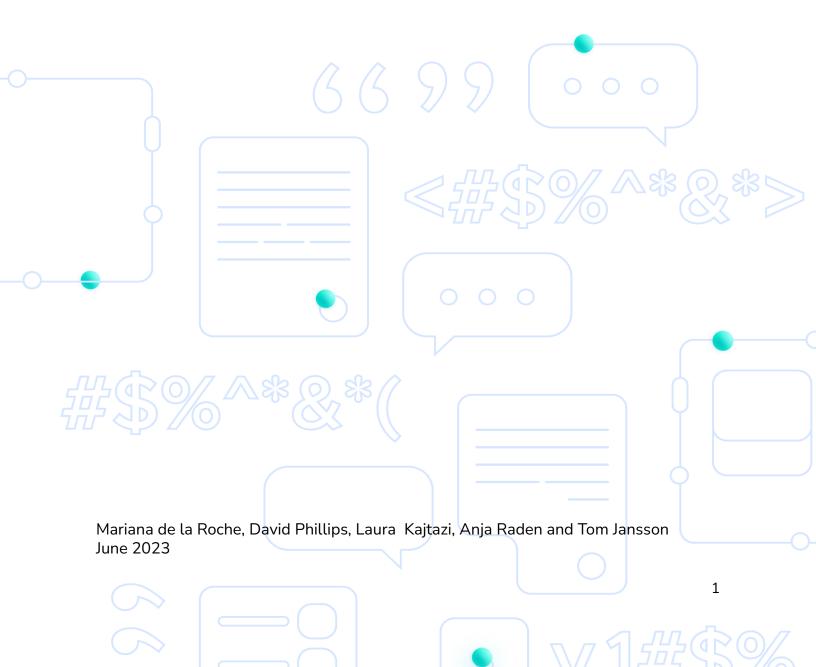# Bridging the gap between technology and regulation with dialogue

Findings from conversations between the IOTA Ecosystem, industry leaders and European Institutions

Mariana de la Roche, David Phillips, Laura Kajtazi, Anja Raden and Tom Jansson
June 2023

Getting to grips with blockchain technology is not an easy task. Nevertheless, regulators are expected to understand not only the current state of the industry but also upcoming innovations in a way that enables them to set the rules of the game. However, it is difficult to set the rules for a game in constant change.

On the one hand, blockchain and crypto evolve rapidly, bringing new applications and possibilities on almost a daily basis. This makes it hard for regulators to have a thorough understanding of the industry. On the other hand, it's also an uncertain landscape for the industry's players and innovators, who develop solutions without knowing how they could be impacted by future legislation.

An open dialogue between policymakers and industry players sheds light on where the key pain points are on both sides, and to address legislative and regulatory needs while allowing innovation to flourish. Within this dialogue, it is important to make room for small players to be part of the conversations, especially in dealing with blockchain. The decentralization and devolution of power to the individual and small players is very much part of the engrained philosophy of the industry, and as such it is coherent to invite small players to participate in consultative processes where their interests are also reflected so the voices of big players are not the only ones that legislators heard.

To accomplish this goal, the IOTA Foundation organized a series of events with FTI Consulting and projects from the IOTA community during the second semester of 2022 and the first semester of 2023. The purpose of these events was to initiate policy discussions about how regulation in the European Union should evolve with regard to digital assets, especially in the areas of Decentralized Finance (DeFi) and Non-Fungible Tokens (NFTs), two of the key focus areas when policymakers introduce new regulations in the coming years.

The goal of the events was not to seek legal advice from policymakers and regulators but to raise questions about where the regulation of this space is or should be heading. From the industry perspective, the main goal was to spread awareness about where the industry is going. In this area, the IOTA Foundation and FTI Consulting invited experts from the IOTA community to participate and help policymakers understand the technology and the needs of the industry so they can take a balanced fact-based approach when proposing, discussing, and negotiating new regulations in this space. Four events were organized:

1. **Increasing Trust, Accountability, and Ease-of-Use in Self-Hosted Wallets with SIS and Reusable KYCs,** with Identity Expert (IOTA Foundation), Charlie Varley (IOTA Foundation/Firefly), and Marius Kat (European Parliament).
2. **The Future of NFT Regulation: NFT Beyond Art**, with Song Choi (Soonaverse), Vitaly Semko (Minted Vodka) Joachim Schwerin (DG GROW, European Commission) and Jeff Bandman (European Securities and Markets Authority).
3. **Tokenization and the Real Economy**, with Rob Daykin (Nakama), Gianfranco Campos (Zignar Technologies) and Barbara Brandtner, and Ernst Ferdinandusse(EuropeanCommission Markets and Cases III: Financial Services, Antitrust: Payments Systems at the Directorate General for Competition).
4. **The Cost of Regulation and Uncertainty for SMEs and Startups**, with Dennis Schouten (Chunk Works), Bas van Sambeek (Chunk Works), Peter Kerstens (DG FISMA-

European Commission) and Jan Klesla (Technical Group, European Blockchain Partnership European Commission)

This report presents a summary of the conversations held during these events, their primary key points and pain points. It includes reflections and recommendations for both industry and policymakers.

Interinstitutional collaborations such as this series of events reflect the willingness of the industry and policymakers to find common ground and push innovation forward while also protecting the rights of consumers.

Disclaimer: The information and positions presented in this report are solely the views and opinions of the individuals that participated in the events and roundtables and do not represent the official stance of the European institutions. While every effort has been made to ensure the accuracy and comprehensiveness of the content, readers are advised to exercise their own judgment and discretion when interpreting and applying the information contained herein. The report serves as a platform for open dialogue and knowledge sharing among industry players and regulators, fostering a better understanding of the subject matter.

Table of Content

People that made this possible

We are grateful for the time and effort dedicated to producing this report. In particular, we thank the policymakers, industry experts and community members of the IOTA ecosystem for providing their time and valuable insights, as well as the FTI Consulting and IOTA teams that made this possible with their hard work. It is important to note that a few participants have preferred to remain anonymous in the report.

Current regulatory landscape

With the Markets in Crypto Assets Regulation (MiCA), Europe is already leading in setting a standard regarding public policy in the crypto environment. MICA aims to create a harmonized EU regulatory system for the operation of crypto-asset markets and to ensure that these markets operate properly while ensuring consumers' and investors' rights, market fairness and financial stability. MiCA is part of the digital finance package, which is a set of policies intended to maximize the value of digital finance in terms of growth and competitiveness while minimizing the risks. Although MiCA was the last stage of the legislative process, discussions have already started on a potential MiCA 2.0 and on the multiple uses of tokenization in the real economy, particularly for SMEs. However, the need for a MiCA 2.0 is still under discussion.

A European token economy is emerging, thanks to local and European regulations. Besides MiCA the DLT Pilot Regime is also a very relevant legislation. It establishes the conditions for permission to operate a DLT market infrastructure, limitations on the DLT financial instruments that can be admitted to trading and settled on the DLT, and cooperation between market operators, competent authorities and European Supervision Markets Authority (ESMA).

Among other capabilities, blockchain technology offers an alternative to traditional technologies or business models that build trust amongst different parties. In essence, it offers trust, without the need for a trusted third party. However, the fallout from recent shakeups in the crypto-sphere has catalyzed a heavy-handed tone from the official sector both in Europe and abroad as to how best to ring-fence the use of blockchain in financial markets. Legislators are worried about the high-risks to investors and the absence of specific proper safeguards and protection provisions. These events have upped its rhetoric around crypto-assets in the wake of the bankruptcy of one of the world's largest crypto exchanges which now shifts the attention to DeFi as it is not regulated yet.

Besides the more financial aspects, new legislative proposals such as the Product Liability Directive, the AI Act the Data Act or Digital Operational Resilience Act (DORA), established another type of requirements aimed to ensure a level of consumer protection guarantees in relation to the applicability of the technology or cybersecurity aspects.

The Data Act established requirements for the design of Smart Contracts; The AI Act lays down prohibitions of certain artificial intelligence practices; The Product Liability Act would allow compensation for damages caused by any product, including its failures to address cybersecurity vulnerabilities.

Moreover, the European institutions have showcased its commitment to explore and increase

legal certainty for innovative blockchain technology solutions. An example of this is the European Blockchain Regulatory Sandbox which represents a dialogue opportunity between policymakers and industry players.

Executive Summary of the conversations between the IOTA Ecosystem, industry leaders and European Institutions

The four roundtables hosted by the IOTA Foundation provided valuable insights into the regulatory landscape of decentralized technology and cryptocurrency. The regulation of self-hosted wallets, tokenization of real world assets, Non-Fungible Tokens (NFTs), and the impact of regulation on SMEs and startups were discussed, providing a range of perspectives on the potential benefits and challenges of implementing certain regulations.

The key take-aways of the roundtables were the following:

- **Increasing Trust, Accountability, and Usability in Self-Hosted Wallets with DID and Reusable KYCs**

  The first roundtable focused on the regulation of self-hosted wallets in the context of the Transfer of Funds Regulation and the potential risks of money laundering and terrorism financing. The roundtable proposed the use of decentralized identifiers (DID) to link identities to wallets, zero-knowledge proofs (ZKP) to address data protection concerns, and an incentive-driven system to encourage users to identify themselves. The discussion aimed to strike a balance between individual privacy on the one hand and Anti-Money Laundering/Countering the Financing of Terrorism (AML and CFT) measures on the other. It also addressed regulatory uncertainties and inconsistencies, and promoted innovation and interoperability within the crypto industry.

  The roundtable revealed that the main concern of EU regulators about self-hosted wallets is the lack of infrastructure or solutions that enable the owner of a wallet to be identified when there is a risk or suspicion of money laundering or terrorism financing.

  In response, the roundtable proposed generating a portable KYC credential in the self-hosted wallet that is reused for every interaction with a Crypto Asset Service Provider (CASP). to enhance Know Your Customer (KYC) processes in self-hosted wallets: However, to achieve this solution, the industry will need to agree on KYC standards for the CASP and the self-hosted wallet. Additionally, education on using and protecting keys and passwords, backup solutions and strategies, and self-sovereign identities were discussed as important measures to address security concerns and eliminate friction.

- **The Future of NFT Regulation: NFTs Beyond Art**

  The second roundtable discussed the potential use cases of NFTs beyond the cultural sector and their role in the real economy. The invited experts highlighted the importance of regulation based on use cases rather than on the underlying technology and the need for industry standards to differentiate financial use versus non-financial use cases. Embedded supervision was presented as a regulatory framework for decentralized markets, and the roundtable emphasized the importance of considering new organizational forms in decentralized contexts, such as Decentralized Autonomous Organizations (DAOs). Finally, the roundtable highlighted the importance of modularity in the NFT space and the need to define the metaverse and Web3 while ensuring they remain free from big tech dominance.

  The main takeaway from this discussion was that the European Commission is exploring the Decentralized Finance (DeFi) sector, notably to identify real-economy use cases for NFTs. As such, a creative approach to regulation is warranted, and it is especially important to explore the potential of self-regulatory frameworks and blockchain technology to enable embedded supervision.

- **Tokenization and the Real Economy**

  The third roundtable discussed tokenization and its potential use cases. It highlighted the need for regulatory clarity and global harmonization to provide users with confidence if problems with digital assets or tokens occur on the network. The process of tokenization has the potential to enhance competition and transparency, optimize operations, and foster financial inclusion. However, it is crucial to acknowledge and mitigate the inherent risks and fulfill regulatory and legal obligations.

  The discussion emphasized the importance of distinguishing between open and closed systems, governance structures, and compliance measures, as well as the exchange of sensitive information. Blockchain technology and smart contracts offer a degree of enforcement of obligations based on data, but it is essential to trust the data provided by custodians of the assets to the oracles, which feed information to the blockchain. Overall, tokenization presents exciting possibilities for the future of finance and investment, but it is crucial to ensure a responsible and regulated approach to realize its full potential.

