BDAP

WHARTON BLOCKCHAIN AND DIGITAL ASSET PROJECT

# Quo Vadis Digital Asset Regulation?

## The Seventh Reg@Tech Roundtable on Digital Assets

June 2022

Wharton
University of Pennsylvania

# Foreword

Reg@Tech 7 was the first in-person meeting of our global roundtable on digital assets since the pandemic lockdowns started in 2020. It reinforced that, as useful as virtual meetings can be, there is something irreplaceable about the interaction that happens when a group of people share the same space. Given the tremendous evolution of the digital asset world, we included new participants and topics, along with some of both that were part of Reg@Tech when it started in 2017.

This report summarizes key discussions and learnings from our conversations in Philadelphia in March 2022. For the first time, we conducted a scenario planning exercise, in which groups built up for distinct visions for the future of digital assets. The activity was so fruitful that it deserves its own report. You will find a brief overview here, and a full discussion of the scenarios in a subsequent paper.

Envisioning the future is important for making decisions in the present. We can never be sure where the world is going, especially in an area as fast-changing and multi-faceted as blockchain and digital assets. Listening to diverse perspectives and projecting what might occur under different assumptions is our best bet for thoughtful policy-making, regulation, and business decisions. Reg@Tech will continue to provide such a platform.

**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 the main topics of discussion at Reg@Tech 7 and relates them to relevant recent developments. 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.*

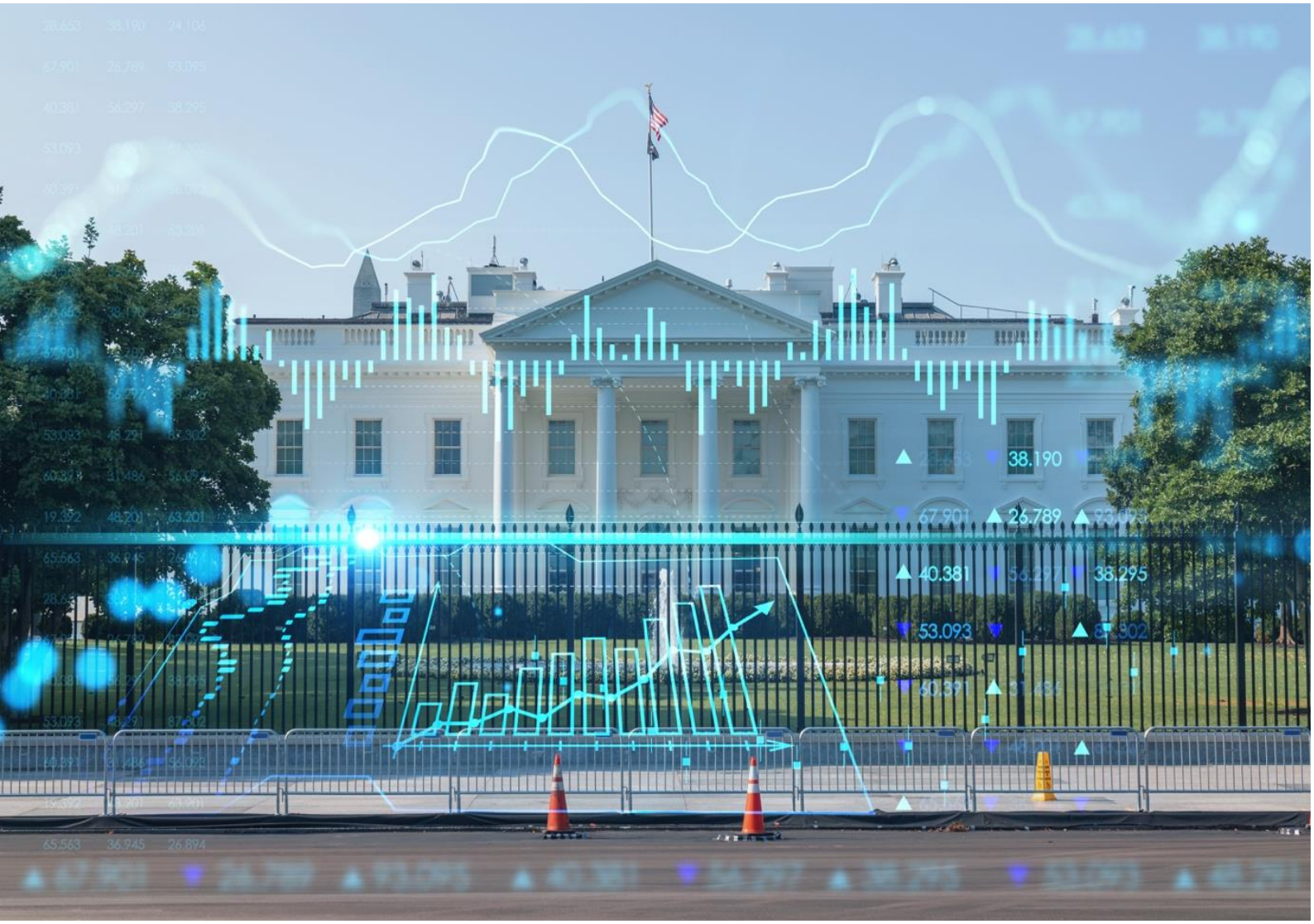
# Introduction

Major digital assets-related regulatory action plans have recently been announced around the world. There are several factors leading to these developments. The market capitalization of digital assets exploded, surpassing $3 trillion in November 2021. A growing number of people own cryptocurrencies, and most countries are exploring central bank digital currencies (CBDCs). Digital assets are becoming mainstream in many ways. However, there remain substantial regulatory uncertainties and risks posed to consumers, financial stability, national security, climate, and other important (inter)national interests.

