchain company or the credibility of regulators such as the SEC.

However, these markers are increasingly not seen as indicative of trustworthiness, as was evidenced by the FTX scandal, which was highly trusted by investors and regulators. Therefore, there's a need for redefining these trust markers and re-evaluating how trust is established in this space.

Lastly, a key point of discussion revolved around the role of technology in building trust. While blockchain is often deemed "trustless," it's more accurate to say it requires users to "trust the code." This means that trust is placed in the code underlying the blockchain, rather than in any individual counterparty. However, when hacks or system gaming occur, this trust in the code can be undermined. While regulation may not entirely solve these issues, it's an important element to consider in trust-building strategies.

The Evolution of Trustlessness

The term “trustless” has frequently been used in the blockchain industry, but its usage and meaning have evolved significantly over time.

JP Vergne explained that the term “trustless” originated in network engineering, where it referred to systems that did not require servers to establish a handshake. However, it was subsequently adopted by the wider public and imbued with a more common, albeit misunderstood, connotation of not requiring trust in any third party.

Vergne noted that this notion of a self-operating, trustless system is a misinterpretation of the original intent of the term. In recent years, the term has fallen out of favor as it became evident that complete trustlessness is not a feasible or desirable characteristic of these systems.

Vergne further highlighted that from a social science perspective, trust is typically broken down into three dimensions: reliability, accountability, and predictability. Recent controversies within the blockchain industry have highlighted significant shortcomings in these areas:

1. Reliability: There have been instances where blockchain systems have proven to be unreliable, such as smart contracts being hacked or entire blockchain networks, like Solana, experiencing hours of downtime.
2. Accountability: Certain instances have displayed a lack of accountability, with significant issues resulting in individuals becoming fugitives and evading responsibility.
3. Predictability: Blockchain systems have also shown a lack of predictability. This unpredictability stems not only from technical aspects but also from uncertain regulations, leaving stakeholders uncertain about the future of these systems.

Given these challenges, Vergne suggested that trust in blockchain systems does not simply need to be rebuilt, but rather needs to be built from scratch. This fundamental construction of trust would require addressing the issues of reliability, accountability, and predictability that currently plague the industry.

The Role of Governance in Trust and Increasing Tech Literacy

Some argued that the more fundamental issues relate to governance and regulatory oversight. They noted that KYC is traditionally associated with financial surveillance and anti-money laundering, rather than systemic risk or consumer and investor protection, making its inclusion in this context potentially confusing.

FTX, a major Centralized Finance (CeFi) organization had no board of directors. According to Peter Van Valkenburgh, this indicated a fundamental failure within the industry, with vast sums of money being entrusted to organizations without the necessary governance structures in place. There was also criticism of the role of venture capitalists and tech luminaries, who have made poor investment decisions that retail investors then followed.

Van Valkenburgh saw the lack of regulated, competitive alternatives to these poorly governed entities as a significant part of the problem, resulting in a clear need for the creation of federally regulated custodians for crypto and a regulatory landscape that allows

for competition and innovation within secure, regulated entities. The absence of such entities - it was argued - would continue to push investors towards risky offshore entities.

The discussion at the roundtable also highlighted the significant shift in perception of Decentralized Finance (DeFi) within key regulatory bodies over the past few years. Notably, initial skepticism and dismissal of DeFi as a passing fad has evolved into a more nuanced understanding of the technology and its potential risks and benefits.

The shift was exemplified by the European Council's response to the FTX situation. Within 24 hours of the incident, the analysis concluded that the issues with FTX were attributable to governance failures, not the cryptocurrency sector itself. This understanding marked a significant step away from the blanket skepticism of blockchain technology seen in earlier years.

The roundtable participants stressed that trust cannot exist without understanding. Initial resistance from regulators was often attributed to a lack of understanding of the technology. As such, some in the group emphasized the importance of education in fostering understanding and, consequently, building trust.

The roundtable discussion highlighted efforts to engage regulators and other key stakeholders, encouraging their attendance at events and participation in discussions to increase their understanding of the technology. Participants also pointed to the European Blockchain Services Infrastructure as a significant endorsement of the technology's potential, demonstrating a level of trust in blockchain's ability to underpin citizen services.[6]

The roundtable discussions underscored the growing trust in the blockchain and cryptocurrency sector, a testament to the significant strides made in understanding and engagement over the past few years. This trust, however, must be met with caution, as significant funds have been entrusted to entities with inadequate governance structures and unclear credentials.

While Know Your Customer (KYC) and Decentralized Finance (DeFi) present legitimate issues, these concerns must not overshadow the more immediate problem of weak governance in the crypto space. Addressing these governance issues is crucial to sustaining and enhancing trust in this rapidly evolving sector. Ultimately, the establishment of a more secure and accountable environment, facilitated by better governance and continued understanding, will be key in maintaining the positive trajectory of trust in the blockchain and cryptocurrency industry.