- **The Cost of Regulation and Uncertainty for SMEs and Startups**

  The fourth roundtable provided valuable insights into the regulatory challenges faced by small and medium-sized enterprises (SMEs) and startups in the decentralized technology and cryptocurrency space. The roundtable highlighted the impact of regulation on SMEs and promoted a regulatory approach that enables entrepreneurs to make informed decisions based on their risk appetite. The importance of building utility in decentralized technology was discussed, and solely prioritizing token value and market capitalization was deemed unviable. A careful regulatory approach that addresses legal issues and balances government control and individual freedom was fully supported by all participants. Finally, the sandbox model was discussed as a

valuable tool for promoting innovation, guiding innovators, and establishing trust with regulators and society.

According to the four roundtables, the general perspective of regulators is as follows.

There is a need for regulatory clarity and harmonization in the decentralized technology and cryptocurrency space. The regulators emphasized the importance of balancing innovation and regulation and addressing potential risks such as money laundering, terrorism financing, and market manipulation. They also stressed the need to protect consumers and maintain financial stability while promoting innovation and competition. Additionally, the regulators acknowledged the importance of collaboration and dialogue between innovators, regulators, and society to create a regulatory framework that fosters innovation while addressing societal concerns.

Overall, the regulators struck a note of caution and balance, recognizing both the potential benefits and risks of decentralized technology and cryptocurrency, and advocated for a responsible and regulated approach to realizing the technology's full potential.

The General Perspective of Industry Experts can be summarized like this.

Throughout all four roundtables, the invited representatives of the DLT/blockchain/crypto industry emphasized the importance of finding a happy medium between innovation and regulation. They advocated for a flexible and dynamic regulatory environment that can foster innovation while ensuring necessary regulations are in place. They also argued for regulatory clarity and global harmonization of laws in order to provide users with confidence in the event of issues with digital assets or tokens on the network.

Industry representatives acknowledged the importance of complying with regulatory requirements, while also highlighting the need for regulations that fit the transparent nature of decentralized technologies. They expressed interest in participating in more conversations on the topic and finding practical solutions to challenges that arise. They highlighted the importance of transparency throughout the development process, from code reviews to public audits, to build trust and lead to better outcomes. They emphasized the significance of understanding the legal landscape and conducting risk assessments before pursuing certain endeavors, as well as aligning European values of mutual care with the goal of fostering innovation.

Why is dialogue so important?

Distributed ledger technology has ushered in a new era of digital innovation, disrupting traditional industries and challenging existing legal frameworks. Navigating this landscape requires a deep understanding of the technology, its implications, and the legal considerations that come with it. The roundtables provided a platform for experts to share their insights, exchange knowledge, and address the emerging legal challenges posed by blockchain.

Through these discussions, participants gained insights into the legal and regulatory frameworks that govern DLT, exploring various perspectives and identifying areas for improvement. The roundtables facilitated open dialogue, allowing stakeholders to address key

issues, clarify uncertainties, and propose solutions collaboratively. The diverse expertise brought to the table fostered a comprehensive understanding of the subject matter and encouraged cross-industry collaboration.

These roundtables helped to demystify the legal landscape surrounding blockchain technology. By breaking down complex concepts, exploring case studies, and sharing practical experiences, the events promoted clarity and increased awareness among participants. The deep dive into legal considerations fostered a more informed and educated community that can navigate the intricacies of DLT confidently.

Given the complexity and rapid pace of change in the blockchain ecosystem, it is imperative that more events like these roundtables are being promoted. Continued engagement, collaboration, and knowledge sharing are necessary to keep pace with the evolving legal landscape. By hosting regular roundtables and similar events, the industry and regulatory stakeholders can stay abreast of the latest developments, exchange best practices, and collectively contribute to the establishment of a robust legal framework for blockchain.

Chapter 1: Increasing Trust, Accountability, and Usability in Self-Hosted Wallets with DID and Reusable KYCs

In November 2022, the IOTA Foundation held a roundtable with the following participants: Marius Kat, Head Parliamentary Assistant to MEP Paul Tang (SnD, NL) from the European Parliament; Charlie Varley, Director of Engineering, Firefly and a full-stack Identity engineer, both working for the IOTA Foundation. Also participating were members of the IOTA Foundation's Legal and Regulatory team Mariana de la Roche, Laura Kajtazi, Anja Raden, Tom Jansson, and David Phillips, and Adriana Torres, Maxime Malherbe, and Dea Markova from FTI Consulting.

The goals of the roundtable were to demonstrate the industry's strong support for efforts to harmonize the European Union's Anti-Money Laundering/Countering the Financing of Terrorism (AML/CFT) framework, of improving the detection of suspicious transactions and closing loopholes used by criminals, and of exploring solutions that would provide self-hosted wallets and decentralized finance with the same level of AML/CFT as fiat transfers, including risk mitigation, monitoring of suspicious transaction patterns, and processes to bring these to the attention of regulators.

This chapter starts by (I) tracing the policy outcomes of the Transfer of Funds Regulation followed by (II) the remarks of all participants and an overview of the key points about Decentralized Identifiers (DID) for self-hosted wallets. The chapter concludes with a summary as final remarks (III).

I. Background: Crypto and the Transfer of Funds and Anti-Money Laundry Regulations

Current status quo: The Transfer of Funds Regulation (TFR) extends the Travel Rule established for traditional finance to cover crypto asset transfers. The Travel Rule requires that information about the source of an asset and the beneficiary 'travel' with the transaction and is stored on both sides of the transfer. Applied to crypto, it requires Crypto Asset Service Providers[1] (CASPs) to collect this information and hand it over to national competent authorities during an AML investigation. The Travel Rule also covers transactions between self-hosted wallets and custodial wallets. Essentially, CASPs will need to collect and verify personally identifiable information about their customers and report the information to competent authorities when requested.

Legislative process: The treatment of self-hosted wallets was a contentious issue during discussions on the TFR text between the European Parliament and the European Council. Self-hosted wallets enable the owner to have total control of their digital assets (only the owner controls the private keys which give access to their blockchain-based assets). This is in contrast to custodial wallets, where a third party manages digital assets on behalf of the owner (the owner delegates management of their private keys to the third party). Both the European Council and industry players were concerned about the European Parliament's stance that the originator and beneficiary of any transaction between a CASP and a self-hosted wallet should be verified. Not only are there concerns about the potential vulnerability of such data, but also the potential obstacles to innovation and adoption should the process be too bureaucratic. Although the rule was, in the end, significantly diluted, it will be reviewed by the European Commission 18 months after the TFR enters application.

Know Your Customer (KYC)

KYC is a process used by companies to verify the identity of their customers or clients. KYC is a regulatory requirement in many industries, including finance and banking, to prevent illegal activities such as money laundering, fraud, and terrorist financing. The KYC process involves collecting information about the customer and verifying that information against reliable sources such as government-issued identification documents. The goal of KYC is to ensure that companies are doing business with legitimate individuals or entities and to minimize the risk of financial crime

---

[1]According to the *definition used by the EU's Markets in Crypto-Assets (MiCA) regulation,* "*Crypto-Asset Service Provider' means a legal person or other undertaking whose occupation or business is the provision of one or more crypto-asset services to third parties on a professional basis, and are allowed to provide crypto-asset services in accordance with Article 53*".

II.   Remarks and Key Points about Self-Hosted Wallets as Discussed at the Roundtable

1.   Addressing the European Parliament's skepticism about self-hosted wallets

The roundtable's representative of the European Parliament highlighted that the ID of wallets is often obfuscated either on purpose or because there is no infrastructure to link identities, which makes policymakers hesitant unless an effort is made to enhance transparency across the entire market. Therefore, the rise of the anonymous and unregulated decentralized finance (DeFi) sector has made policymakers eager to bring regulation to the financial intermediaries sector. Policymakers see AML and CFT risks in any technology that enhances anonymity, and their regulatory approach to the interaction between self-hosted wallets and CASPs has been based on the principle of "same risks, same rules". Self-hosted wallets are seen by several parties in the European Parliament (such as S&D and the Greens) as a vehicle for money laundering (ML) and terrorism financing (TF) and a way to evade regulatory scrutiny. These opinions were compounded by sanctions following the Russian invasion of Ukraine and the current condition of the crypto market. These fears have prompted regulators to set up stronger due diligence measures for providers, who will have to comply with verification requirements on ML/CT risks and identification of sanctions or other restrictive measures before making the crypto assets available to beneficiaries.

According to the IOTA Foundation's representatives at the roundtable, an infrastructure that could link identities to a wallet is decentralized identifiers (DID). The W3C standard for DID allows self-hosted wallet users to create a portable digital identity. The user can perform a single KYC authentication and reuse that KYC event for every new CASP they interact with. For users of self-hosted wallets, this would remove the tedium of having to run through KYC processes with each new CASP and avoid unnecessary disclosure of personal information with each new CASP and its subcontractors. As this solution depends on voluntary identification by the wallet owner, it is important to make it as privacy-preserving and frictionless as possible.

What is DID?

Decentralized Identifier (DID) is a W3C standard that enables identity subjects to manage their identifiers and associated cryptographic key material on registries like distributed ledgers. DID enables the creation of interoperable permissionless identity systems while enhancing the trustworthiness of information about the subject exchanged in a self-sovereign manner. This information is typically encoded in Verifiable Credentials and Presentations, which are currently in the W3C recommendation status.

DIDs can be stored in self-hosted wallets for crypto tokens or identity credentials. Although IOTA's Firefly wallet can handle both crypto transactions and identification, industry experts anticipate that separate wallets for crypto and identification will be the standard in the near future. Therefore, entities will probably use a separate application for their crypto assets and authentication material for regulated interaction with a CASP.

To enable separate wallets for crypto and identity, it would be necessary to have a solution that links an identity to the crypto wallet's address. For example:

- A linking credential could connect an identity with a wallet and raise red flags in case of any changes to the wallet. It is worth noting that, during the TFR negotiations, the European Parliament supported a system where one identity could be used for multiple platforms.
- A record kept by CASP providers that a wallet was authenticated by a certain identity (though this doesn't guarantee that the same wallet can't be used by a different identity).

The Firefly Wallet

[Firefly](#) is an open-source, secure, and lightweight digital wallet for managing cryptocurrency tokens. With a mobile and desktop app, Firefly has ~50K users. Firefly enables users to send and receive tokens with zero fees in seconds, with a clean, minimalistic UI, seamless usability, and industry-leading security. Features extend beyond simple cryptocurrency payments to include staking tokens and participating in governance decisions through a decentralized voting system. Future features include decentralized identity, NFT management, and purchasing cryptocurrency with a credit/debit card.

In the short term, having the DID taking place in the self-hosted wallet itself (regardless of whether it is in one wallet that can host both tokens and identity or in separate linked wallets) addresses data-protection concerns shared by the IOTA Foundation's representatives. From their point of view, the need for CASP providers to store the plaintext identity information included in a DID credential is risky because it could be leaked or hacked and used to connect the DID to a person.

A long-term solution proposed by the IOTA Foundation's representatives involves Zero-Knowledge Proofs (ZKP), which reveal limited information that enables assertions to be made without sharing the actual data. For example, it could confirm that "this person is of minimum age" without giving away the user's actual date of birth. This approach works best with numbers and less well with more nuanced information, so an attribute-based or permission-based credential could be used, where the issuer is trusted sufficiently to confirm verification (e.g. "He is of age") without the ZKP credential revealing complete information.

ZKP research is still at an early stage and EU-level research into ID credentials could take several years. Also, running a ZK algorithm and creating and verifying a credential is slower and more expensive than using plain text or minimal attribute credentials. However, the investment expected to occur in the ZKP field within the next five years should change this. For example, the IOTA Foundation is working with an academic consortium to explore how ID credentials provide partial reveals, the privacy-preserving revocation aspects of ZKP, and optional reveals (where authorities can reveal the whole credential).

The roundtable also discussed how some ZKP schemes offer an optional ID reveal, where the same credentials for ZKP assertions can be disclosed to law enforcement authorities. However, this can be complex because access rights to the information need to be established at the time

of generating certificates. Nevertheless, this was deemed desirable as long as the CASP can store but not access the information.