The topic of the seventh iteration of the Reg@Tech Roundtable was "Digital Assets and the Future of the Financial System". Leading up to the roundtable, there were two major public policy developments. In the United States, the Biden Administration issued an Executive Order (EO) on "Ensuring Responsible Development of Digital Assets" on March 9, 2022.[1] The EO outlines for the first time a "whole of government" approach to addressing the risks and harnessing the potential benefits of digital assets and their underlying technology. Meanwhile, the European Parliament adopted its position on MiCA, the European Markets in Crypto-Assets regime first proposed in 2020.[2] MiCA seeks to introduce a harmonized framework for digital assets in Europe beyond existing securities regulation.

The roundtable included presentations from White House and European Commission officials on these developments, as well as perspectives from active participants in the policy development process on both sides of the Atlantic. Aside from these major developments, the roundtable also discussed the intersection of regulation and decentralization, tracking many important issues, such as how to future-proof regulation, challenges regulators face, the need for coordination at a global level, and the instigation of regulatory sandboxes. A major focal point of the discussion was on digital identities and their importance for growth of the digital asset economy. Russia's invasion of Ukraine also heightened the stakes on ensuring financial sanctions can be carried out, creating further pressure for a robust digital identity framework. However, the more our social and financial lives shift to the Internet, the greater the risk to privacy. Striking the right balance is a major challenge.

# Recent Developments




## United States – The Biden Administration's Executive Order

The six key priorities and policy objectives highlighted in the Executive Order are (i) to protect consumers and investors, (ii) to ensure financial stability, (iii) to prevent illicit finance, (iv) to reinforce US leadership in the global financial system, (v) to ensure economic competitiveness, financial inclusion, and safe and affordable financial services, (vi) and to promote responsible innovation. The EO creates an overarching vision and directs various agencies and departments to produce a series of assessments and frameworks for digital asset regulation.

Notably, the Executive Order establishes an Interagency Policy Committee (IPC) that is co-chaired by the National Security Adviser and the Assistant to the President on Economic Policy. This approach combines the efforts of several agencies with various types of authorities in order to ensure not only that a clear regulatory regime is developed, but also that other tools the US government has at its disposal are brought to the table in a mutually reinforcing manner.

The role of government in facilitating innovation was highly debated during the roundtable. For example, in the US, some state governments have a formal mandate for innovation, whereas most federal agencies do not. However, innovation mandates can clash with other policy goals. Legislatures can help by providing clear priorities between different policy goals but doing so is challenging because so much depends on the context. Even without an official innovation mandate at the federal level, some objectives in the Executive Order are clearly intended to promote innovation. Even though there has been significant fintech development and financial innovation in recent years, much of it involves high-tech frontends like Venmo or PayPal that hide rickety financial rails. In the words of one participant, "it might look like a Ferrari, but on the backend, it's horse and buggy". A mandate for innovation can pave the way for addressing the underlying infrastructure of the financial system. However, it could also open the door to political pressure, as powerful interests seek to advance their own objectives.

# European Union – MiCA Regulation and Proof of Work Debate

The European Union seeks to implement a comprehensive regulatory approach to crypto-assets that is balanced, at the same time closing the loopholes, creating incentives for the industry to be innovative, but also taking regard to the risks, especially regarding stablecoins and trading of securities. Much like in the US, the starting point for the European regulatory discussions was related to whether a specific token could be regarded as a security. However, in the European Union the concept of security can be interpreted differently in EU member states, where the same token could qualify as security in one member state but not in another, jeopardizing the harmonization efforts underway.

The legislative process on the proposal for a Regulation on Markets in Crypto-Assets (MiCA) is underway.[3] In addition, the European Union seeks to enable easier market access for blockchain technology. The second legislative proposal thus seeks to create a *Pan European regulatory sandbox* for using DLT in trading and post trading of securities. This proposal allows for an exemption from some rules, which typically apply in securities markets, but which do not fit distributed ledger technologies (DLTs), in particular for central clearing depositories.


Although the MiCA regulation as an instrument to protect the integrity of financial markets is not necessarily an instrument for climate protection, concerns surrounding the detrimental environmental impact of proof of work due to the amount of computational energy necessary have significantly influenced the discussions in Parliament. A proposal before European Parliament's Committee on Economic and Monetary Affairs on March 14, 2022, to ban proof of work-based crypto assets, was narrowly defeated.[4] An alternate proposal was adopted by Parliament that would direct the European Commission to put forward a legislative proposal to incentivize the industry to migrate from proof of work to proof of stake.

In this context, there is a potential conflict. While some take the view that more environmentally-friendly consensus mechanisms such as proof of stake could lead to centralization and control of networks by those who hold the most assets, others, however, see oligopolistic tendencies precisely in the non-environmentally friendly proof of work blockchains. Thoughtful balancing and weighing of different network designs and their consensus mechanisms, as well as their implementation issues, will become more important. Data-driven decision-making is desirable but may prove

difficult due to the nascent nature of the technology. Still, equating proof of work with "democratic" and proof of stake with "less democratic" is too simplistic.[5]

Another point of tension identified was AML and identification. In light of the current Ukraine crisis, the need to identify counterparties in financial transactions is particularly evident and can be seen as one of Europe's priorities. The EU is in the process of revising and implementing the latest recommendations of the Financial Action Task Force (FATF). One challenge in the EU is to meet the requirements for transferring very detailed personal data to countries that do not necessarily have the same high standards of data protection as required by the General Data Protection Regulation.

# The Journey of Digital Assets

After examining these recent developments, the discussion at Reg@Tech 7 took a longer-term perspective on the evolution of the digital assets and the regulatory debates surrounding them.

When a new technology emerges, it is only natural that understanding it properly takes time. Blockchain technology seems to demand a particularly steep learning curve. This is partly the case because blockchains are multidisciplinary as they combine expertise from many different knowledge fields. In addition, they challenge societal belief architectures and force rethinking in various domains, from *what money is* to *what assets or digital assets in general are*. Discussions of this nature require open-mindedness.