Toward a Shared Vision of Risk Management

The roundtable discussion then focused on the development of consistent risk management procedures for digital assets. The conversation covered unique technology risks and the need for risk management when governance differs from traditional assets. Participants emphasized the importance of regulatory protection and the opportunity to use technology to build trust layers, preventing potential harm to retail customers without limiting innovation.

Challenges in Decentralized Finance (DeFi)

The discussion brought to light the opportunities and risks associated with the development of DeFi platforms. In particular, the inherent experimental nature of this open-source software landscape was acknowledged as a double-edged sword. On one hand, it allows for rapid innovation and discovery of vulnerabilities, leading to improved security. On the other hand, this trial-and-error approach can expose retail investors, who may lack the understanding to navigate these risks, to potentially significant losses.

There was a suggestion that the industry has an opportunity to use its own technology to create trust layers and "walled gardens" of experimentation, providing a safer environment for retail investors. By ensuring development happens in safer ways, the industry might mitigate the need for heavy-handed regulatory intervention. Currently, there is a perceived unfair risk distribution, with retail investors bearing the brunt while founders often secure their profits early on.

The discussion also highlighted the need for DeFi to take a page from traditional software development practices, where code is developed in controlled environments, thoroughly tested, and any bugs are rectified before deployment. Participants questioned why more DeFi projects are not utilizing test nets and other safer platforms for development, even though it may be more time-consuming and costly.

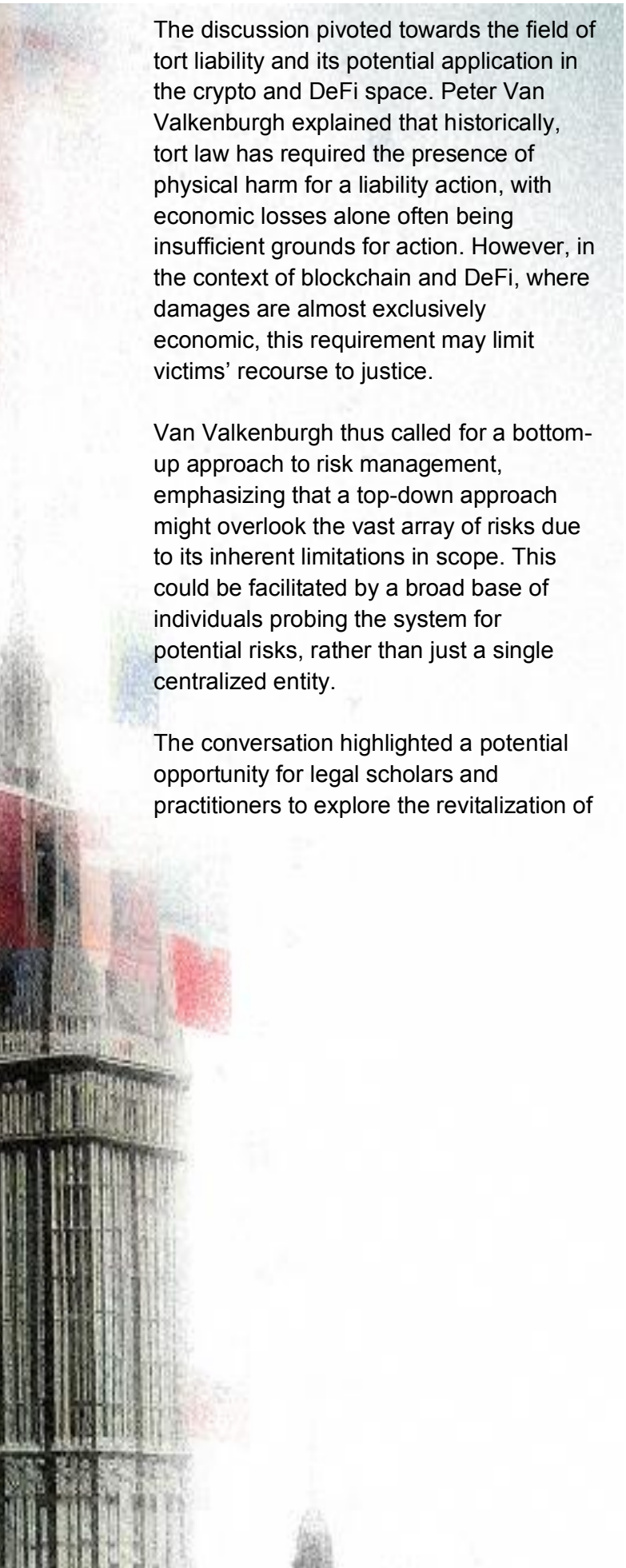
As society becomes increasingly reliant on autonomously functioning code, the consequences of deploying code with potential bugs and little liability need to be carefully considered. The conversation concluded with a call to establish clear signals of trustworthiness as we entrust more and more to these software systems, emphasizing that this discussion should be a priority in the industry.