2. From a punitive to an incentive-driven approach

The European Parliament representative reminded the roundtable that the TFR designates self-hosted wallets as non-obliged entities. This means that users cannot be forced to identify themselves, and the obligation to identify self-hosted wallets is placed on the CASPs. As such, Recital 34a of the TFR clarifies that CASPs must verify transactions between a hosted and self-hosted environment on a risk basis. The regulation also tasked the European Banking Authority and the European Commission to assess which enhanced due diligence measures should be implemented by CASPs to mitigate these risk factors. This includes the use of analytic tools based on decentralized cryptocurrency and blockchain technology to detect the origin or destination of crypto-assets that could prompt deeper verification analysis.

Because self-hosted wallets are non-obliged entities, the IOTA Foundation's experts believe that it is worth promoting an incentive-driven system (rather than a punitive one) to encourage users to identify themselves. This could happen by allowing the KYC to happen within their wallet and not with a CASP.

The European Parliament representative considered that the interaction between self-hosted wallets and CASPs is the point where the unregulated and regulated parts of the crypto markets meet. This was described as a potential blind spot at the entrance to the regulated crypto market.

What is Self-Sovereign Identity?

Self-Sovereign Identity is a decentralized paradigm for identity management and authentication, enabling individuals, companies, and things to safely and reliably interact. SSI gives holders full control over their identity without relying on third-party providers to manage their data.

SSI is implemented through DID Documents, which contain data such as public keys, enabling the holder to prove ownership over their personal data contained in Verifiable Credentials. SSI allows holders to prove their identity when accessing services and applications.

The IOTA Foundation's representatives explained that the industry is moving in a direction where self-hosted wallets do more than just send and secure cryptocurrency tokens, and many wallets can integrate different features inside the wallet app such as buying cryptocurrency tokens, trading NFTs, or swapping tokens on decentralized exchanges. This means that the user may interact with multiple CASPs when using their wallet, and if each of these CASPs requires a separate KYC process, the result would be a cumbersome onboarding process. Therefore, allowing the KYC process to happen in the self-hosted wallet and be re-used when interacting with different CASPs will minimize friction. However, although it is currently technically possible for a KYC event to be generated in the wallet, its acceptance by different

CASPs would require a level of standardization amongst CASPs and industry cooperation that do not yet exist. However, the eIDAS regulation could be a starting point for these standards.

3. Moving the regulatory focus toward a long-term vision

According to the roundtable's European Parliament representative, the European Commission's focus in the TFR was on financial intermediaries such as service providers. Because the use of cryptocurrency for goods and services is currently relatively limited, crypto holders still have to rely on traditional finance by exchanging their cryptocurrencies for fiat money (government-issued legal tender not backed by a commodity) via financial intermediaries.

While this is acknowledged as a good starting point, it does not consider that DeFi is characterized by a lack of financial intermediaries, and transactions without intermediaries are outside the scope of the TFR.

Therefore, while policymakers currently prioritize the identification and verification of the originator or beneficiary of a transaction with a self-hosted wallet, the European Parliament has a long-term aspiration to utilize the full potential of emerging decentralized cryptocurrency and blockchain technology. After the conversation with the IOTA Foundation's representatives, the parliamentary representative recognized that Self-Sovereign Identities could create transparency while protecting user privacy by connecting self-hosted wallets with digital identities and enabling even large transfers to be identified.

Moreover, the roundtable's IOTA Foundation representatives highlighted that current regulation is only focused on private individuals. This does not consider the complex ownership of wallets, especially in the context of the future machine economy, like a wallet being owned by multiple parties consisting of any combination of machines, humans, and organizations, including Decentralized Autonomous Organizations (DAOs). For instance, a car could use a wallet to pay toll fares while driving, or a Digital Product Passport could accompany a product along the supply chain. Nevertheless, the parliament representative noted that ownership of wallets is currently human-centered, and there is no legal system for things owning wallets.

4. Breaking the blockchain bubble through education and user-friendly design

The IOTA Foundation and the European Parliament believe that blockchain technologies will scale and be adopted by people outside the blockchain ecosystem. For this to happen, security concerns need to be addressed. In particular, the IOTA Foundation's representatives stressed the need to educate non-crypto experts on using and protecting their keys and passwords, as long as there is no centralized authority in crypto that can return a lost or forgotten password. The recovery of a key or seed (a "seed" is the key to a wallet) is not technically possible in most cases, therefore European Institution initiatives like CHAISE are highly appreciated.

Moreover, the IOTA Foundation's representatives argued that several backup solutions and strategies can be put in place where some form of pre-existing restore mechanism is built into the wallet, so there is no need to drive people to use custodial wallets. Examples of backup solutions include:

- **Social backup** involves giving a set of trusted guardians the ability to collectively restore a wallet on behalf of the user. If the user loses their crypto key, they only have to interact with a few guardians to restore access to their wallet. One example of a wallet that takes this approach is [Argent.](#)
- **Semi-custodial backup** involves creating multiple keys through multi-party computation technology. Together with a user's backup or biometric scan, a centralized recovery service can restore access to the wallet. But the centralized party cannot transfer the user's assets without one of the user's other keys. One example of a wallet following this approach is [ZenGo](#).
- With **Self-Sovereign Identifiers like DID**, the key material can fundamentally change in the background, allowing users to replace compromised keys and create backup keys used to restore access in case of loss, which is desirable for users new to the crypto space.

5. Eliminating friction with reusable KYC credentials

Finally, it was highlighted that in the early conversations about the TFR, the European Parliament wanted wallets to be verified, including owner verification, AML analysis of suspicious transactions, and links to other bank transactions and individuals. However, this expectation was not included in the final regulation. Instead, CASPs are required to assess the risk level of transactions from self-hosted wallets through an analysis-based approach, such as examining the wallet's transaction history and conducting blockchain analysis. Therefore second-level legislation will establish how compliance can be achieved, for example by clarifying the production and processing of risk assessments and determining which transactions require risk assessment. As previously stated, blockchain analysis tools can be employed for risk assessment, with an alert system triggering further verification analysis.

The European Commission has a five-year window in which to gather data on the impact of the first round of TFR and AMLR regulations on self-hosted wallets. Based on this data, a long-term solution could be developed that does not assume that most transactions go through a centralized environment. For example, Article 59a of the March 2023 version of the European Parliament's AMLR (still under negotiation) intends to establish a €1000 threshold for crypto payments between self-hosted addresses unless the customer or beneficial owner of the self-hosted address is identified.

The IOTA Foundation's representatives reiterated that when reviewing the impact of regulation on the crypto sector, regulators should consider that DeFi is defined by the proliferation of services, implying dozens of KYC events. However, if each of these applications causes a KYC process for each CASP, the result would be a cumbersome onboarding for wallets. A more technically-feasible solution is to move towards the existing DID standard, where the self-hosted wallet is given a portable KYC credential that is reused for every CASP within and outside the wallet. Not only would this cause less friction in terms of user experience, but it would also serve to incentivize users to identify themselves.

Final remarks for Chapter 1

The roundtable centered on the regulation of self-hosted wallets in the context of the TFR and the potential risks for money laundering and terrorism financing. The roundtable proposed using decentralized identifiers (DID) to link identities to wallets, zero-knowledge proofs (ZKP) to address data protection concerns and an incentive-driven system to encourage users to identify themselves. The roundtable also highlighted the need for a long-term vision and regulatory focus that considers the full potential of emerging decentralized cryptocurrency and blockchain technology. Additionally, education on using and protecting keys and passwords, backup solutions and strategies, and self-sovereign identities were discussed as important measures to address security concerns and eliminate friction. Finally, the roundtable emphasized the importance of striking a balance between AML and CFT risks and individual privacy, addressing regulatory uncertainties and inconsistencies, and promoting innovation and interoperability within the crypto industry.

The main concern of EU regulators about self-hosted wallets is the lack of infrastructure or solutions that enable the wallet owner to be identified when there is a risk or suspicion of money laundering or terrorism financing.

These concerns can be addressed by blockchain solutions that enhance KYC in self-hosted wallets: for example, by generating a portable KYC credential in the self-hosted wallet that is reused for every interaction with a CASP. This solution also eliminates the friction for self-hosted wallet users as long as KYC will be a one-time event instead of multiple events. This improves the user experience and incentivizes self-hosted wallet owners to comply with the KYC process.

However, to achieve this solution, the industry will need to agree on KYC standards for CASPs and self-hosted wallets; eIDAS could be a starting point to address this.

The discussion provided an opportunity for the regulator to gain more insight into the benefits and challenges of implementing certain regulations, as well as the perspectives of industry and community experts.

Chapter 2: The Future of NFT Regulation: NFTs Beyond Art

In January 2023, the IOTA Foundation conducted a roundtable with the following participants: Dr. Joachim Schwerin from DG GROW, Jeff Bandman, founder of Bandman Advisors and COO/General Counsel of 6529 Holdings; Mariana de la Roche, Laura Kajtazi, Anja Raden, Tom Jansson, and David Phillips from IOTA Foundation and Adriana Torres and Maxime Malherbe from FTI Consulting.

The roundtable also included two members of the IOTA ecosystem: Song Choi, Head of Marketing and Founder of SoonLabs, makers of Soonaverse.com, a Web3 Ecosystem-as-a-Platform; and Vitaly Semko, Founder of MintedVodka, an NFT marketplace. They were invited as representatives of the industry to share information with the regulators on the technical aspects of how NFTs are built, the underlying technology, who can create NFTs and the off-chain and on-chain aspects of NFTs.

The roundtable aimed to showcase to policymakers that the industry is highly supportive of the legal certainty brought by NFT regulations. The industry is in favor of regulation based on use cases and not on the underlying technology, as it believes this approach can better target specific risks and challenges. However, the industry fears that premature and highly prescriptive regulation (specifically on AML) could hamper the development of the NFT market.

This chapter starts by presenting the NFT regulatory landscape (I.), followed by interventions and remarks of all participants and an overview of the key points (II), and concludes with a summary (III).

What is an NFT and how is it transacted?

A Non-Fungible Token (NFT) is a digital asset that represents a unique (i.e. non-fungible) item or property (in contrast to a fungible digital asset, such as a cryptocurrency coin or a dollar bill). Each NFT is linked to a specific account and transactions follow the rules of a smart contract. This means that, when a buyer pays for an NFT, a function is executed in the smart contract to implement the change of ownership of the NFT by linking it to the buyer's blockchain address. Regulators are interested in the parties involved in NFT transactions and who executes the smart contract. Policymakers need to understand these factors to establish requirements for NFT service providers in a future regulatory regime.

I.   Background: The Regulatory Landscape of NFTs

Although there is no specific regulation for NFTs currently in place, several recent landmarks of regulation impact NFTs:
- NFTs have raised the attention of international regulatory bodies such as the Financial Action Task Force (FATF), which addresses NFTs in its latest update (published in October 2021). Headline-making high-value NFT transactions and the widespread use of cryptocurrency have raised concerns among bodies like FATF over whether these

transactions are being used to circumvent anti-money laundering regulations. The work of FATF impacts European regulatory reforms and the EU's Anti-Money Laundering (AML) framework, which is presently being deliberated by the European Parliament and Council.

- The European Commission also [recommends](#) that NFT sales platforms are included in the categories of entities obligated to submit to Know Your Customer (KYC) processes.
- This approach has been tentatively adopted by the European Parliament's Anti-Money Laundering Regulation (AMLR), where amendments have been introduced in Article 3 to include persons providing services for the sale and purchase of NFTs as obliged entities. The proposed changes would aim to fill the MiCA gap, and align the Anti-Money Laundering Rulebook with FATF rules (as the Commission recommends) and therefore mandate NFT platforms to comply with KYC obligations. However, the European Parliament is still discussing the final text; once agreed upon, it will need to be confirmed in an ECON-LIBE Joint Committee before starting the trialogue negotiations with the Council.
- The European Parliament drafted an Own Initiative Report at the end of 2022, which would have requested the European Commission to propose NFT legislation. However, it was canceled due to unrelated circumstances, and the Parliament agreed to exclude NFTs from MiCA for the time being. Instead, the Parliament prefers to focus on specific use cases, such as IP rights regulation, rather than proposing an overall regulatory approach.

MiCA and NFTs

The Markets in Crypto Assets (MiCA) regulation exempts unique and non-fungible crypto assets from its application, as they have limited financial use and associated risks.