In sketching the development leading up to the *status quo*, since the launch of Bitcoin, there have been four major developments, depicted as follows:

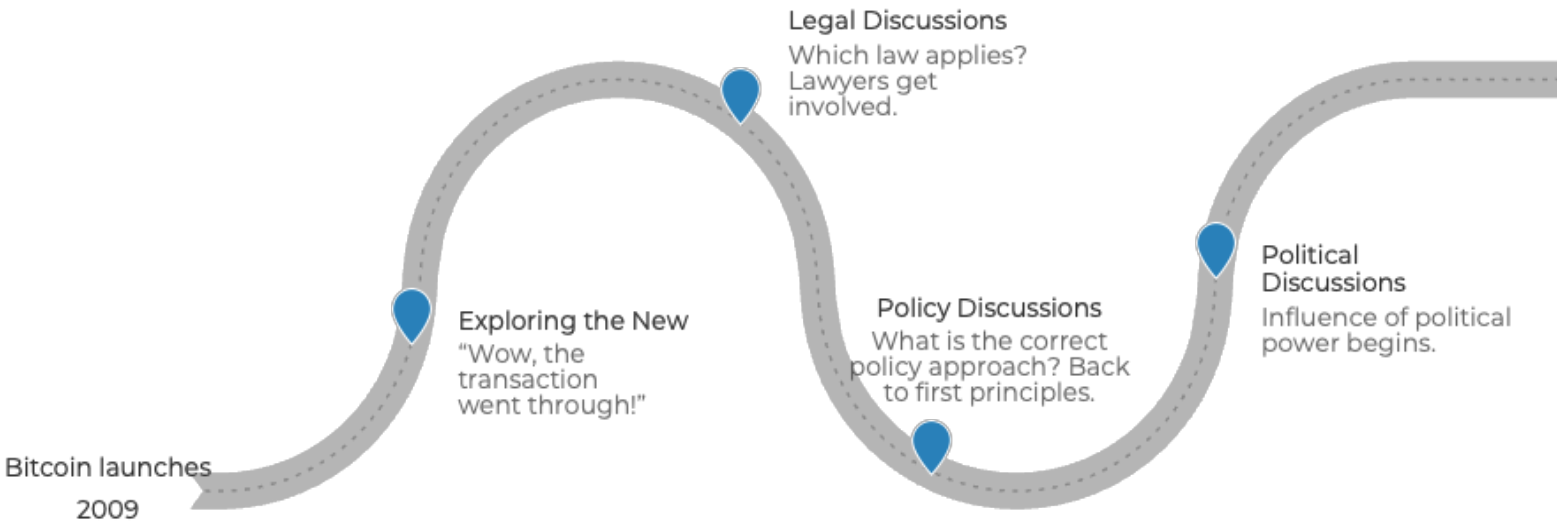



*Figure 1. Milestones in the Journey since Bitcoin's Launch*

In the first phase "Exploring the New", early adopters of the technology, curious-minded individuals, and technical experts experimented with Bitcoin and its blockchain. This phase is characterized by trial and error, enthusiasm when things worked, and most of all, curiosity.

The second period is marked by government enforcement, legal discussions, and increased lawyer involvement. The initial period has passed, and from an online game played by outsiders, libertarians, and cryptography enthusiasts, blockchains have started to become serious business. The next period is one of legal queries and actions brought against crypto exchanges and individuals, whether it be the closing of the darknet marketplace Silk Road or the sheer amount of Ponzi schemes, scams, and investor fraud, which found a peak during the Initial Coin Offerings (ICOs) craze, facilitated by the ease of creating tokens.

Many projects and startups started to seek assistance in setting up their company structures. A famous example is the Ethereum Foundation which was established in Zug, Switzerland. Much remains in the dark, and legal certainty is far from being reached. The technology is global but legal discussions remain within the borders of countries' jurisdictions. Some jurisdictions, such as Switzerland, Liechtenstein, Singapore, Gibraltar, and others take advantage of this fact and begin attracting crypto startups to set up shop under their regulatory regimes.

From a mere mailing list curiosity that started with Bitcoin, blockchains have begun to proliferate in a manner that could no longer go unnoticed. The third period is characterized by policy considerations. The correct policy approach is being contemplated worldwide, while some countries take a strict approach and shut down crypto operations altogether and forbid individuals from trading, other countries start creating friendly and inviting environments, while others again remain in a state of observation, unwilling to take a stand on either side.

Since the onset of the pandemic and the subsequent unprecedented growth of the digital asset market, a new period has begun, one of political power and the balancing of interests. In the United States, the maturation of the crypto industry is reflected in a series of congressional hearings with representatives of the largest crypto companies, government officials of financial authorities, academics, and other institutions. The question is whether the correct policy approach will still be seriously contemplated or whether some interests which have more political power will prevail, regardless of the best possible approach to be followed.

During the Reg@Tech 7 sessions, it was noted that the legacy system itself has many flaws. In the United States, according to the Office of Management and Budget (OMB), $281 billion in improper payments are made each year. And although billions are spent on Know Your Customer (KYC) compliance, there is an estimated $300 billion annually in money laundering.[6] The question raised on the basis of this data was whether it would not make sense to compare what is being built in the digital asset space to the *status quo*, which has some profound deficiencies.

# Future-Proofing Crypto Regulation

A major topic that runs like a thread through all regulatory discussions is how to best design regulation for this rapidly evolving space. A suggestion voiced at one point during Reg@Tech 7 was to forget all existing laws and start with a blank sheet of paper. Next, one would assemble the smartest policymakers and the brightest engineers in one room to draft an entirely new framework based on agreed-upon policy objectives, such as preventing illicit activity and promoting financial inclusion. Attention was drawn to the fact that some old legislation might not be useful anymore, especially since technology has advanced so rapidly. An example given was the Bank Secrecy Act (BSA), which was enacted when people were still using the rotary phone.