Standardization as a Regulatory Principle

The roundtable touched on the need for standardization and certification in the digital asset industry, focusing on security and risk management. Some participants acknowledged the importance of these, particularly for digital asset custody services. They also discussed the growing demand for code auditing and the need for more resources and standards in this area. The potential for using blockchain technology to better understand and manage risks in traditional finance was explored.

The International Organization for Standardization (ISO) standards for blockchain technology were highlighted as a helpful tool for achieving this standardization, which some European regulatory authorities use.[7] This comprehensive standard was developed with input from various experts.

The Application of Tort Liability in Digital Assets



The discussion pivoted towards the field of tort liability and its potential application in the crypto and DeFi space. Peter Van Valkenburgh explained that historically, tort law has required the presence of physical harm for a liability action, with economic losses alone often being insufficient grounds for action. However, in the context of blockchain and DeFi, where damages are almost exclusively economic, this requirement may limit victims' recourse to justice.

Van Valkenburgh thus called for a bottom-up approach to risk management, emphasizing that a top-down approach might overlook the vast array of risks due to its inherent limitations in scope. This could be facilitated by a broad base of individuals probing the system for potential risks, rather than just a single centralized entity.

The conversation highlighted a potential opportunity for legal scholars and practitioners to explore the revitalization of tort law to account for purely economic damages, particularly in the field of software development where damages are commonly financial. However, this proposition would not be without its challenges, argued Van Valkenburgh. Enabling a private right of action against developers for financial losses could lead to a surge in frivolous claims or lawsuits designed to suppress public participation.

These potential issues were acknowledged as secondary effects that could be managed if tort liability was reformed to accommodate the digital economy. This specific discussion concluded with a recognition of the importance of providing victims of economic harm with appropriate legal recourse. Rather than solely relying on regulatory bodies like the SEC, victims should have the ability to seek justice through common law and traditional theories of tort liability.

Rethinking Regulatory Frameworks, Approaches & Concepts

In accordance with the Reg@Tech tradition, the participants were divided into four working groups for focused discussions and brainstorming sessions on topics that transcend immediate concerns. The purpose of these breakout sessions was to stimulate thinking, encourage innovative discussions, and develop concrete ideas that advance our understanding in various areas. The goal was to generate new ideas and insights in a collaborative and engaging environment through the experimental and open-ended nature of these breakout sessions.

Each group was assigned a topic and a moderator. The groups had the liberty to diverge from the predefined topics and explore different directions, as long as the discussions remained relevant and useful.

The four topics assigned to the groups were:

- Risk Management: This group was tasked with envisioning risk management practices for blockchain-related projects or platforms.
- Consumer Protection: This group was to explore beyond consumer and investor protection and consider other stakeholders and potential mechanisms to address concerns.
- Same Risk, Same Regulation, Same …? : This topic invited the group to demystify and elaborate on the idea of same risk, same regulation.
- Privacy-Protected Technologies: This forward-looking topic prompted the group to think about policy considerations concerning emerging technologies such as zero-knowledge proofs.

Participants were encouraged to contribute to the group discussions actively. In this section, the report delves into the innovative ideas and concepts developed by the working groups.

Consumer Protection - The “Dojo” Framework

The working group on consumer protection in the context of blockchain platforms and protocols began by discussing various topics such as the bipartisan bill, GDPR, and zero knowledge proofs. The group came up with a set of karate-inspired principles for consumer protection, called the “Dojo” Framework, acknowledging that there is no one-size-fits-all solution.

The principles of consumer protection for on- and off-chain transactions on a blockchain include:

1. Consumer protection should not be lower for on-chain transactions compared to off-chain transactions.
2. Transaction partners should be treated as consumers by default unless proven otherwise.
3. The Dojo Framework, which involves risk education based on karate belt ratings to allow consumers access to riskier assets in a gamified way.

Various ways to categorize assets in a decentralized environment, and the use of embedded supervision in smart contracts as a means of ensuring consumer protection were discussed. The participants also mentioned a regulatory kill switch and emphasized the importance of considering consumer protection in on-ledger transactions. The group touched upon the differences and similarities between public and permissioned blockchains, noting that undoing a transaction on a blockchain is similar to reverse booking in classical bookkeeping. The importance of risk education for consumers in the crypto industry was also emphasized.

A multi-stakeholder platform was proposed, where private actors, and public authorities come together to educate people before they take a test to become potential “samurais”. Once they pass the test, they can choose to go through a safe door or a high-risk-high-return door. The latter requires risk education and due diligence, and disclosures are made available for consumers. The safe door limits the availability of products, with more licensing and regulations.