However, MiCA does state that the fractional parts of a unique and non-fungible crypto asset should not be considered unique and non-fungible. It also specifies that the issuance of crypto assets as NFTs in a large series should be considered an indicator of their fungibility. Mere attribution of a unique identifier to a crypto-asset is insufficient to classify it as unique or non-fungible, as the assets or rights represented must also be unique and non-fungible

Moreover, MiCA mandates the European Securities and Markets Authority (ESMA) to develop guidelines for classifying crypto assets as financial instruments. These guidelines will provide the criteria under which crypto-assets can be deemed as unique and non-fungible. National competent authorities will be the ones ultimately challenging the classification of a crypto asset as an NFT, for which MICA recommends a substance-over-form approach to which asset features determine qualification, regardless of the designation proposed by the issuer.

Nonetheless, it remains crucial to regulate NFT service providers without stifling innovation, thereby enabling us to profit from the technology's advantages while guaranteeing legal certainty and market integrity. Experts from FTI Consulting have noted that regulators view NFTs in three ways:

- A sign of technological progress and innovation with all the associated economic benefits, of which the legislator wants to take advantage.

- An economic element that can be invested in and used as means of payment and trade.
- A potential channel for money laundering.

With this in mind, the IOTA Foundation organized a roundtable in January 2023 on which this report is based.

II. Remarks and Key Points as Discussed at the Roundtable

1. No one-size-fits-all approach for NFTs

With the implementation of MiCA, Europe recognizes the significant advantages of NFTs as a subcategory of blockchain technology for real-world applications. Although the role of NFTs in art is important, their potential use cases extend far beyond the cultural sector. A selection of potential and current use cases of NFTs is included in the next section.

The roundtable's European Commission representative described several NFT and blockchain priorities of the Commission in 2023. These include exploring the metaverse, developing a programmable or digital euro in two well-established workstreams, and identifying real-economy use cases for NFTs. Additionally, the Commission is examining the decentralized finance (DeFi) sector through an industry initiative with the support of the Directorate General for Internal Market, Industry, Entrepreneurship, and SMEs.

The European Commission representative highlighted the importance of regulating NFTs in a way that benefits the real economy and avoids imposing top-down approaches to regulation from either big tech or the public sector. The preferred approach is community-driven regulation that complies with European data rules.

Moreover, the European Commission representative highlighted the role of industry standards in delineating NFTs for financial use versus non-financial use, helping regulators and policymakers to see what is primarily non-financial and therefore falls into yet-to-be-developed categories of regulation and governance.

To those remarks, the roundtable's industry representatives highlighted that digital assets are mass products originally used as payments and therefore it is understandable that authorities first look at NFTs from a financial framework. However, there is a range of NFT use cases, and a one-size-fits-all approach to NFTs and unique non-fungible digital assets would be both a costly and a damaging mistake. Despite the hype around NFT collectibles selling for millions of dollars, the main NFT value is more likely to approach zero. Therefore, and in the spirit of *de minimis*[2], the proposal to run a chain analysis check on every single NFT would be prohibitively expensive.

From the perspective of the roundtable experts, most NFTs are better described as consumer products than as financial products and therefore, those that are not financial products should not primarily fall under financial regulatory logic. This means that a regulation based on use

---

[2] (*de minimis non curat lex*, or "The law does not concern itself with trifles")

cases and not on the underlying technology will better target specific risks and challenges without hampering innovation.

To illustrate the variety of NFT trends and use cases as a demonstration of their utility for the economy, the experts highlighted the following real-world examples:

- NFTs can improve transparency around ownership, authenticity[3], and remuneration for goods and services.
- Relevant value of NFTs (and blockchain technology in general) in developing digital skills and education. Given that there are over [three billion estimated gamers worldwide](#), the potential for the gaming sector to draw young people into the digital economy is an opportunity to encourage younger generations to become innovators and entrepreneurs in digital solutions.
- NFTs disrupt the monopoly of big tech in Web2, where tech giants own digital objects and content like books and music instead of the individual. With NFTs, creators can reclaim ownership of their digital assets and avoid intermediary gatekeepers such as the Apple store, Facebook, or Amazon, who take large percentages of sales. NFTs empower individuals to exercise sovereignty over their digital objects and support the creator economy.
- NFTs can capture the intangible value and consumer goodwill of brands. Brands can create digital objects for their fans as a way of finding new revenue streams and engaging with their audiences through digital assets.

The roundtable experts described the divide between the "real" and "digital" economies as blurred. Therefore, any European policy framework should take into account the high degree of integration between NFTs, Web2 (the current stage of the internet), and Web3 (the next stage of the internet). Moreover, they considered that application of minimum KYC thresholds is proportionate to the risks and practicalities because (and despite attention-grabbing headlines to the contrary) the average NFT sale price and expected value of most NFTs are very low.

Moreover, it was noted that many companies related to NFTs are either not incorporated and exist only as entities in the crypto space or are incorporated in a tax haven with a foundation in another company. In other words, they are often inaccessible to the law. Hence, pushing responsibility for the enforcement of regulation onto the platforms could create uncertainty and push projects further into semi-illegality, rather than encourage them to invest and incorporate in Europe.

The participants agreed that over-regulation of the sector should be avoided. Because NFTs can represent almost anything, from birth certificates and company shares to artworks and currency, there will always be modifications and new solutions, so there is little point in putting too much weight on regulatory definitions. To advance future regulation, discussion with industry partners is important, as they are the stakeholders that will use the standards and regulations. In turn, industry players need to be clear about what they need to move forward in innovating their business models. An assertive stance is important because there will always

---

[3] For example, NFTs can be used as digital twins of a product to accompany the product along the value chain as a means of protection against counterfeit good

be opponents who do not support cryptocurrencies and blockchain technology, preferring instead to protect their interests.

Finally, the roundtable participants agreed that more work needs to be done on the legal definition and taxonomy of NFTs and their associated intellectual property rights. Moreover, use cases should be defined by industry players and should include all the different technical elements, data storage, oracles, and platforms. Industry standards will help to differentiate financial use versus non-financial use, making it easier for regulators to delineate suitable regulations and governance. For example, if property rights are recorded in the underlying smart contract and other contractual frameworks relating to the NFT, are the rights also exchanged in the transaction? Clarification on this subject is needed as the upcoming standards would aim to bring legal certainty and consumer protection rights.

2. Exploration of NFT use cases

In contrast to Web2, Web3 represents the real economy and will encompass the time people spend in digital spaces, whether creating, consuming, or playing games, to a much more immersive extent. It is here where MiCA offers Europe a real opportunity to grow and lead. In most cases, NFTs are and represent a utility, therefore they are not speculative in nature. Unlike art NFTs, users won't want to trade utility NFTs but rather hold onto them, so their financial value will not increase. To illustrate these, the industry representatives presented the following cases:

- Decentralized Autonomous Organizations (DAOs) and Web3 ecosystems like Soonaverse use NFTs for many different purposes. Different actors (e.g. NGOs, developers, or credit issuers) create their DAO space within the Soonaverse and create NFTs for purposes like the certification of membership to a particular space or guild. Voting or share tokens belonging to that guild will only be given to people who hold that particular NFT (see insights by SoonLabs and Minted Vodka below).

- NFTs can also be used as proof of certification and reputation: for example, an NFT can be used to certify the authorization of carbon credits or whether someone has paid a Know Your Customer administration fee.

- NFTs could help establish the presence of a brand in the metaverse. The metaverse itself will likely be designed with NFTs as customized objects. For example, a meeting room or board room in the metaverse could be decorated with NFTs as customized furniture, logos, branding, and artwork.

SoonLabs Insights

Song Choi, Head of Marketing and Founder of SoonLabs, explained how NFTs are used in Soonaverse.com, a Web3 Ecosystem-as-Platform. Initially built on the feeless and energy-efficient IOTA protocol, SoonLabs has since expanded its capabilities to include a feeless NFT marketplace and token launch pad, so users can make and distribute tokens from their own marketplaces. SoonLabs' primary focus was on building a non-custodial token exchange rather than a centralized exchange that could be hacked and lose user funds.

The Soonaverse then moved to the <u>Shimmer</u> network, enabling third parties to integrate tools like a DEX, aggregator, and yield vaults onto the platform.

Song Choi highlighted what they call the "Buildaverse", which is an Ecosystem or Platform as a Service, a Web3 operating system that is given to enterprise partners that want to deploy an ecosystem as a platform and a plug-in to their current enterprise systems. An organization can set up its own "verse" in the Soonaverse and use the Soonaverse's core feeless modules or third-party modules to create a confederation of self-governing organizations with an underlying theme. These "verses" use NFTs to carry out their operations.

For example, if the European Commission would create an "EnviroVerse" dedicated to environmental topics, it could create a federation of stakeholders including NGOs, carbon credit buyers, regulatory agencies, and credit issuers. Each of the Commission's stakeholder groups would be able to have its own individual DAO or space that complies with the EnviroVerse. The Commission could spin up an NFT marketplace to certify membership in a particular space or that a particular carbon credit had been authorized and validated. Additionally, a smart contract or oracle could establish that one metric ton of carbon had been removed from the atmosphere, generating an NFT via the platform, which could be sold to a voluntary carbon marketplace.

Minted Vodka Insights

Vitaly Semko of Minted Vodka focused on innovation in NFT creation and interoperability, as well as physical products and services represented and managed as NFTs. For example, MintedVodka is one of the first organizations to mint software in the form of Distributed Autonomous Packages that can be shared as NFTs.

Minting software as NFTs allows small or large software packages to be quickly and effectively distributed and their unique rights and availability to be managed in new ways. This applies not only to consumer software but could also be applied to IoT devices.

Another potential software-related case study applies to open-source. Although much of today's tech innovations are built on open-source software, the creators of open-source software are seldom financially rewarded for it. However, this could change in the future using DLT. For example, when someone pays for a software package, the payment could be distributed automatically in a fair manner along the whole dependency tree of the open-source modules that have been used.

Moreover, Minted Vodka believes that although regulation and oversight are needed, the crypto space is too dynamic, volatile, and beyond the borders of a single country. Also, the necessary regulatory technology and manpower to tackle this are lacking, and if regulators try to push the responsibility for oversight and regulation onto the platforms, they will only scare those platforms away from the reach of regulation. Regulation based on outmoded approaches will only create more bureaucracy, more bad behavior, open loopholes, and

hinder innovation. Minted Vodka believes that an almost automatic oversight opens the doors of innovation by allowing gradual implementation and incentivizing transparent behavior. An example of how this might work as suggested by Minted Vodka is [Walt.id Finance](#), which bridges the gap between traditional finance and cryptocurrency, ensuring transparency, traceability, and compliance in the digital asset world. It focuses on the "edge" of the crypto space, where digital assets interact with the traditional financial system.

3. Embedded supervision and regulation

Embedded supervision was one of the primary topics during the round table. In summary, it refers to a regulatory framework that provides suitable compliance for decentralized markets, allowing them to be automatically monitored by reading their ledger. The ledger contains relevant information for supervision purposes, improving the quality of available data while maintaining privacy and reducing the need for firms to collect, verify and report data to the authorities. To the roundtable participants, the embedded supervision offers an effective technology-neutral regulation so that similar risks are subject to the same rules. However, any discussion on embedded supervision and embedded regulatory action has to take into account new organizational forms, especially the Decentralized Autonomous Organization (DAO), and how they relate to DeFi and Web3. The key to embedded regulation is to think of new organizational forms, e.g. DAOs, and how they connect with DeFi/Web3. In a decentralized context, the collective is responsible, not the individual – this makes it difficult to legislate.

The decentralized nature of the metaverse and Web3 presents unique challenges, and this will have to be taken into account for any regulation. For example, in a decentralized environment, the collective rather than the individual holds legal responsibility and any regulation could backfire if access to data flow storage is not controlled. The danger would be to end up in a surveillance state, where everything is monitored either directly by people or by embedded regulation.

It is important to define the metaverse and Web3 and ensure that, unlike Web2, they remain free from the dominance of big tech companies. The European Commission representative is opposed to the idea of a centralized predominance. Instead, use cases should be defined by industry players including startups, and should include all the different technical elements, including nodes, data storage, oracles, and platforms. From there, this will allow regulators to work out how standards can be set and interoperability ensured. Yet the definition of use cases should not be the task of regulators but of the industry players.