A contrary view expressed was that existing laws do not need to be radically changed, but rather that an innovative approach to compliance is needed. One example would be embedded supervision. How could monitoring be built better and in a more holistic manner into the actual transactions themselves to meet certain safety standards? Another suggestion given was that regulators could work with validators on blockchains to combine the function of using tokenized information about individual users so as to enforce KYC and AML norms.

# Technology-Enhanced Regulation, Compliance, and the Need for Resources

Some suggestions on regulatory technology (RegTech) were made. Regulators need to carefully consider and approve viable RegTech-type solutions and innovations developed by engineers. One discussant noted that policymakers should incentivize the production of such products to make the whole ecosystem more inclusive and safer. A question raised was how to scale requirements, oversight, and enforcement in this space in a prudential manner.

A widespread concern was whether government had sufficient resources to enact its policy objectives. The best regulatory approach may not succeed if resources are missing. Thus, a considerable challenge is the lack of sufficient resources to acquire the level of technical expertise needed to get knowledgeable and up to speed about the technology. Furthermore, examiners may not be comfortable dealing with this new technology. The crypto industry has grown into organisms that regulators are not used to regulating and are not used to seeing with a vertical stack of services and products provided by one entity. Participants largely agreed that the public sector thus needs more expertise and excellent educational material of which there is not enough.

However, one must keep in mind that not everything needs to be regulated, careful consideration needs to be given as to what to regulate. An opinion voiced during roundtable discussions was that regulation seems to be most required in two instances:

- When there is the worry that new developments may implode the traditional financial system.

- When the virtual markets activity directly affects real people and jobs and if there are security implications.

Regarding compliance with the law, a question was raised as to what policymakers and regulators could do to partner with the private sector and what incentives for good behavior could look like.

## Coordination at a Global Level

There was general agreement that an international collaborative effort is needed to ensure responsible innovation for digital assets. International alignment for crypto regulation is beginning to surface, which means the development of rules that have some commonality across jurisdictions. These efforts include the investigation of illicit activity, holding entities accountable, and tackling the complexities of international jurisdiction by enforcing the Financial Action Task Force (FATF) standards, standards to enhance anti-money laundering (AML), and countering financing of terrorism (CFT). A joint statement was released by President Biden and President von der Leyen, which announced: "deeper collaboration to combat the illicit use of digital assets, including their potential misuse in evading multilateral sanctions imposed in response to Russia's unprovoked military invasion of Ukraine".[7]

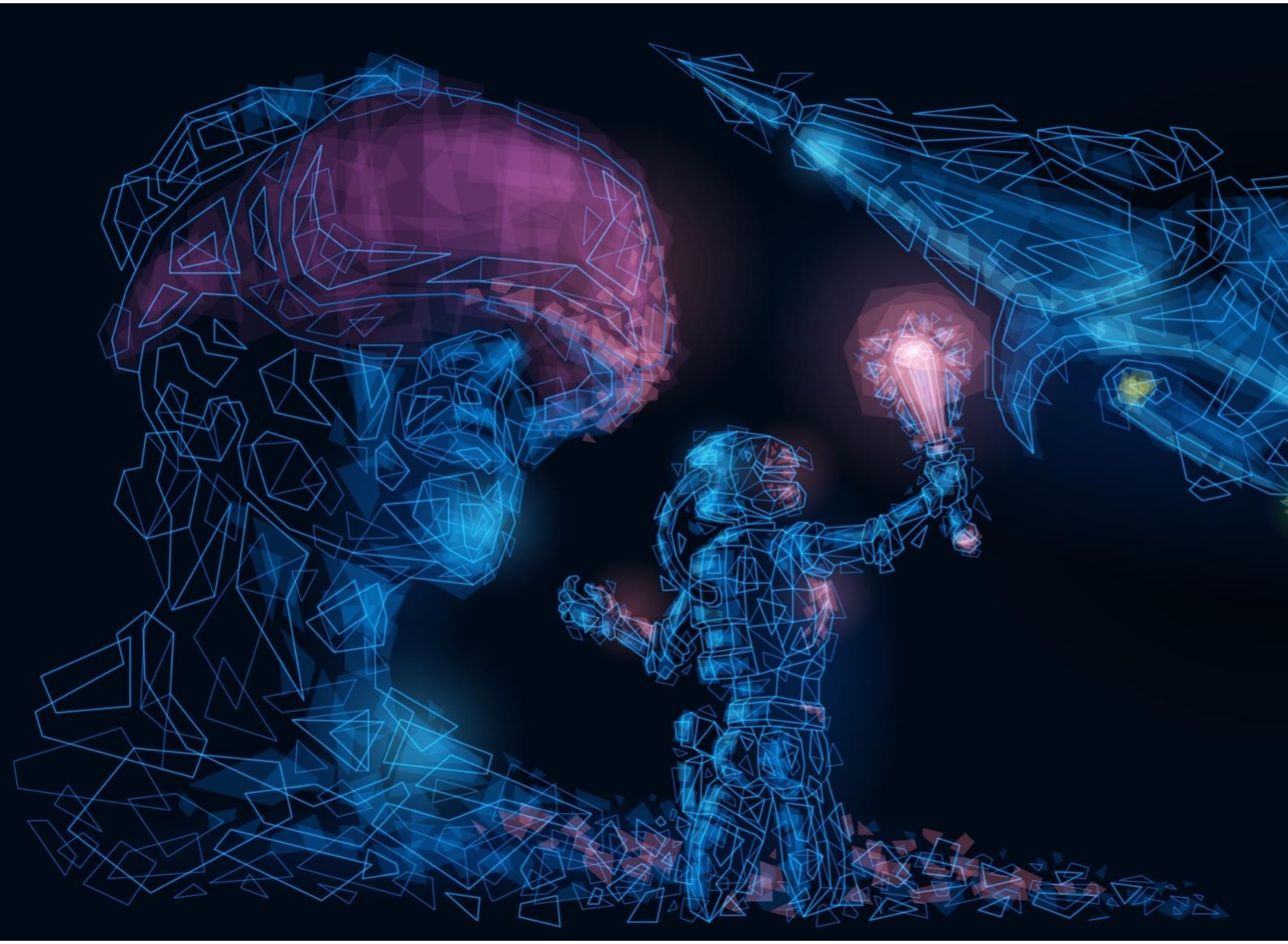
Moreover, the Executive Order released by the Biden Administration specifically recognizes that an international engagement framework, as well as partnership with industry, is critical for accomplishing every single of its objectives. The US is seeking to continue to enhance that collaboration through law enforcement channels, regulatory and supervisory channels, diplomacy, and other efforts. All these elements implicate necessary partnerships with like-minded nations and ensure that democratic principles are built into these financial systems to combat authoritarian exploitation and other undesirable results. There is recognition that necessary partnerships need to be established with the industry as well to ensure that desirable features are integrated into the financial platforms.