The challenges of regulatory oversight in the world of NFTs and cryptocurrency were addressed, including the need for individual assessment and the potential for a public permissionless ledger. The concept of a “soul bound token” was introduced as a way to track progress and increase risk as an individual becomes more involved in the crypto world.

Lastly, the idea of creating a universal system for credential recognition in different countries was discussed, comparing it to the rating system for fridges. To implement such a system, regulators, industry experts, and researchers would need to come together to determine appropriate frameworks. However, there are limitations to this idea, and it may limit choice in certain industries.

Risk Management Regulatory Framework

The discussion in this working group focused on risk management in the context of blockchain-related projects and platforms, specifically addressing the CeFi and DeFi industries. Participants in the group explored the challenges associated with implementing traditional risk management frameworks in these unique domains.

One of the significant issues raised in the discussion was the regulatory uncertainty in the United States, particularly concerning anti-money laundering (AML), countering the financing of terrorism (CFT), and Office of Foreign Assets Control (OFAC) compliance. The Federal Reserve has identified bank-level compliance as challenging due to the unique risks posed by cryptocurrency custody, insider threats, and the inability to fully insure the value of accounts. Furthermore, the potential for protocol breaches in blockchain technology introduces additional vulnerabilities that need to be addressed.

The working group identified five key categories of risks associated with cryptocurrencies, such as Bitcoin and Ethereum. These risks include financial, technical, operational, legal and compliance, and strategic risks. Settlement risk emerged as a major concern since traditional banking standards do not address the simultaneous settlement of digital assets against fiat transactions. Technical risks discussed included protocol risk, cybersecurity, and social media risks.

A particular emphasis was placed on the dangers of social engineering and hacking in handling digital assets. The group highlighted the importance of operational risk management, business continuity, and disaster recovery in the cryptocurrency industry. An example was shared in which a Trust Company was hacked after an insider called the police, causing the entire staff to evacuate the building. The participants suggested implementing a living will for digital asset custody banks to provide regulators with instructions on how to operate the institution in case of insolvency.

In the context of the CeFi industry, the group identified challenges such as lack of insurance for customers, operational continuity, third-party risks, legal compliance, consumer protection, and asset volatility. The participants acknowledged that the industry is constantly changing and adapting to new market conditions, which requires a flexible and responsive approach to risk management.

In conclusion, the working group emphasized the need for collaboration between regulators, industry experts, and CeFi organizations to develop and implement effective risk management practices tailored to the unique challenges posed by blockchain-related projects and platforms. As the industry continues to evolve, a proactive and adaptable approach to risk management will be crucial to ensure the safety and stability of these innovative technologies.

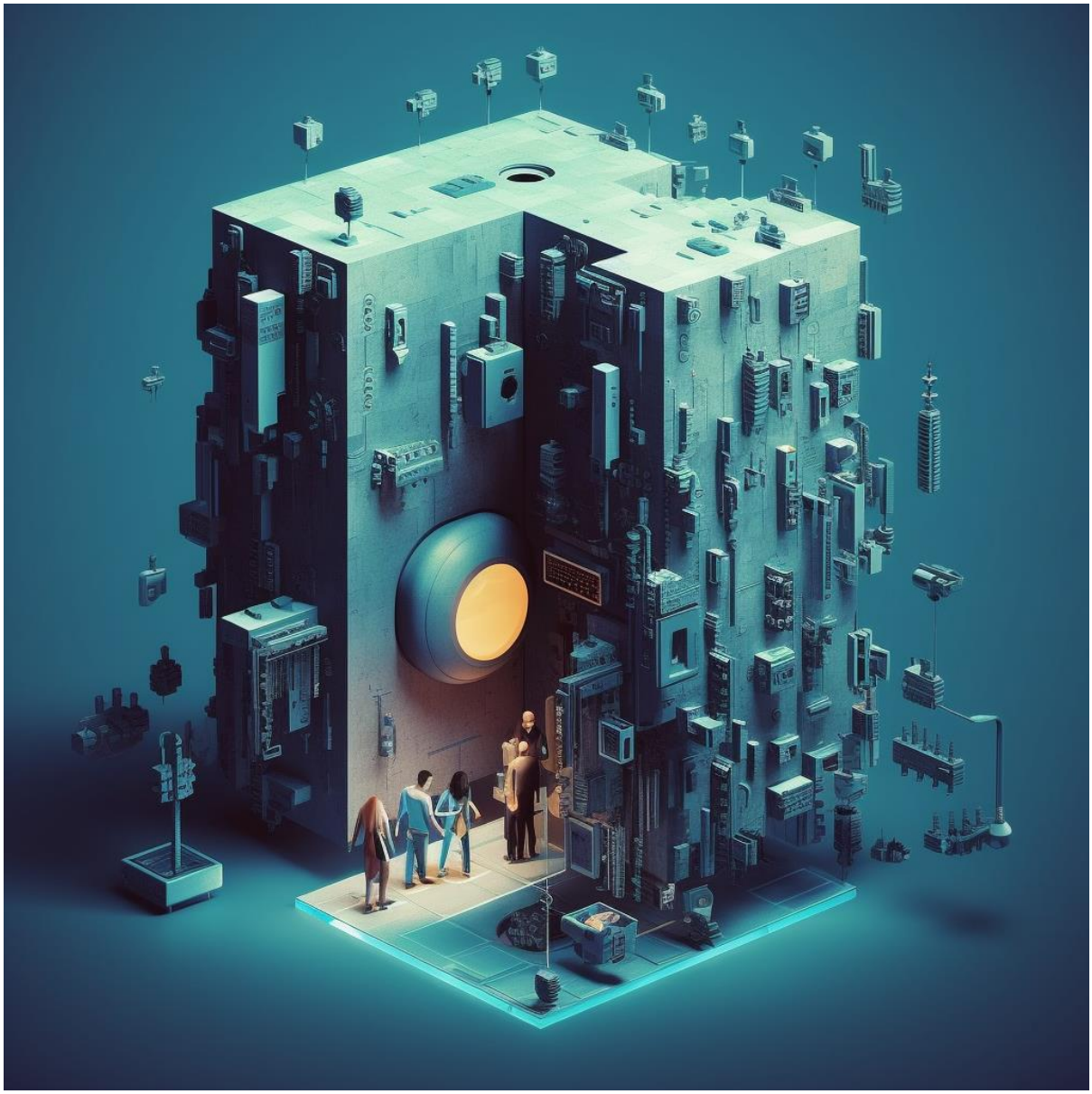
Same Activity, Same Risk, Same … ?