A last point to remember is that not all use cases have the same needs and as such, modularity in the NFT space will become key sooner rather than later. This is a technology that will span industries and any regulation has to be flexible enough to recognize that.

III. Final Remarks for Chapter 2

The roundtable discussed the potential use cases of NFTs beyond the cultural sector and their role in the real economy. The European Commission is exploring the DeFi sector to identify real-economy use cases for NFTs. The experts highlighted the importance of a regulation based on use cases rather than on the underlying technology and the need for industry

standards to differentiate financial use versus non-financial use cases. The roundtable also discussed embedded supervision as a regulatory framework for decentralized markets and emphasized the importance of considering new organizational forms, such as DAOs, in decentralized contexts. Lastly, the roundtable highlighted the importance of modularity in the NFT space and the need to define the metaverse and Web3 while ensuring they remain free from big tech dominance.

In conclusion, more work needs to be done on the legal definition and taxonomy of NFTs and their associated intellectual property rights. Clarification will bring legal certainty and consumer protection.

When it comes to the future of NFT regulation, the European Commission is flexible and willing to listen. Hence it is necessary to organize spaces for dialogue between industry players and policymakers to discuss how regulation in the European Union should evolve – like this roundtable hosted by the IOTA Foundation.

A creative approach to regulation is required, and it is especially important to explore the potential of self-regulatory frameworks in combination with the potential of blockchain technology to enable embedded supervision. Given the wide range of (potential) use cases for NFTs, a one-size-fits-all approach to regulating digital assets would be a mistake, especially given that NFTs are more consumer than financial products and shouldn't primarily fall under financial regulatory logic.

Chapter 3: Tokenization and the Real Economy

In February 2023, the IOTA Foundation conducted a roundtable on regulation in the tokenization space. The participants were: representatives of the European Commission Unit for Markets and Cases III- **Barbara Brandtner, Director for Financial Services and Ernst Ferdinandusse is a Senior Expert in Antitrust at the Payment Systems Unit in DG Competition** Mariana de la Roche, Laura Kajtazi, Anja Raden, Tom Jansson from IOTA Foundation, and Adriana Torres, Maxime Malherbe, and Adriana Torres from FTI Consulting.

The roundtable also included members of the IOTA ecosystem as representatives of the industry: Rob Daykin, Co-Founder of Nakama, a web3 and DeFi builder and venture fund; and Gianfranco Campos, Co-Founder and CEO of Zignar Technologies an organization leading the development of Zentangle, the first data annotation, NFT marketplace and decentralized autonomous organization (DAO) to speed up AI training.

This chapter starts by providing an overview of tokenization (I.), followed by the contributions and remarks of all participants in the roundtable (II) and a summary (III).

I. An Overview of Tokenization

Blockchain tokenization is becoming a popular topic in the context of financial services, real estate, and other aspects that involve traditional assets. Following is a short overview of the different categories of assets that can be tokenized, the advantages and disadvantages of tokenization, and some real-world examples.

> **What is tokenization?**
>
> The tokenization of crypto assets is the process of creating digital tokens that represent ownership of a physical or virtual asset, such as real estate, artwork, or even fiat currencies. These digital tokens are usually created on a blockchain platform and are typically backed by the underlying asset.
>
> The tokenization process typically involves several steps. First, the asset is evaluated to determine its value and ownership rights. Once this is established, the asset is then "tokenized" by creating a digital representation of it on the blockchain. This can involve the creation of a smart contract, which is a self-executing contract that allows for the automatic transfer of ownership when certain conditions are met.
>
> The tokens created through this process are usually transferable and can be traded on digital asset exchanges. Tokenization has gained popularity in recent years as it provides a more efficient and transparent way to buy, sell, and trade assets. It also allows for fractional ownership, which makes investing in expensive assets more accessible to a wider audience.

Tokenization will be key in making the EU more competitive, strategically resilient, and autonomous. It has the potential to provide more liquidity and the ability to use collateral across different time zones, as well as enable faster settlements for quicker asset turnover and, as a result, higher liquidity (this is in line with the aims of the EU's Capital Markets Union Project, which plans to unlock funding for Europe's growth). Supply chains, trade finance, logistics, and public services can all be transformed into seamless and efficient processes through tokenization. Introducing a token economy to financial markets will lead to greater efficiency, increased security, and trust, while significantly reducing complexity.

If Europe can fully leverage the potential of tokenization in the next few years, tokenization will become the backbone of a digitalized industry 4.0 across the economy. Therefore, legislators and regulators play a crucial role in developing a token economy by creating a harmonized legal framework that facilitates innovation and incentivizes corporates and citizens to drive tokenization while maintaining security and protection.

> **Liechtenstein's Blockchain Act: example of a regulation that addresses tokenization**
>
> The Liechtenstein Blockchain Act allows any rights or assets to be tokenized through a Token Container model. Any goods or rights can be tokenized and "loaded" into the container. This enables the right and the asset to be separated and the token to run on a blockchain-based system. This means that the rights and regulations applicable to an asset before it is

tokenized are still enforceable after tokenization, regardless of who owns the asset. Licensed service providers operating as validators must identify the holder of the tokens and ensure the contractual enforcement of the represented real-world rights and obligations in a vault. Validators must establish correct business processes in case of disruption and damages or risk losing their license. With this approach, the Act assigns responsibility to the licensed service providers to guarantee perfect synchrony of the physical and digital worlds through the physical validator. In summary, the licensed service provider as validator has the responsibility of ensuring the fulfillment of the real-world rights and obligations represented in the vault.

However, according to FTI Consulting, there is no legislative approach regulating decentralized finance (DeFi) other than a gatekeeper-based regulation. Liability will be one of the main questions to be addressed as consumers and regulators will want to know what guarantees they are getting and what processes are in place to be protected. Moreover, supervision is at the top of the minds of regulators: can the industry provide solutions, either based on voluntary compliance or to encourage companies to build solutions?

There is a need for definitions to frame the scope of the legislation. While the commonly used concepts and references are highly technical, recent use cases enable understandability for a broader audience. So far, the focus has been on crypto investment and less on DeFi. But regulators could trigger the market's thinking on developing a set of standards if they point to the topics that could benefit from best practices.

Furthermore, policymakers are interested in learning DeFi business models and use cases and are currently scrutinizing the opportunities, risks, and challenges of DeFi.

II.   Remarks and Key Points about Tokenization Discussed at the Roundtable

How tokenization and blockchain combine in the real world

Digital tokens on the chain represent and store the value, history, rights, etc., of the asset off-chain, which continues to exist virtually and in the real world. Any asset, either virtual or 'real world', can be tokenized and registered on the blockchain.

For example, Yenna Tech is a project that utilizes tokenization for financial inclusion in the agriculture industry.

Yenna Tech tokenizes farmland to support farmers by facilitating their access to funding. Properties of farm owners are tokenized and divided into fractions representing the business value, such as plants, crops, or construction of a specific unit of land. The farmland is then offered as tokens for trading at a marketplace. This form of tokenization facilitates access to the farm investment market as it does not require large amounts of capital - one can participate by investing in just a fraction of the farmland. Moreover, it enables micro-financing and the possibility for farmers to raise funds from several investors. The investors receive rewards at the end of the harvest, which can also be tracked transparently, thanks to the combination of tokenization and blockchain. Yenna Tech is built on the Shimmer

network launched by the IOTA Foundation. Automated processes written into smart contracts ensure that the regulatory needs of farmers and investors participating in the marketplace are covered. For example, clients complete KYC, authorized professionals analyze documents to validate the farmland, and the original land documents are secured in a vault.

1. **The need for regulatory clarity and standards**

When approaching blockchain regulation, the DG COMP representative believes that it is crucial to consider the type of system used – open or closed, permissioned or non-permissioned. For example, a more closed system could potentially limit transparency and allow a limited group of participants to control it and limit access to others, raising concerns from a competition perspective. Additionally, the process of developing standards, the governance structure, and compliance measures all play a significant role. The possibility of exchanging sensitive information between members and the interaction of the network with third parties are also important considerations.

The roundtable's industry representatives believe that, as the industry grows rapidly without clear regulations, it will be challenging to develop a transparent and efficient model while being regulatory compliant. They hope that (as seen in MiCA), the EU's focus on standardizing regulation and compliance is not only within the region but worldwide.

The goal is to achieve global harmonization and standardization of regulatory rules for Web3 applications. Launching an application only in the EU and geofencing other jurisdictions is not a practical solution; however, complying with every jurisdiction is currently a complex and challenging task.

The roundtable's industry representatives summarized two needs related to regulations:

- Regulatory clarity and standardization across the globe to ensure developers can build a transparent and efficient model while being regulatory compliant.
- Regulations that apply to Web3 and fit its transparent nature. However, the challenge is that the Web3 space moves quickly, and it is difficult to keep up with the changes.

The industry representatives acknowledged the difficulty facing regulators when trying to understand the nuances of the crypto space and expressed interest in participating in more conversations on the topic.

Pilot Regime Sandbox

(Note: The Pilot Regime Sandbox that will be launched in May should not be confused with the [Regulatory Sandbox](#) to be launched in April)

Alongside MiCA and DORA, the European Commission has introduced a DLT Pilot Regime regulation to create a regulatory sandbox for tokenized securities, which has already passed

the legislative process and started applying in March 2023. The DLT Pilot requires ESMA to assess if the regulatory technical standards (RTS) developed under MiFIR relative to certain pre-and post-trade transparency and data reporting requirements must be adjusted to be effectively applied to securities issued, traded, and recorded on DLT.

Although the sandbox's scope is limited due to asset and product capitalization restrictions, its primary goal is to establish a safe space for experimentation with emerging technologies. The Commission recognizes that the highly regulated nature of the financial services market may hinder the development of DLT-based technologies and has thus sought to overcome such obstacles by creating a conducive environment for innovation.

DG COMP is keen to learn more about industry players' plans for the forthcoming regulatory sandbox and their views on the EU's prudent approach compared to the US. They welcome feedback and insights from the industry on the matter.

One interesting point to outline is the pilot sandbox to be created by the Commission. The pilot regulation establishes a maximum capitalization of six billion euros and lays out exemptions from applicable regulations. To be admitted to the sandbox, interested parties must apply to national competent authorities for trading, settlement, or a combination of both. Once admitted, they will be supervised by the European Securities and Markets Authority. The regulation, which runs over 30 pages, requires platforms to take full liability for the platform, to guarantee that investor money won't be lost, and to convert back to fiat at any given point. The speaker suggests contacting DG FISMA or the competition units for further details.

2. Differences between decentralized and traditional finance

Decentralized finance (DeFi) is fundamentally different from traditional finance. First of all, the organizations at the heart of DeFi are often decentralized and/or rely on decentralized governance. Unlike traditional finance, a decentralized organization can be led globally from any jurisdiction. This is made possible because a decentralized organization offers open access, meaning that one does not need to possess a certain passport to be eligible to join the organization.

Moreover, compared to traditional finance, there is transparency in the number of funds available and their allocation. Thereby it is possible to verify ownership of a given address without having to identify the owner of the funds.

A final key difference is the non-custodial nature of DLT, meaning that users have full control over their assets without handing custody of their funds to a third party.

In summary, these four aspects – decentralization, open access, transparency, and non-custodial control – are the key differences between DeFi and traditional finance. These differences allow for services such as lending and borrowing, asset management, stable coins, decentralized exchanges, and insurance. DeFi has adopted different mechanisms from traditional finance, and regulatory clarity is necessary to provide users with confidence in the event of issues with digital assets or tokens on the network. This would enable law

enforcement to apply users' rights in a manner similar to that of traditional finance but adjusted to the particularities of DeFi.

The idea of multiple communities claiming ownership of the same asset raises concerns over transparency and fraud prevention. Without a clear understanding of who owns the asset, it could be difficult to enforce property rights and ensure consumer protection. While the ease of trading through tokenization may be appealing, the risk of a non-existent asset being traded is a significant issue that must be addressed for the technology to gain widespread acceptance.

However, to address those challenges, it's important to consider the role of the certifier or issuer and ensure trust in the authenticity of the asset. Additionally, various types of rights can be enhanced through tokenization, beyond just property rights. As an example, the industry is moving towards so-called "soulbound" tokens, which are non-transferable tokens that offer more security and guarantees for users in certain use cases.