# Regulatory Sandboxes

A global cooperative effort could extend to regulatory sandboxes. There are a lot of sandboxes at the state level in the US, the UK, and now the European Union. Regulatory sandboxes are a way to give startups a chance to explore fintech innovations and test them out in a less stringent regulatory setting. Regulatory requirements may be lifted temporarily, such as legal and licensing requirements, or in the case of "hubs", requirements are not lifted, instead, startups receive guidance.

Startups generally have a difficult time competing with established banks that have big legal departments and are used to handling financial regulatory rules. Some argued that such sandboxes enable a level playing field by helping young innovative firms understand the complexity of the financial regulatory set. While such experiments were generally supported, some expressed concern and questioned the need for sandboxes by stating that "adults get a license, and kids play." They suggested that companies could apply for a license or do what is needed to obtain full regulatory clarity rather than "play in the sandbox".

Sandboxes face significant risks, which include favoritism, unfair advantages for companies within the sandbox, manipulation of the marketplace, tampering, and ambiguity.[8] There are different ways to mitigate such risks, including publishing detailed reports on all the use cases within the sandbox, all learnings, and findings, which can then be shared openly.



# A Gamified Universe and Non-Fungible Tokens

The digital asset space is developing into a "gamified universe" or "metaverse", which is growing and becoming more complex. However, what is the metaverse exactly? And is there more than one? Participants discussed the idea of games becoming worlds and the "gamification of everything", including the proliferation of Non-fungible tokens (NFTs) and the move from web2 to web3. In the web2 era, people are sliced into smaller groups for the targeting of advertisements. The vision of web3 is that functional, vibrant, dynamic communities will instead create value that is shared more extensively and fairly with participants. Some participants argued that, despite the prominence of financial motivations, the heart of the crypto ecosystem remains the community aspect, as seen in the growth of decentralized autonomous organizations (DAOs) and other developments.

That crypto universe is almost boundless and abundant. All kinds of goods can be created in the digital space without being subject to the same restrictions as in the "real world". Valuations of NFTs have reached record-breaking numbers. The question is at what point must the big and important public policy choices be made. As investors pour hundreds of millions of dollars into buying digital real estate, the question becomes: What does it mean to buy digital real estate? The lines keep blurring, not only between the real and virtual worlds but also between what's a game, what's an asset, and what's space to host activity?

Several more questions were raised, such as how are these new digital assets part of real companies and the real economy? What are the laws and rules for the metaverse? A metaverse system, where mainstream brands create digital collectibles that can be used in a system and even in-between multiple systems, implicates many unresolved questions. Moreover, if these systems remain completely private, the question arises as to how they will provide for public goods. We may need to rethink how to provide for the real economy and facilitate capital formation beyond the digital world.

Global banks face similar challenges as they contemplate offering digital asset-linked products to their customers. They may need to rethink the entire onboarding procedure, as someone may be a resident of country X when opening the account or when onboarding but may have relocated to country Y when performing the transaction.


# Connecting Decentralized Autonomous Organizations to the Legal System

An important concern voiced was that there is no common understanding of many concepts, including Decentralized Autonomous Organizations (DAOs), the metaverse, and others and that definitions are generally lacking. Questions were raised related to what an optimal legal structure for DAOs could look like and how DAOs should be structured for a metaverse, where people could potentially be spending a lot of their time in the future. Also, participants discussed the notion of "decentralization" and agreed on the need for viable metrics to grasp what decentralization effectively means.[9]

A hard and complex question remains: what is the appropriate regulatory framework for these phenomena?

Two states in the United States are taking the lead in figuring out how to integrate DAOs into the existing legal system, one is Colorado with its cooperative law and the other is Wyoming with its DAO LLC law. However, under neither of these two approaches can a DAO be truly decentralized. In each case, there needs to be a control person in the US, making it possible for the legal entity to pass KYC requirements.

One could argue that if a DAO wanted to achieve true decentralization, it would have to abstain from registering, in which case there would be no connection, no control person, and no possibility to open a bank account. During the discussions, the point was made that if a DAO never registers, there may potentially be no viable means to restrict it by regulators.[10] Regulation can be restrictive or enabling (defining and giving legal status). Many regulators and policymakers do not understand the technology well enough to understand that restricting any given activity even if they wish to do so may not be entirely possible. It was thus suggested that providing projects an incentive to register under now developing frameworks would be a better way than going the route of restricting them because by providing incentives to register, DAOs can have limitations of liability and access to the traditional financial system.

The Wyoming LLC concept is said to be designed to adapt to the reality of what a DAO is, which is that its operating agreement is not in analog form but in code form. In such a case, the law says that if a dispute arises, the judge must use the code as the source of the governing control for the legal entity. This resulted in a debate on the infamous *The DAO* incident. "The DAO", supposed to be the first operating DAO, was created in 2016. It raised about $150 million in ether in a short amount of time to create a collective investment fund.[11] However, a vulnerability in the DAO smart contract was exploited.[12] The series of events that unfolded subsequently led to an Ethereum hard fork to return the funds.