The third working group discussed the challenges of regulating the crypto industry with the same activity, same risk, same regulation approach. They used transportation as a metaphor to illustrate how new risks emerge with technological advances: Risks change depending on the mode of transportation and vehicle concerned, from walking to horses, to wagons, bicycles, trains, automobiles, planes, and rocket ships.[8] In the crypto space, multiple roles are often compressed together, which creates unique features and risks.

To address these complexities, the working group proposed evaluating activities and risks through the lens of disintermediation, contrasting traditional finance with centralized and decentralized crypto entities. They acknowledged that some concepts can be both mitigating and aggravating risks, depending on the context, which calls for a more nimble and nuanced approach to regulation.

The group suggested that legislators and regulators need flexibility to make informed decisions and adapt to the rapidly evolving crypto landscape. They called for tech-neutral solutions that account for the varying degrees of disintermediation in the industry. To achieve this, they recommended empowering regulators to adopt a more flexible approach and engage in dialogue to develop appropriate rules for different situations.

Privacy Protecting Technologies



The working group on privacy protecting technologies convened to discuss the impact of cryptographic mechanisms such as zero knowledge proofs, multi-party computation, and homomorphic encryption on privacy protection. The group explored various aspects of these technologies and their potential role in preserving privacy, maintaining compliance with regulations, and fostering innovation in the digital space.

One major focus was the use of zero knowledge proof-based systems in blockchain technology to balance investor protection principles and privacy while managing and controlling illicit activities. The group emphasized the importance of collaboration between authorities, policymakers, and technology providers in demonstrating effective solutions to these challenges. Standards and onboarding/offboarding procedures for networks were also discussed, with a call for cooperative efforts to ensure the security and privacy of digital assets.

Concerns were raised about the centralization of data and the need for a central authority to validate identities in networks. The group proposed that authorities and policymakers work with the industry in non-adversarial formats to explore technological solutions to address these risks. This collaboration is seen as vital in striking the right balance between privacy and transparency while navigating the complexities of the digital space.

The challenge of achieving political compromise that fits all parties was discussed, particularly in the context of regulating cryptocurrency. A proposed solution involved developing a voluntary, zero-knowledge-based identity system that would allow users to prove they are not on the OFAC list without requiring full identification or outright banning. While acknowledged as a challenging middle ground, this approach could potentially bridge the gap between regulators and the crypto community.

Challenges of credentialing and identity management in the digital age were examined, with an emphasis on individual control of digital identity assets and the appropriate credentials to share. The absence of a dedicated government approach to digital infrastructure in the United States was criticized, and the need for open solutions to digital identity management was underscored. In this context, participants discussed the potential role of governments, the importance of open standards, and the interplay between financial inclusion, cross-border transactions, and privacy concerns. They cited India's implementation of a digital identity system as an example to consider.