Moreover, a non-fungible token (NFT) can represent any fiscal asset, including buildings, and provides a clear way to define ownership, especially for digital assets. For example, in the past, trading digital art was difficult due to the lack of transparency and access to ownership records, and digital art could also be copied and an ownership claim made. But now, the transparent ledger provided by NFTs allows for clear ownership of digital art and other digital assets.

NFTs are also transforming the art space by representing physical artworks. The physical artwork is held in custody by a custodian until the digital NFT has been transferred as ownership.

Publicly traded stocks are one of the most sensible assets to tokenize, as they are usually accessible to retail investors. However, there are some complexities around automating the clearing house and certain services such as stamp duty, which can be addressed over time.

It's also important to differentiate utility tokens. These provide access to a product or service and are valued based on the utility of the platform, but do not offer ownership rights. They may provide benefits such as discounts or premium access to features. Stablecoins are another type of token that is pegged to stable assets, such as fiat currency, gold, or another cryptocurrency, and may offer ownership rights, such as the ability to redeem the underlying asset.

Regarding stablecoins, MiCA's Article 44 on issuance and redeemability of electronic money tokens is clear: if a coin corresponds to, for example, one euro and the holder can redeem the coin for one euro, there is no issue. This means that issuers of such e-money tokens should also grant users the right to redeem their tokens at any moment and on par value against the currency referencing those tokens.

On the other hand, MiCA's Recital 50 and Article 21 establish that the issuer of Asset-Referenced Tokens (defined by MiCA as stablecoins pegged to a value of a good other than a fiat currency) can be redeemed either by paying funds other than e-money to an amount equivalent to the market value of the assets referenced by the Asset-Referenced Tokens or by delivering the assets referenced by the token. However, it should always provide an option to

the holder to redeem the token in funds other than e-money that the issuer accepted when selling the token.

Furthermore, it is important to note that there is close collaboration between regulators such as DG FISMA and the Central Bank on the development of a digital euro. Central Bank digital currencies are favored due to the added security provided by having a central bank behind them. However, a cryptocurrency pegged to another cryptocurrency may be less attractive, as it may lack the same level of security.

Tokenization can also automate payments for loans, bonds, and notes, including interest and repayment. This automation can be captured within a token. It can be achieved for example through smart contracts that enforce compliance with rules governing payment terms and asset transfers. For example, the smart contract could restrict asset transfers to certain addresses approved by the regulator, which can help ensure compliance with regulations. This automation can lead to increased efficiencies and exciting possibilities for the future.

Token categories

Fungible assets are not unique and can therefore be replaced by a similar item, like a Euro coin that cannot be distinguished from any other coin. Examples of fungible assets include gold and money that, in most cases, can easily be divided into smaller fractions.

Non-fungible assets are unique and irreplaceable assets that cannot be divided into fractions in the analog world. A famous example of non-fungible assets is the painting of the Mona Lisa. Besides fungible and non-fungible assets, we should also consider *intangible* assets (i.e., assets that lack representation in a physical object), such as patents and copyrights, which can also be tokenized.

Security tokens provide the holder with rights, just like traditional security: for example, the right to a share. However, the definition of security tokens depends on the relevant jurisdiction. The most commonly-applied definition is the US-based Howey Test which defines securities: as "*an investment of money in a common enterprise with a reasonable expectation of profits to be derived from the efforts of others.*" This definition is also used for cryptocurrencies that fall under those characteristics in April 2022 following a speech given by Chair of the US Securities and Exchanges Commission (SEC), Gary Gensler, who said that most crypto tokens likely qualify as investment contracts and, therefore, should be registered with SEC.

Utility tokens give the token holder access to an existing or prospective product or service. These are usually limited to a single network (the issuer) or a closed network linked to the issuer. For example, a tokenized store card, Disney Dollars, or specific gaming tokens might be considered types of utility tokens.

3. Tokenization of assets to enhance competition

According to the DG COMP representative, the European Commission is committed to promoting innovation in financial services through digitalization, DLT, and emerging

technologies, with a focus on improving competition to benefit consumers. However, certain technologies and their applications may pose substantial risks in the current market. Notably, FTX has caused significant financial losses to numerous individuals. To address these concerns, the European Union has adopted a cautious approach by regulating specific aspects of the space, including the Marketing Crypto Assets Regulation (MiCA) and the Digital Operational Resilience Act (DORA). These measures aim to establish a secure environment for trading and settling tokenized assets, including future payments and securities.

> **Digital Operational Resilience Act (DORA)**
>
> The goal of DORA is to set out uniform cyber security requirements for entities operating in the financial sector. The new rules will require financial entities, including CASPs, and third parties providing ICT services to financial entities to set up the appropriate internal governance arrangements and a control framework to ensure the effective and prudent management of all ICT risks. The management body of the financial entities is designated under DORA to define, approve, oversee, and be accountable for the implementation of all ICT risk management framework arrangements. Financial entities will also need to use and maintain updated ICT systems, protocols, and tools to manage and address ICT risks.

The DG COMP representatives reaffirmed the importance of promoting innovation in financial services while ensuring it occurs pro-competitively. One example of its commitment is the preliminary antitrust investigation launched by the European Commission against the stablecoin of Meta (or Facebook, as it was then called) before it was abandoned and sold. DG COMP considered the investigation necessary due to the potential risks associated with tying a new product (in this case, a stable coin payment system) to an already dominant social media platform like Facebook/Meta. The European Commission believes such issues raise classical competition dilemmas and require thorough analysis to ensure that competition occurs on the merits.

Apart from the Facebook/Meta case, there haven't been many instances of competition issues involving new financial products on digital platforms. However, competition principles related to standards-setting and governance still apply to the tokenization of assets, especially when setting up new trading venues or settlement systems. This could lead to classic allegations of price fixing or tying products. If a dominant player like Meta is involved, there could also be concerns about abuse of dominance or foreclosure.

Launching new products by large platforms may lead to rapid scaling and concerns about network effects and tipping markets, requiring close and timely monitoring by competition enforcers. Input from developers is valuable in this process and the DG COMP representative welcomes the IOTA Foundation's initiative as long as it promotes the integration of their principles and combines the traditional approach of looking at markets and market developments with the expertise of those who know how these new technological innovations are developed.

Various social media platforms may introduce their own tokens. To address this, it is important to apply concepts and ideas from other industries to the blockchain space. Transparency is crucial in understanding ownership and development processes, and industry standards should

be established, users and communities educated, and best practices followed, emphasizing security. By focusing on these critical points, organizations can avoid issues like those faced by FTX, and regulators can ensure that these new economies operate responsibly. DG COMP is committed to closely monitoring developments in the financial services and payment space. It aims to gain a better understanding of the technologies and dynamics involved and to be vigilant in monitoring market developments.

After understanding the DG COMP representative's concerns, the industry representative explained that decentralized finance can enhance competition by providing users with services outside the traditional finance market and challenging the small number of dominant players in the industry. Tokenizing assets can increase competition in several ways. For instance, it can provide more trading options for users and enable trading on decentralized exchanges, which are more transparent and efficient. Moreover, decentralized finance can streamline the process of securing loans against assets and reduce the time and cost involved. Similarly, DLT can provide more transparency, efficiency, and cost savings in trading, which is currently a costly and time-consuming experience due to the involvement of Clearing Houses and traditional systems that lack transparency.

As these examples show, adopting DLT brings many advantages, but regulatory and legal uncertainties around tokenizing real-world assets and developing regulatory-compliant DeFi present significant challenges. Overcoming these challenges could attract more investment into the space, drive more competition, and provide end-users with greater choices and cost savings.

In summary, tokenizing assets can increase competition by providing more trading options on decentralized exchanges. Decentralized finance can streamline loan securing and offer cost savings in trading due to more transparency and efficiency provided by DLT.

Blockchain technology and tokenizing real-world assets could increase transparency and provide compliance and regulatory oversight efficiencies. This could help avert crises such as the 2007/2008 credit crisis. For instance, if assets were tokenized, regulators could access real-time immutable information about bank balance sheets. By adopting this technology, companies and regulators can automate a significant portion of the compliance and regulatory oversight function.

Building applications for real-world assets on top of blockchains could be highly beneficial. Developing a regulatory model that provides clarity to developers could provide more liquidity into markets and increase access to users while also automating regulatory functions.

Traditional finance companies are exploring the possibility of tokenization. FTI Consulting believes that tokenization could lead to faster use of capital markets in the next five to 10 years, as younger generations are already trading with currently available tokens on their crypto exchanges. If the real economy were tokenized and traded on these applications, it could unlock many possibilities for European investors and the economy. However, there are already solid rules and methods in place for financial trading due to past financial crises and the need to protect investors.

Some Central Bankers view the intersection of crypto technology with the world of finance as risky, which raises questions about merging the two worlds, and here DG COMP considered that it is important to hear from developers about whether financial rules are too limiting and what is needed to attract traditional finance players to use the technology.

4. Tokenization of a full asset vs fractionalized tokenization

Tokenization enables non-fungible indivisible assets in the analog world (for example, real estate or artwork) to be divided into fractionalized digital tokens. Several people can own an asset through fractional ownership. The value of an asset is broken into fractions representing a certain percentage of the total value, which allows the possibility of having multiple owners of the asset through fractional ownership. Not only does this lower the barrier to investments in these kinds of assets, but it also increases global access to investment opportunities, which promotes financial inclusion and contributes to the democratization of investment. Tokenizing real estate assets lowers the barrier to property investment by enabling people without a large amount of capital to invest in a fraction of the property and enjoy their investment yields without the requirement for complex legal agreements. Moreover, fractional ownership through tokenization increases liquidity as <u>investors can easily and quickly trade their tokens rather than wait years to receive profits from large and illiquid assets</u>.

The DG COMP representative considered the process of transforming shares into tokens and how it would affect the understanding of the asset. If one share equals one token, there is no confusion, and the same applies to collateral, where everyone knows the property's value and market size. However, suppose a tokenized asset is fractionalized, resulting in one asset corresponding to multiple tokens. In that case, this could encourage speculation, according to the DG COMP representative, especially if that asset is a share.

The roundtable's industry representatives agree that one share representing one token is indeed the logical approach. However, even when that is not the case, pure speculation is unlikely to drive the token's value. Moreover, the tokenization of shares can offer benefits like automated dividend payouts, share ownership tracking, and KYC authentication, leading to potential efficiencies. Tokenizing shares may add value to the token by offering more utility to the holder and cost savings for the company. Still, the token value should not exceed the original share value due to speculation. Tokenizing publicly traded stocks is a sensible option as they are accessible to retail investors. Still, there are complexities to automating the clearing and other services such as stamp duty that can be addressed over time.

It is challenging to control situations where multiple networks or communities claim ownership of the same asset and sell that ownership to their members, each with its own methods of enforcing transactions. It is possible that only one of these communities has actual ownership of the asset and can physically control its location or legal ownership, especially if it is a physical asset. In cases like these, it can be challenging to have oversight.

However, blockchain technology offers smart contracts that can enable a degree of enforcement based on data, which is fed to smart contracts through oracles that monitor the real world. The challenge here is to trust the data provided by custodians of the assets to the oracles which feed information to the blockchain so that communities can rely on the network's claims about assets.

5. **The tokenization of real estate assets**

The representative from DG COMP presented another potential use case for tokenization, which involved the tokenization of real estate assets, such as an apartment building. This process would enable the fractional ownership of the building by many individuals. However, DG COMP expressed concerns that this could lead to a disconnection from the actual physical asset and raised questions about who would be responsible for its upkeep. Additionally, they highlighted the potential risk of slicing and packaging assets, as seen in the financial crisis of 2007-2008. To ensure financial and macroeconomic stability, DG COMP stressed the importance of understanding the risks involved in the tokenization process by obtaining feedback and opinions from the DLT space. The roundtable's industry representative clarified that tokenizing real estate enables assets to be fractionalized, allowing individuals to own a portion of an asset they may not have been able to otherwise. However, returning to the example of an apartment building, it is important to comply with real estate fund regulatory and legal obligations and have a manager responsible for overseeing the asset, similar to a real estate fund.