Participants debated what would have happened in 2016 if *The DAO* had registered under Wyoming law. Would the hacker have won before a judge due to being able to rely on the code? What would it mean for a judge to have to decide based on an operating agreement defined in code?

One issue is the distinction between having control and having ownership of a digital asset: Just because someone was able to control the asset under the code does not mean that they have gained ownership of the asset under private law, which is a legal concept. One could argue that ownership would have remained with the DAO even if the asset had been transferred to the hacker's wallet. For legal analysis, one would have to discern what the code provides and apply laws and legal concepts by

analogy. But each case may be different, and in the case of *The DAO*, it could be argued that the person who is often referred to as "the hacker" did exactly what they were authorized to do since the creators of *The DAO* set the terms in advance and made clear that the code would prevail. In the end, it boils down to the interpretation of the terms of *The DAO* code as to whether the withdrawal of assets, as permitted by the code, also implies a transfer of ownership. This debate shows that our legal understanding of blockchain technology-based innovations is still in its infancy. *The DAO* incident happened six years ago, yet there is no widespread consensus since no court has ever taken a stance on this issue.

# Digital ID as the Key to Unlock Web3

Although the hacker's identity in the DAO incident may have recently been revealed, a common feature of blockchain transactions is the ability to remain pseudonymous without having to identify oneself to the counterparty, which raises concern in relation to AML and CFT. On several occasions during the discussions, the roundtable thus focused on the issue of identification. An official identity is a prerequisite to almost any interaction in modern society, from school enrollment to opening a bank account, to accessing healthcare, to voting, marrying, or traveling cross-border.[13] Digital identification enables authentication by digital means and can be seen as a key to unlocking many benefits.

A report published by the Center for Digital Development at the United States Agency for International Development (USAID), states that "in many ways, the roughly 1.1. billion people who lack official identity are invisible, discounted, and left behind".[14]

Aside from giving access to a host of services to the many currently excluded individuals, digital IDs also have the potential to save billions of hours in government services and associated costs.[15] However, there are also many risks associated with a digital technology-enabled ID system, such as system failure, hacks, privacy infringement, and misuse. Data in motion is much less secure than data at rest.

Even in traditional finance, there is a rampant amount of synthetic identity fraud, which points to the fact that identities are not being verified properly upfront. Strengthening identity is something that can benefit all parts of the financial sector as well as other sectors that are affected by fraud. Since individuals can self-custody their digital assets and hold their own keys to their funds without needing any traditional intermediaries, they might need to identify themselves to authorities in the network as opposed to intermediaries identifying their customers. The European Union is presently developing a standard for digital identity wallets in the EU and a technology toolkit that all Member States can use to issue such digital identity wallets to citizens.

There was widespread agreement among the roundtable participants that a digital identity or a "decentralized identity" will be the cornerstone for all digital services. It is true that identity is critical to any risk-based AML/CFT regime. However, digital identities will have implications beyond AML and can ensure that financial sanctions can be carried out. Digital identity is key not only to using crypto assets in a legitimate way, but also for web3, and for all the value-added functionalities of the internet. One of the major benefits of digital identification is access to financial services and thereby attaining the objective of financial inclusion. With a proper design architecture and risk-mitigating incentives, digital IDs can be powerful tools for significant economic and noneconomic growth and benefits.[16]

One of the concerns raised was control over personal data and privacy issues. There is optimism that privacy-enhancing technology will provide effective solutions for credentialing without having to share one's personal information. A digital identity would be beneficial in order to hinder the proliferation of one's information in many different places one may in the end not even be aware of. A way to ameliorate this would be to allow banks, financial institutions, and crypto exchanges to rely on third-party attestations like digital/decentralized identities. In the United States, the Customer Information Protection rule requires each bank to have to duplicate the verification of each customer, and copies of personal information at each bank account.

A question posed was how to create a privacy-preserving data architecture that is going to enable us to compete effectively with a true 21st-century infrastructure in the future. There is a delicate balancing act that needs to be attained between surveillance to

combat illicit finance and preserving privacy. The prospect is that the maturation of at least four different technologies (federated learning, zero-knowledge proofs, differential privacy, homomorphic encryption) that have grown largely separately, could together form a robust privacy protection architecture.

# The Future of Digital Assets

After discussing recent developments and current challenges, one of the big questions this roundtable addressed was what the digital asset space will look like in the future. There is a general sense that the global financial system in a digital age will rely heavily on digital assets.

In a Scenario Planning exercise, roundtable participants had the opportunity to take the time to step out of their current reality and envision prospective futures. In preparation for the exercise, participants were first asked to identify uncertainties in four main categories: What political, economic, social, and/or technological developments are uncertain today and could be relevant to the state of the crypto economy in 2035?