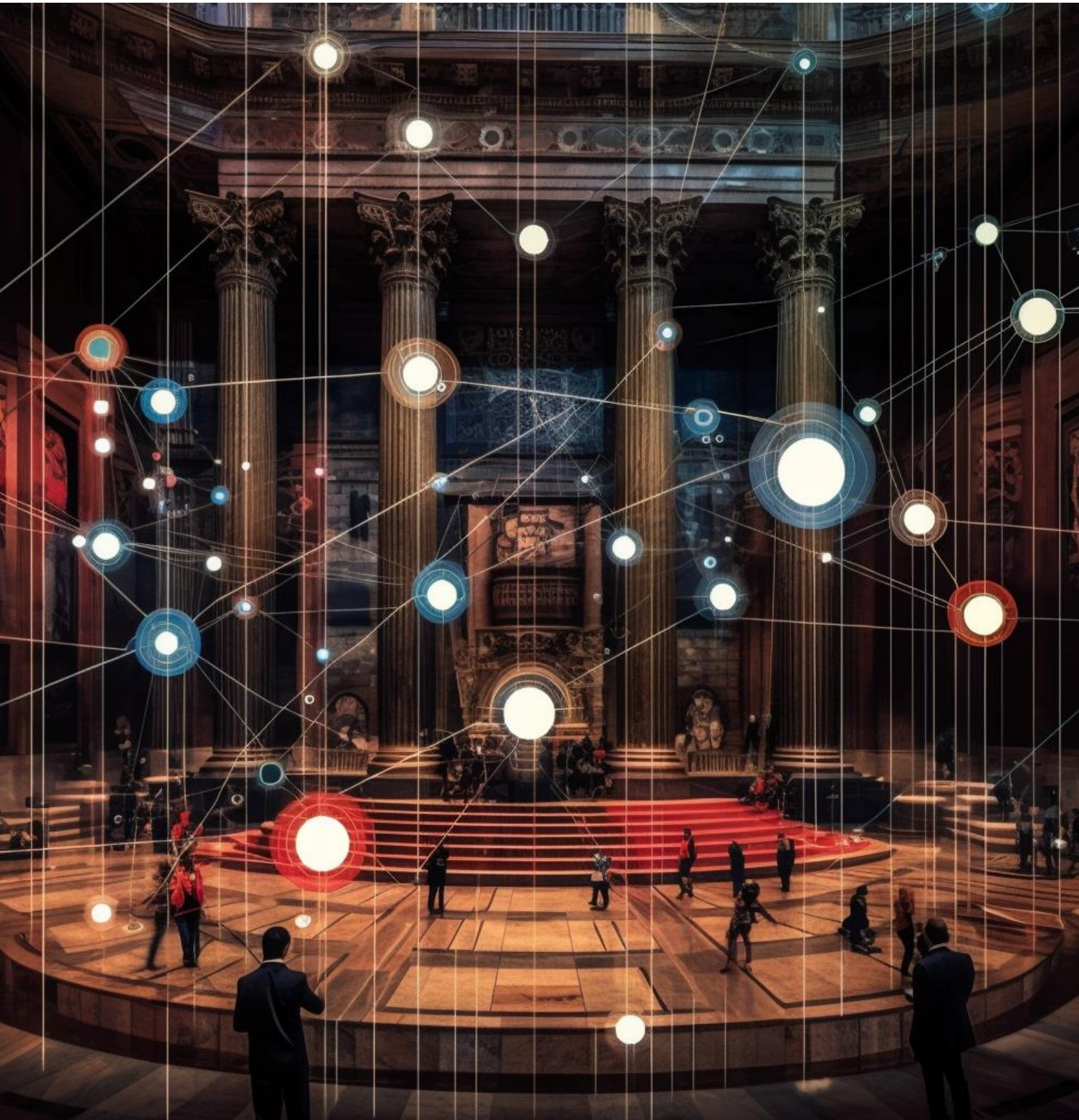
The concept of financial inclusion was discussed as a potential benefit for disenfranchised groups, such as African Americans or Syrian immigrants. While concerns about cryptocurrency being used for illicit activities were acknowledged, participants argued that focusing on social good could lead to positive outcomes. They emphasized the need for a digital identity standard and considered competition between stablecoins and the US dollar as an opportunity for innovation.

The discussion also touched on the current structure of the internet and industrial policy in the US, which fails to address privacy, AML, KYC problems, and other issues. The Improving Digital Identity Act,[9] currently in Congress, was briefly mentioned as a potential solution to some of these challenges.

Lastly, the group discussed the challenges of financial institutions sharing customer due diligence, such as KYC information to prevent duplicative procedures and promote efficient risk management. Information-sharing technologies and artificial intelligence were proposed as potential solutions to this collective action problem, allowing institutions to assess risks individually while cross-referencing data.