Fractionalizing a real estate asset can make it more accessible to retail investors and potentially increase the asset's total valuation. Ideally, speculation can be limited by regulating how the asset is marketed and whether it complies with the regulatory framework. Hence, it is important to avoid overselling the asset to retail investors in the offering memorandum (which is essentially an investment offering or sales pitch to potential investors that for real estate funds is generally well-regulated to protect investors).

Tokenizing real estate has several benefits, including fractional ownership, increased liquidity, transparency, accessibility, lower costs, increased efficiency, global reach, and asset diversification. It can make real estate investing more accessible, affordable, and diversified, while also reducing transaction costs and increasing transparency and efficiency.

Obligations attached to real-world assets

Owning real assets comes with obligations (real estate taxes, withholding taxes for dividends, voting rights on shares, etc). In the traditional finance world typically these "back office" services are provided by custodians. However, those duties do not disappear with tokenization.

Although complicated, it is possible to automate many of the back office services by writing functions within the smart contract code of the tokens. For example the automation of tax payment or dividends to each holder's blockchain wallet, and independently verifiable blockchain voting. The complexity of this task is ensuring each real asset is dealt with in accordance with local jurisdiction taxes, laws, and regulations.

III. Final Remarks for Chapter 3

Overall, the roundtable discussion on tokenization and its potential use cases highlighted the need for regulatory clarity and global harmonization to provide users with confidence in the event of issues with digital assets or tokens on the network. Tokenization can increase competition and transparency, streamline processes, and promote financial inclusion, but it is crucial to understand the risks involved and comply with regulatory and legal obligations. The roundtable also discussed the importance of distinguishing between open and closed systems, governance structures, and compliance measures, as well as the exchange of sensitive information. Blockchain technology and smart contracts offer a degree of enforcement based on data, but it is essential to trust the data provided by custodians of the assets to the oracles, which feed information to the blockchain. Overall, tokenization presents exciting possibilities for the future of finance and investment, but it is crucial to ensure a responsible and regulated approach to realize its full potential.

Although it represents a small fraction of the finance market, decentralized finance has proliferated and requires increased regulatory scrutiny. It challenges traditional finance by offering more user services and increased competition. When considering the transparency and competition of tokenized assets, it is important to consider factors such as the type of blockchain system used, its development standards, governance structure, and compliance measures. For example, when establishing new trading venues or settlement systems for tokenized assets, competition principles related to standards-setting and governance and concerns about abuse of dominance or foreclosure should be considered, especially with the involvement of dominant players.

Regulatory and legal uncertainty in tokenizing real-world assets poses significant challenges. Overcoming this uncertainty could attract more investment, increase competition, and offer end-users greater choices and cost savings. Developing a transparent regulatory model could provide more liquidity and automate regulatory functions, while decentralized exchanges like UniSwap prevent market manipulation by centralized exchanges like FTX. The EU's efforts to standardize regulations through MiCA are commendable, and developers hope for continued compliance facilitation worldwide.

Establishing a universal set of regulatory rules for Web3 applications to achieve global standardization and regulatory harmony is desired, as it is not feasible to launch applications in one jurisdiction and geofence others while adhering to all jurisdictions' regulations.

Regulators can use tools like asset tokenization to ensure user safety and provide regulatory clarity. Moreover, compliance measures can be incorporated into the tokenization model. For instance, an investor can verify their expertise and KYC with a platform for privately traded stocks. Finally, the potential disadvantages can be overcome through cooperation with stakeholders including regulatory agencies, which is key in the harmonization of rules across the globe. The focus should be on implementing standardized rules through smart contracts and compliance automation based on the transparent nature of blockchains.

Chapter 4: The Cost of Regulation and Uncertainty for SMEs and Startups

In March 2023, the IOTA Foundation conducted a roundtable on the impact of regulation on SMEs and startups in Europe. The participants were: Peter Kerstens, representative of the European Commission, Department for Technological Innovation and Cybersecurity at the European Commission's financial services (DG Fisma); Jan Klesla, member of the Board of Directors of the International Association for Trusted Blockchain Associations (INATBA); Mariana de la Roche, Laura Kajtazi, and Tom Jansson from the IOTA Foundation, and Adriana Torres and Maxime Malherbe from FTI Consulting. The roundtable also included two members of the IOTA ecosystem: Dennis Schouten and Bas van Sambeek from Chunk Works.

This chapter starts by providing I.) an overview of the regulatory landscape for SMEs followed by II.) the remarks of the roundtable

I.   The regulatory landscape for SMEs

On 24 September 2020, the European Commission published its digital finance package which notably included a digital finance strategy and legislative proposals for the Markets in Crypto Assets (MiCA) regulation and digital resilience (DORA).

> **Digital finance package:**
>
> The European Commission's digital finance package seeks to put the European Union at the forefront of the digital transformation of finance while regulating crypto-asset markets and ensuring digital operational resilience. MiCA lays out the EU's regulatory framework for crypto-assets and their service providers in the EU and provides a single licensing regime across all Member States (although DeFi and NFTs are not in the scope of MiCA). DORA sets uniform requirements for the security of network and information systems of companies and organizations operating in the financial sector as well as critical third parties which provide ICT (Information Communication Technologies)-related services to them, such as cloud platforms or data analytics services.

One of the core objectives of the European Commission's Digital Finance Strategy is to unlock new ways of channeling funding to EU businesses, particularly SMEs. This is linked with the EU's objective to foster a thriving environment of technologically-inclined SMEs. Although MiCA was approved in April this year, discussions have already started on MiCA 2.0 and the role of tokenization and decentralized finance (DeFi) in the real economy, particularly among SMEs. However, the fallout from recent shakeups in the crypto sphere has catalyzed a heavy-handed regulatory approach in the EU and abroad to the question of how to ring-fence the use of blockchain in financial markets. This approach could place undue burdens on SMEs. Legislators are worried about risks for investors and the absence of proper safeguards and protection. Regulatory rhetoric around crypto assets has increased following the bankruptcy of

one of the world's largest crypto exchanges. Events like this shift attention onto DeFi, as it is not yet regulated and its potential risks are not fully understood. Besides the purely financial aspects, new legislative proposals such as the [Data Act](#) (which establishes requirements for the design of smart contracts), the [AI Act](#) (which prohibits certain artificial intelligence practices) and the [Product Liability Directive](#) (which would allow compensation for damages caused by any product, including its failures to address cybersecurity vulnerabilities) could further increase the regulatory burden on European SMEs active in the DLT space.

Product Liability Directive:

Published on 28 September 2022 the [revised Product Liability Directive (PLD)](#)aims to make EU consumer protection laws fit for the digital age. It lays down common rules on the liability of economic operators for damage suffered by natural persons caused by defective products. The new rules would allow compensation for damages caused by any product, including its failures to address cybersecurity vulnerabilities. The PLD does not apply to free and open-source software provided outside the course of commercial activity but does apply when software is sold at a price or when personal data is used for purposes other than exclusively for improving the software's security, compatibility, or interoperability. Injured parties could claim compensation if a software causes them damages either when they are used independently (i.e. unhosted wallet) or when they are embedded in other products (i.e. smart contracts). DeFi protocols would thus fall under the software category, being considered a non-tangible product when supplied in the course of a commercial activity.

According to FTI Consulting, policymakers are scrutinizing the nature of DeFi and its opportunities, risks, and challenges. To foster the knowledge of regulators, it is important to provide industry feedback on how the industry envisions regulation.

II.   Key Points Discussed at the Roundtable

The roundtable began by highlighting the rapid regulatory developments in the sector, both current and upcoming, such as a potential MiCA 2.0, as well as the regulatory concerns surrounding DeFi and non-fungible tokens (NFTs). The delicate balance between regulation and innovation was also acknowledged, particularly the need to avoid placing restrictions on innovation while implementing necessary regulations.

1.   Regulatory Challenges for Decentralization and SMEs

SMEs in the DLT and crypto-asset industry face a number of challenges due to the innovative use cases they build and the unclear regulatory landscape. For example, regulatory uncertainty has made it difficult for the roundtable's industry representatives to launch their solution. Clear and nuanced regulation is needed to help SMEs in the industry.

The roundtable's industry representatives have developed a Layer 2 data storage solution that can scale to 30 billion data channels per year, allowing for real-world levels of implementation.

They believe that decentralization is important because a gatekeeper function does not scale well. They argue that using a decentralized solution like a Layer 1 for establishing trust can enable all Internet of Things (IoT) devices certified on the blockchain or the IOTA ledger.

Because the current state of cryptocurrency and decentralized technology is immature, the industry representatives agree with the need for regulation to prevent excesses. Therefore, they have removed the cryptocurrency component that was previously part of their solution and positioned their company as a trust anchor to enable companies to have a contract and Service Level Agreements with them, removing the trustless function that crypto offers.

Regulatory uncertainty has caused the industry representatives to refrain from issuing a token, which has made funding difficult to obtain, as investors from Europe tend to be risk-averse. Regardless of uncertainties and legal issues, they aspire to be a significant player in data storage for the EU.

Layer 1 vs Layer 2

Layer 1, also known as the protocol layer, is the foundational layer of a blockchain network that defines the basic rules and protocols for the network's operation. It consists of the core blockchain architecture and underlying infrastructure, including the consensus mechanism, data structure, and validation rules. Layer 1 is responsible for securing the network, verifying transactions, and maintaining the integrity of the blockchain. It determines the network's performance, scalability, and security, and any changes made to Layer 1 require a hard fork, which is a significant and often controversial process in the blockchain community. Layer 1 is essential for the functionality of the entire blockchain network, and any changes or upgrades made to this layer can have a significant impact on the entire ecosystem. Examples of Layer 1: IOTA, Bitcoin, Ethereum, and Polkadot.

Layer 2 protocols are built on top of Layer 1, normally designed to improve scalability, reduce transaction fees and latency, and enhance the overall user experience of the blockchain. Layer 2 solutions, such as state channels, sidechains, and plasma chains, help to offload transaction processing from Layer 1 while still maintaining security and decentralization. Although Layer 2 is generally less secure than Layer 1, it can still provide a high degree of security and privacy through various mechanisms, such as cryptographic proofs and fraud proofs. Layer 2 plays a critical role in enabling the adoption of decentralized applications and the growth of the blockchain industry. Examples of Layer 2 include Polygon, Arbitrum, and Optimism.

The industry representative explained that the token in their system could have multiple functions. Firstly, it serves as a means of exchange for buying and selling data. Additionally, it has security functions in a permissionless participation system where there needs to be skin in the game. When a node has a deposit at risk, it can be trusted by random users to work in their best interests, ensuring the node behaves honestly to avoid losing the deposit. If a node engages in malicious behavior, the deposit is penalized or "slashed." Therefore, the token serves both as a means of exchange and a security mechanism to ensure honest behavior in the network.

Moreover, they clarified that their solution for decentralized storage does not have a public network yet and that they act as providers. The system slices files into parts called chunks, adds redundant data in the form of parity chunks (Reed-Solomon error codes), and distributes these over a decentralized infrastructure. They identified a potential industry bottleneck in the lack of consideration given to these types of solutions, emphasizing the need for forward-thinking. They were part of a consortium researching privacy data for e-health, where they encountered numerous regulations and certifications that hindered adoption. They believe that there is a huge appeal in decentralized solutions, particularly for SMEs that require enterprise-grade control over data and security. However, there are legal issues and potential conflicts with legislation, particularly around emergency access to data.

> **PiPE Decentralized storage:**
>
> The industry representative explained that their solution for decentralized storage creates a data channel that structures the data within it and then stores this data on a distributed node infrastructure. One of the key features is its indexability, which enables easy access to specific files without having to download the entire blockchain. The solution uses [Read-Solomon error correction](#), which divides data into chunks and distributes them across multiple servers, ensuring redundancy. The client software used by the user is responsible for encrypting and distributing data chunks, and ensuring that the file can still be retrieved even if a data center that stores part of the file is temporarily offline. In the public solution, any server can join the network, and the company currently uses various EU-based storage providers to remove problems with a single hosting provider as a barrier for a user to access data.