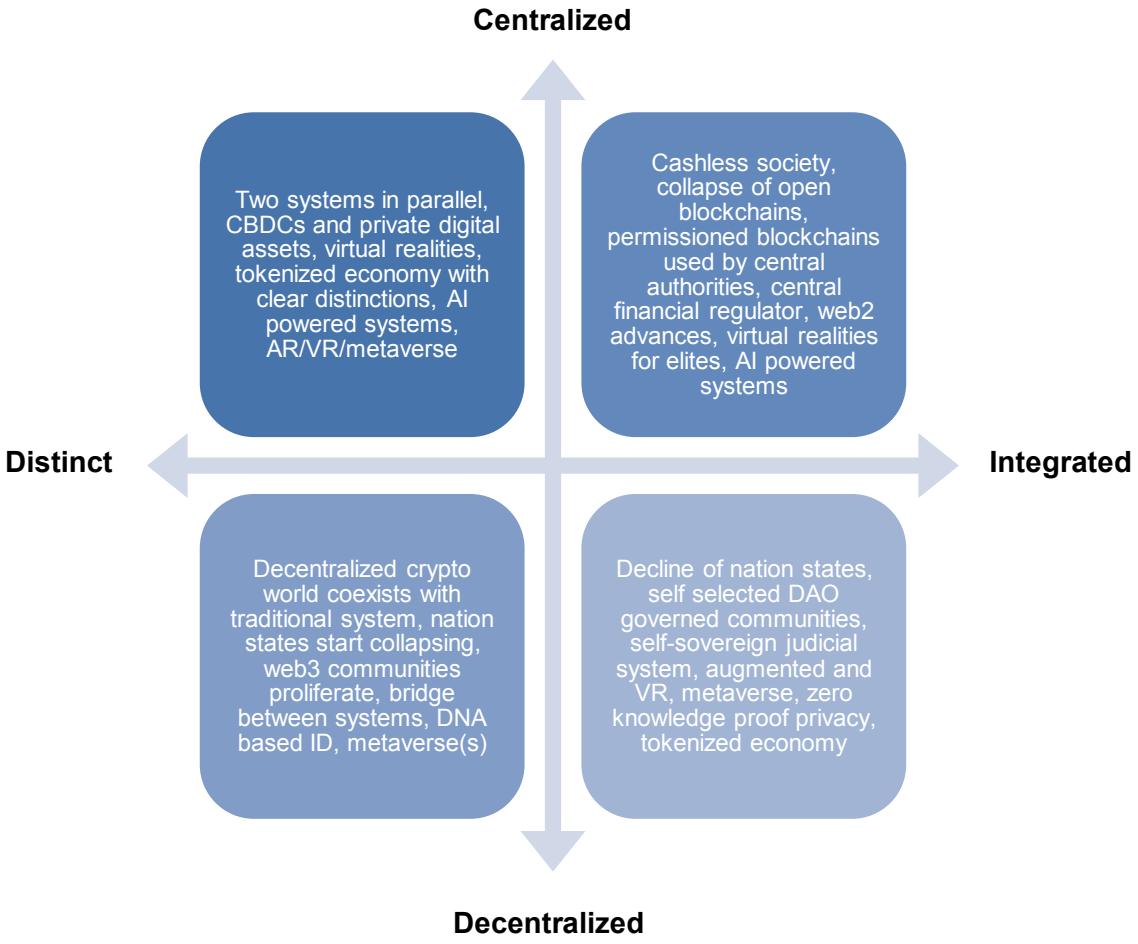
Some of the political uncertainties that were discussed during this session included the risk of partisanship and polarization, globalization vs. nationalist movements, dictatorships and unstable regimes, instability, and sudden collapse of geopolitical powers. In terms of economic factors, some of the uncertainties were the rise of tokenization and virtual economic web 3 ecosystems (metaverse) and what effects that may cause, potential collapse of major fiat currencies and its implications as well as the possibility for the occurrence of another major financial crisis.

Social factors contemplated were personal freedoms, virtual identities becoming more valuable than real world identities, greater wealth inequality, introduction of universal basic income, social scoring, end or revival of religions, and possible alterations of DNA, leading to a change in human lifestyle trends and demographics. Among the many technological uncertainties discussed, were, for example, the effects of quantum computing on blockchains, perfect deep fakes, artificial wombs, technological breakthroughs that lead to a voice empowered device-less world, advancement of artificial intelligence, and singularity.

After this initial exercise, participants were split into four groups along a matrix of four quadrants (centralized vs. decentralized, distinct vs. integrated), and asked to time travel to the year 2035. Each group was then tasked to contemplate what the future digital asset world in 2035 may look like and what factors influenced that outcome.

| Centralized vs. Decentralized | Distinct vs. Integrated |
|---|---|
| Is the world going to be radically more decentralized than it is today or is it going to be less so? Is it going to look a lot more like there's control by central intermediaries? | The digital asset world and the established financial system - will those be two things or one thing? Will they be distinct or integrated? |

The following graphic summarizes some of the key aspects of each scenario.




In all scenarios, technology advances rapidly and some sort of metaverse or AR/VR enhanced reality extends beyond what we can imagine today. In the centralized spectrum, the two envisioned scenarios turned out rather negative, one descended into a fascist scenario, the other into a highly centralized system with considerable disadvantages. Nation states still very much exist in the centralized worlds, not, however, in the two decentralized ones, where instead digitally networked communities flourish. Whereas in the decentralized spectrum, the outcome was not as gloomy, the scenarios faced several challenges in terms of appropriate governance structures and widely accepted privacy-preserving digital ID systems.

From all the potential scenarios that could have been envisioned, it was intriguing to see what each group came up with. Since participants come from different parts of the world, the discussion was informed by a global approach, which is beneficial, especially since the technology is global in nature.

A subsequent report will describe the four scenarios in greater detail.

# Conclusion

Reg@Tech 7 participants not only looked thirteen years into the past to when Bitcoin launched and reflected on the journey of digital assets so far, but also took a snapshot of current developments in two important parts of the world, and then set out as time travelers on a journey to the future thirteen years away.

A visitor joining the discussions midway may have mistaken the workshop for a science fiction movie screenwriting exercise. Especially once we started talking about gamified multiple universes, digital avatars, multiple identities, DNA enhancements, and combining blockchains with artificial intelligence. However, commonplace technologies in the present often would be considered science fiction by observers from the past.

The fact that such radical scenarios were imagined for futures only slightly more than a decade away is telling. The pillars needed to make the future a sound one were mentioned throughout the sessions, such as enhancing regulation itself with technological means, greater global cooperation and partnerships, the need for a common understanding of the disparate and confusing terminologies, and the necessity to get digital ID infrastructures right.

The future is shaped by the decisions we make and the actions we take today. The Reg@Tech Roundtable on Digital Assets will continue to convene experts, decision-makers, and shapers of the future in this challenging yet exciting area.