Digital Asset Regulation as a Global Phenomenon

One of the key topics discussed during the conference was the global nature of permissionless blockchains and how they create tension with national legal systems. Participants acknowledged that this tension has led to the need for cross-border enforcement and harmonization. They emphasized the challenge of striking a balance between enabling innovation and ensuring compliance with regulatory frameworks. The diverse approaches to regulation by different countries were also highlighted as a complicating factor in creating global standards.



Regulatory Competition, Coordination and Cooperation

Regulatory competition was identified as a primary driver of digital asset regulation. Participants debated the potential for regulatory arbitrage and its consequences, ultimately agreeing on the need for a global framework for crypto regulation. The International Organization of Securities Commissions (IOSCO) was mentioned as an example of organizations working towards such a framework through the formation of a financial task force.

Participants proposed key questions about layer two solutions and technology, emphasizing the need for international coordination and the involvement of institutional organizations in creating global standards. They acknowledged the importance of understanding how different international bodies function within the crypto ecosystem and identified the need for further discussion and guidance.

The lack of regulatory coordination and cooperation across jurisdictions was another major issue raised during the conference. Participants discussed the challenges posed by the offshore US dollar market and the difficulties faced by regulatory agencies in controlling the market. The use and banking of Tether was also brought up as a case study, sparking a lively debate on the effectiveness of centralized international standard-setting bodies in creating homogeneity in policies affecting different players in the decentralized cryptocurrency ecosystem.

Throughout the workshop, participants grappled with the challenges of regulating the digital asset industry. They highlighted the importance of international organizations in creating global standards and the need for clear regulatory frameworks that acknowledge the diverse and evolving nature of the industry.

The concepts of market integrity, investor protection, and consumer protection were central themes in the discussions surrounding digital asset regulation. Participants explored the role of custody rules in safeguarding customer assets and debated the differences in rules between physical and digital assets. They also discussed the legal and regulatory framework for custody of tokenized assets, stressing the need for greater alignment, disclosure, and protection of customer assets.

The conversation also touched upon sensitive data replication and its interplay with enforcement on a national level. Participants discussed the building of regulatory organizations and best practices for supervision in the financial industry, exploring solutions proposed by compliance and RegTech companies. Participants also noted the potential impact of AI on blockchain technology development. They also touched on the potential merger of legal and technological worlds and the need to educate future generations of lawyers and jurists on technology and coding.

BDAP
WHARTON BLOCKCHAIN AND DIGITAL ASSET PROJECT

Paving the Way from Chaos to Order

The discussions highlighted the importance of evolving from the current chaotic state of the crypto industry towards more structured and defined roles akin to the traditional financial system. The early days of the financial system in the United States, for example, were chaotic, with rampant failures and fraud, but over time, the industry figured out a system of functional separation. Exchanges focused solely on providing marketplaces, broker-dealers performed specific roles, and banks had their own functions. This structure of incentives and regulations helped build trust, not in individual entities, but in the system as a whole.

In the crypto industry's early period, there is a fundamental question around whether it is possible to clarify and define similar structural separation. Bitcoin, initially intended as a payment system safe from government control, now exists within a sector filled with a multitude of competing payment infrastructures, lending platforms, investment products, and more. All these different functions are tokenized, making them indistinguishable in form but not essence, leading to confusion and lack of trust.

FTX, for example, as a platform was conducting activities that a traditional exchange would not be allowed to perform. This lack of functional separation and the resulting confusion hamper trust-building and discourage potential users who may be interested in specific services but are overwhelmed by the complexity and opacity of the industry.

The challenge for the industry, therefore, is to grow out of this chaotic stage and establish clear functions for different entities within the sector. By doing so, it can make a stronger case to the public for the use of its technology. This step is crucial, as the majority of the population needs more than just technological excitement to engage with the industry. They need to see that there are safe and comprehensible services available, whether that's a secure investment vehicle or a simple way to send money across the globe.

In conclusion, the crypto industry must work towards establishing clear functional separations and building trust in the overall system rather than individual entities. This will not only foster a healthier environment within the industry but also promote greater public engagement and acceptance.

Conclusion

The ninth installment of the Reg@Tech Roundtable on Digital Assets served as a lively platform for distinguished industry experts, regulatory authorities, and academics to explore key challenges and opportunities within the digital asset landscape.

Our discussion addressed the ongoing developments in digital asset regulation, the practical implications of regulatory frameworks, and the need for global cooperation to craft risk management approaches suitable for blockchain-based platforms. We also focused on crucial customer protection concerns among other pertinent topics.

In summary, the roundtable highlighted the importance of coordinated international efforts, regulatory innovation, and bespoke risk management strategies to navigate the complex terrain of digital assets.

This collaborative endeavor, once again, reaffirmed our commitment to facilitating conversations to better understand, adapt to, and shape the future of the digital asset industry.

Author

Bianca Kremer is the inaugural research fellow at the Wharton Blockchain and Digital Asset Project at The Wharton School, University of Pennsylvania, USA. She holds a Ph.D. in law from the University of St. Gallen.

bkremer@wharton.upenn.edu

Reg@Tech 9 Participants

- Jason Allegrante (Fireblocks)
- Sanjeev Bhaskar (US Department of Justice)
- Tarun Chitra (Gauntlet)
- Peter Conti-Brown (Wharton School)
- Dorothy DeWitt (Office of Senator Gillibrand)
- Jill Fisch (Penn Carey Law School)
- Joey Garcia (Xapo)
- Itay Goldstein (Wharton School)
- Roman Goldstein (Coinbase)
- Keisuke Hayashi (Japan FSA)
- Jorge Herrada (CFTC)
- Linda Jeng (Crypto Council for Innovation)
- Christoph Kreiterling (German BaFin)
- Bianca Kremer (Wharton BDAP)
- Chris Land (Office of Senator Lummis)
- Bill Laufer (Wharton School)
- Caitlin Long (Custodia Bank)
- Max Meizlish (US OFAC)
- Michael Mosier (Arktouros)
- Kevin O'Connor (FinCEN)
- Matthias Obrecht (Swiss FINMA)
- Michael Oh (FINRA)
- Saule Omarova (Cornell Law School)
- Catherine Alden Pelker (U.S. Department of Justice)
- Daniel Resas (Bubbles/Wharton BDAP)
- Joshua Rosenberg (Federal Reserve Bank of New York)
- Mai Santamaria (Dep't of Finance Ireland)
- Lee Schneider (Ava Labs)
- Christoph Simmchen (Gnosis Safe Ecosystem Foundation)
- Valerie Szczepanik (US Securities & Exchange Commission)
- Corey Then (Circle)
- Tomicah Tillemann (Haun Ventures)
- Peter Van Valkenburgh (Coin Center)
- JP Vergne (UCL School of Management)
- Shlomit Wagman (Harvard Kennedy School)
- Kevin Werbach (Wharton School)

Endnotes

[1] The European Parliament approved MiCA on April 20, 2023, see EU Parliament Approves Crypto Licensing, Funds Transfer Rules, Jack Schickler, April 20, 2023, Coindesk, https://www.coindesk.com/policy/2023/04/20/eu-parliament-approves-crypto-licensing-funds-transfer-rules/, see also European Parliament Press Release, Crypto-assets: green light to new rules for tracing transfers in the EU, https://www.europarl.europa.eu/news/en/press-room/20230414IPR80133/crypto-assets-green-light-to-new-rules-for-tracing-transfers-in-the-eu. The Council of the EU adopted MiCA on May 16, 2023. The Regulation was published in the Official Journal of the European Union on June 9, 2023 and will come into force 20 days after publication, see https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2023:150:TOC

[2] For more background information, see Lee Schneider, Chambers Global Practice Guides Fintech 2022 Introduction, https://gpg-pdf.chambers.com/view/907350905/6/; see also David J. Kappos, Lee A. Schneider, Daniel M. Barabander, Callum A.F. Sproule, Fuzzy Tokens: Thinking carefully about technical classification versus legal classification of cryptoassets, Berkeley Technology Law Journal, 2023, https://btlj.org/wp-content/uploads/2023/03/Kappos_WebFile_02-28-23.pdf.

[3] See IRS guidance, March 21, 2023, https://www.irs.gov/newsroom/irs-issues-guidance-seeks-comments-on-nonfungible-tokens. This interim guidance, pending comprehensive guidelines, invites public comments on NFT characterization.

[4] See Cambridge Bitcoin Electricity Consumption Index, https://ccaf.io/cbnsi/cbeci.

[5] See Peter Van Valkenburgh, Report – The Need for a Federal Alternative to State Money Transmission Licensing, Coincenter, January 2018, https://www.coincenter.org/the-need-for-a-federal-alternative-to-state-money-transmission-licensing/.

[6] See European Blockchain Services Infrastructure, https://digital-strategy.ec.europa.eu/en/policies/european-blockchain-services-infrastructure.

[7] See ISO/TS 23635:2022, https://www.iso.org/standard/76480.html.

[8] The working group also showed a picture of the sculpture by Karl Bitter called “Spirit of Transportation” with the quote “The spirit of transportation is represented in triumphal procession of progress led by a little child carrying a model of an airship, a prophetic vision of a mode of transportation to come”.

[9] See Improving Digital Identity Act of 2023, https://www.congress.gov/bill/118th-congress/senate-bill/884/text.

BDAP

WHARTON BLOCKCHAIN AND DIGITAL ASSET PROJECT

Published by the
Wharton Blockchain and Digital Asset Project.

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