## Author

**Bianca Kremer** is the inaugural Wharton BDAP research fellow.

**bkremer@wharton.upenn.edu**

# Reg@Tech 7 Participants

- Kaitlin Asrow (New York Department of Financial Services)
- Christopher Beck (Tradias)
- Sanjeev Bhaskar (Department of Justice)
- David Crosbie (Securities & Exchange Commission)
- Jens Hachmeister (Deutsche Börse)
- Carole House (National Security Council) (Remote)
- Kavita Jain (Federal Reserve Board)
- Julian Jonker (Wharton School)
- Linda Jeng (Georgetown Law School)
- Josh Klayman (Linklaters)
- Michele Korver (a16z Crypto)
- Bianca Kremer (Wharton Blockchain and Digital Asset Project)
- Chris Land (Office of Senator Lummis)
- Caitlin Long (Custodia Bank)
- Sigal Mandelker (Ribbit Capital)
- Giovanna Massarotto (Penn Carey Law School)
- Patrick Murck (Transparent Systems)
- Marina Niessner (Wharton School)
- Aurelia Nick (MME)
- Kevin O'Connor (FinCEN)
- Michael Oh (FINRA)
- Saule Omarova (Cornell Law School)
- Lukas Repa (European Commission) (Remote)
- Daniel Resas (YPOG Law)
- Marco Santori (Kraken)
- Antoinette Schoar (MIT Sloan School)
- Nina-Luisa Siedler (DWF Law Firm)
- Valerie Szczepanik (Securities & Exchange Commission)
- Tomicah Tillemann (Haun Ventures)
- Andrea Tosato (Penn Carey Law School)
- Peter Van Valkenburgh (Coin Center)
- Kevin Werbach (Wharton School)
- Olamide Williams (Wharton School)
- Landon Zinda (Senate Banking Committee)

# Endnotes

[1] The White House, Presidential Actions, Executive Order on Ensuring Responsible Development of Digital Assets, March 09, 2022, https://www.whitehouse.gov/briefing-room/presidential-actions/2022/03/09/executive-order-on-ensuring-responsible-development-of-digital-assets/.

[2] See European Parliament, Press Release, Cryptocurrencies in the EU: new rules to boost benefits and curb threats, https://www.europarl.europa.eu/news/en/press-room/20220309IPR25162/cryptocurrencies-in-the-eu-new-rules-to-boost-benefits-and-curb-threats.

[3] The European Union's legislative process includes three core legislators: (i) The Commission, (ii) the European Parliament, and (iii) the European Council.

[4] See Proposal Limiting Proof-of-Work Is Rejected in EU Parliament Committee Vote (coindesk.com), https://www.coindesk.com/policy/2022/03/14/proposal-limiting-proof-of-work-is-rejected-in-eu-parliament-committee-vote-sources/.

[5] The governance structure of Proof of Work mechanisms tends to become ever more concentrated as miners in pools coordinate with other pools to take decisions on protocol changes.

[6] The White House, Updated Data on Improper Payments, https://www.whitehouse.gov/omb/briefing-room/2021/12/30/updated-data-on-improper-payments/; see also Annual Improper Payments Datasets (paymentaccuracy.gov), https://www.paymentaccuracy.gov/payment-accuracy-the-numbers/; GAO's Latest COVID Relief Report Makes 15 New Recommendations on Improper Payments, Public Health Data Collection, and Critical Manufacturing, https://www.gao.gov/press-release/gaos-latest-covid-relief-report-makes-15-new-recommendations-improper-payments-public-health-data-collection-and-critical-manufacturing.

[7] See The White House, Joint Statement by President Biden and President von der Leyen, March 24, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/24/joint-statement-by-president-biden-and-president-von-der-leyen/.

[8] See, e.g., Brian Knight and Trace Mitchell, The Sandbox Paradox: Balancing the Need to Facilitate Innovation with the Risk of Regulatory Privilege, Mercatus Research Paper, 2020, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3590711.

[9] Decentralization is often seen as a key ethos of web3 and blockchains. However, much of what is portrayed as decentralized may not actually be decentralized. Recently, moves by Metamask, a wallet provider, and Opensea, an NFT marketplace, to block accounts hit by U.S. sanctions puts the decentralization aspect further into question and shows that some entities can still exert considerable control in the web3 era. See Nicholas Gordon, OpenSea, MetaMask confirm they will block users in U.S.-sanctioned countries, Fortune, March 4, 2022, https://fortune.com/2022/03/04/opensea-metamask-block-users-sanctions/.

[10] On the other hand, if a DAO does not register, it could be considered a general partnership, which under US law would result in joint and several liability for all participants.

[11] See David Siegel, The DAO Attack: Understanding What Happened, CoinDesk, March 9, 2022, https://www.coindesk.com/learn/2016/06/25/understanding-the-dao-attack/.

[12] See Phil Daian, Analysis of the DAO exploit, Hacking, Distributed, June 18, 2016, https://hackingdistributed.com/2016/06/18/analysis-of-the-dao-exploit/.

[13] See USAID, Identity in a Digital Age: Infrastructure for Inclusive Development (usaid.gov), https://www.usaid.gov/sites/default/files/documents/15396/IDENTITY_IN_A_DIGITAL_AGE.pdf#page=5.

[14] The World Bank considers these "invisible" people as priority, see World Bank Group, 1.1 Billion 'Invisible' People without ID are Priority for new High Level Advisory Council on Identification for Development (worldbank.org), https://www.worldbank.org/en/news/press-release/2017/10/12/11-billion-invisible-people-without-id-are-priority-for-new-high-level-advisory-council-on-identification-for-development.

[15] McKinsey Global Institute, Digital Identification: A key to inclusive growth, April 2019, https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth.

[16] See McKinsey Global Institute, Digital Identification: A key to inclusive growth, April 2019, https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth.

# 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