To this argument, the regulator mentioned that there are various aspirations and desires, including the idea of granting freedom to individuals and data subjects to control their data and determine where it is stored. However, he pointed out that providing such freedom also means allowing people to operate outside of government control, which some may consider undesirable. He also noted that conflicting objectives arise in legislation, such as the Data Act, where there are discussions about emergency access to data. He suggested that the Data Act does not align with the principles of permissionless distributed ledger technology and that incorporating these principles would require a different approach to legislation

The industry representative pointed out that the Data Act's requirements for emergency access would not be possible with decentralized storage since it requires end-to-end encryption to prohibit any third party from accessing the data. Instead, a data fabric could be created where data markets would always be online, allowing for sufficient data in case of emergencies, as there would be a monetary incentive to sell data. They argued that this market mechanism could eliminate government overreach and address both the concerns of those who want control over their data and those who believe that data is necessary for law enforcement and decision-making. They suggested that having a data fabric where people can choose to keep certain data private, share it with friends, or sell it is technologically possible with decentralized storage and could be a way forward.

Data Act:

Published on 23 February 2023, the [Data Act](#) (DA) proposal lays out rules on who can use and access data generated in the EU across industries. The DA seeks to promote smart contracts interoperability by laying down essential requirements for professionals who create smart contracts for others or integrate them in applications that support the implementation of agreements for sharing data. However, the proposed requirements for interoperability and modifiability of smart contracts will affect their permissionless and decentralized nature. The European Crypto Initiative's Position Paper on the [Data Act](#) highlights that some of the requirements, in particular those incorporated under Article 30, may have a negative effect on the industry and could potentially expose users to additional risks, especially due to the shutdown feature that could be abused or cause damage if inappropriately executed.

They acknowledge that current regulations may not account for decentralized options, but argued that laws are intended to be technology-agnostic and independent of implementation. Hence they called for a move towards a parallel framework that enables decentralized technologies and the reality of owning keys that give access to data. Overall, they highlighted the potential of decentralized storage and the need for a regulatory framework that embraces these technologies while balancing the concerns of individuals and government entities.

The regulator emphasized that laws are not truly technology-neutral or agnostic, despite aspirational statements to the contrary. Instead, they are influenced by the state of technology at the time of their creation, often requiring or assuming the use of specific technology. This ties laws inherently to the prevailing technological landscape and may result in increasing regulatory costs over time, especially when innovations necessitate adapting existing practices. The regulator also highlighted how laws reflect the dominant design in a field, which becomes entrenched even as technology progresses. Changing this practice is difficult and leads to higher regulatory costs. While the regulator suggested focusing regulations on principles and behaviors rather than specific rules, they acknowledged that most regulations tend to be technology-specific and rule-based.

Two points were raised here. Firstly, there is an increased effort to involve smaller players and startups in discussions and events (such as the current series of roundtables organized by the IOTA Foundation and FTI Consulting). Efforts like these bring fresh perspectives not only on the current state of technology but also its future trajectory. Secondly, the idea of regulation based on principles that allows space for development and growth (particularly in the context of "DeFi") was supported. Specifically, avoiding strict and limiting rules for those already in the DeFi space was cited as an important way to allow innovation to flourish without undue restrictions.

The roundtable's INATBA representative described his organization's work in producing principles and ground rules for the industry to incentivize adoption. He argued that the DeFi industry should adopt principles and ground rules to enable self-regulation, which will support small players and nurture startups. The representative applauded the effort of the EU to

explore DeFi and create a flexible regime to achieve strategic autonomy, similar to the UK's approach. The need for a dynamic and flexible approach was emphasized, as well as the need to consider the industry's input to develop self-certification and peer review of DeFi protocols. Moreover, he suggested that the industry should learn from other areas of IT and avoid the over-regulation seen in the AI Act.

> **AI Act:**
>
> Published on 20 July 2021, the [AI Act](#) proposal **aims to ensure that AI systems in Europe are safe, lawful, and in line with EU fundamental rights.** It lays down prohibitions of certain artificial intelligence practices and establishes specific requirements for high-risk AI systems and obligations for operators of such systems. It also includes harmonized transparency rules for AI systems intended to interact with natural persons and lays down rules on market monitoring and surveillance. **It envisages the creation of coordinated AI regulatory sandboxes to experiment with new technologies, including blockchain, under regulatory supervision.**

2. Incentivizing Self-Regulation

This section discusses the impact of regulatory frameworks on SMEs, focusing on a proposed DLT-based compliance system. This approach offers flexibility and alleviates the need for detailed legislation. Support for this framework emphasizes the potential of DLT-based industries to create responsible practices within set guidelines. A cautious approach to DeFi regulation is advised, highlighting the need to balance societal goals and innovation while considering political perspectives.

The industry representative suggested a proactive approach to regulation. Instead of reactive legislation, they proposed the certification of rule sets for specific applications or demanding certain changes to rules. This approach would combine contractual agreements with legal requirements, providing individuals with the freedom to choose which set of rules apply best to their situation while adhering to certification processes demanded by regulators. The industry representative illustrated the concept by discussing his work on addressing bias in AI models. He emphasized the need for rules to mitigate bias and suggested that the EU could require compliance with an unbiased data set and establish rules to ensure compliance. These rules could be certified within individual frameworks without the need for the EU to legislate every detail.

The INATBA representative responded to these ideas, expressing his enthusiasm for implementing such a framework for Europe's AI and other industries. However, the unique position of the finance industry, which requires complementing financial regulation, was highlighted. Even if not directly involved in finance, other industries are often regulated within the framework of financial regulations. Hence, the INATBA representative envisioned a scenario where primary laws and principles are established and accompanied by financial regulations and other regulatory regimes like the Data Act for smart contracts. Within these boundaries, there is ample room for the DLT industry to demonstrate responsible practices and establish boundaries, particularly in DeFi.

The regulator took the opportunity to reflect on the nature of regulation, considering the problems it aims to address. He acknowledged that regulations can have positive and negative consequences, as they create rules that people must comply with, which can benefit some while limiting others. The problems that regulations seek to resolve include market failures, societally undesirable consequences such as privacy leaks, and legal uncertainty that requires clarity. However, the pursuit of clarity through regulation also imposes limitations. He provided insights into the financial industry's experience with regulation, noting that it often follows cycles. Initially, regulations aimed at promoting the competitiveness of the European financial market. However, the financial crisis prompted a shift towards prioritizing financial stability, leading to increased regulations. Subsequently, as the crisis subsided, the focus shifted to fostering innovation and accommodating crypto activity within the EU. But even these regulations act as a straight jacket, particularly affecting smaller enterprises that struggle to absorb compliance costs. Innovative SMEs, which push boundaries and operate at the edges of what is allowed, face challenges due to the high costs associated with compliance.

Regarding developments in DeFi, the regulator advocated for a cautious approach, suggesting that regulation should only be considered once problems emerge. He emphasized the disparity between what the European Commission proposes and what ultimately gets enacted by the European Parliament and Council of the EU, which can lead to varying outcomes. The regulator acknowledged the potential negative consequences of regulations borne by the industry and innovators, who must navigate costly implementations or face limitations on innovation.

While acknowledging the risks and drawbacks of regulation, the regulator stated that the decision to regulate ultimately depends on the societal objective pursued and its magnitude compared to the costs imposed on society and innovation. Different political perspectives shape individuals' tolerance for imposing costs on society and industry in pursuit of desired outcomes. Those with liberal views tend to have a lower tolerance for such costs, while interventionists accept higher costs to address undesirable outcomes.

The regulator concluded that regulation often leads to costs and constraints, and the only solution to mitigate these issues is to avoid excessive regulation. The decision to regulate should carefully consider the balance between societal objectives and the limitations imposed on creativity and innovation. Different political perspectives influence this balance, as some prioritize avoiding costs while others accept them for the sake of correcting undesirable outcomes.

3. Regulatory Sandboxes: Finding Clarity and Advice For SMEs and Regulators

The European Blockchain Regulatory Sandbox can play an important role in addressing regulatory uncertainty for SMEs by clarifying regulatory complexities and fostering dialogue among regulators. Although there are problems in applying the sandbox across borders and its inability to shield against future regulations is also noted, innovators are encouraged to utilize it to minimize legal and regulatory risks.

The industry representative mentioned their application to the EU Blockchain Regulatory Sandbox, which is designed to provide access to legal counsel and help clarify the extent to which they are pushing boundaries. They described this initiative as a smart approach by the

EU that enables a better understanding of the underlying problems, leading to more accurate and proportionate laws.

European Blockchain Regulatory Sandbox

The European Blockchain Sandbox has been created to facilitate dialogue between regulators and innovators for private and public sector use cases. Legal advice and regulatory guidance will be provided in a safe and confidential environment.

The European Blockchain Regulatory Sandbox for innovative use cases involving Distributed Ledger Technologies (DLT) is an initiative of the European Commission. The sandbox establishes a pan-European framework for regulatory dialogues to increase legal certainty for innovative blockchain technology solutions.

The industry representative also emphasized that the European Commission and EU regulators can engage in dialogue with any entity that acknowledges itself as a risk factor in order to better understand their objectives. This approach aims to foster supportive laws while enabling stronger regulation of those who refuse to comply or acknowledge their risk factor. The sandbox's potential as an innovative tool to facilitate the transition from one phase of innovation to another was also acknowledged.

To these remarks, the regulator explained the purpose of the regulatory sandbox as an advisory function, developed because of a recurring problem of misapplication, blunt interpretation, or misguided enforcement of rules. The sandbox embodies what the regulator referred to as the "Dalai Lama principle": understanding the rules well to break them appropriately. He noted that individuals often approach regulators with concerns about certain actions not being allowed, even if the rules do not explicitly prohibit them. With the guidance of competent legal counsel, individuals can navigate the boundaries of permissibility and distinguish between what is within the rules and what goes beyond.

Another aspect of the sandbox is engagement with national regulators to discuss the intentions and objectives of the innovation under scrutiny. The regulator noted that more countries have recently adopted a supportive mindset toward innovators, aiming to guide them through the complexities of regulatory and policy frameworks without necessarily changing the existing rules.

The IOTA Foundation representative described scenarios where the focus of the regulatory sandbox is not on how to comply with existing regulations, but on cases where there is no regulation to comply with. Innovators might be concerned about developing a solution only to have a regulation introduced afterward, which could potentially invalidate their work from the past year.

The regulator answered by explaining that a sandbox cannot protect future regulations because the regulators behind the sandbox are not the ones who create rules; rather, regulations are typically established by policymakers. If an area is not regulated, there are no laws to break and innovators are free to do as they please. However, the challenge lies in

knowing whether an area is regulated or not, and understanding how it is regulated, which is often a complex question.

The INATBA representative emphasized that the European Blockchain Sandbox operates independently from regulators or supervisory bodies. The sandbox's main purpose is to facilitate connections with sandboxes in different countries, but the Commission lacks the authority to enforce this and expanding across countries can be challenging because of Europe's fragmentation. Additionally, the sandboxes themselves can vary significantly. The INATBA representative believes in the sandbox's cross-sectoral and cross-border concept, and that the industry could assist regulators in navigating these complexities.

To those remarks, the industry representative emphasized the importance of having a clear understanding of the legal landscape, even during the negotiation phase. They believe that supporting innovators throughout the legislative process, whether through a sandbox or community dialogue, is crucial. They also mentioned the significance of aligning European values of mutual care to foster innovation, allowing entrepreneurs to make informed decisions based on their risk appetite and compatibility with their objectives.

4. Building Innovation: Moving Beyond Speculation in DLT

Regulation in the crypto-asset industry must recognise the utility of crypto currency and NFTs rather than focusing solely on speculative activities. A cautious regulatory approach may hinder innovation rather than encourage it. In the US, investors beyond the blockchain industry have generally been more risk-tolerant than in Europe. This regulatory uncertainty poses a cost for SMEs, as they may abandon interesting ideas due to regulatory concerns and lack of investment.

The industry representative emphasized that cryptocurrency serves as a foundational layer of DLT but does not encompass the entirety of the technology. Once the foundational layer is established and the legal perspective on decentralized finance (DeFi) is defined, the focus can shift towards building applications such as data storage and open data markets. They also expressed their belief that NFTs have the potential to become a cultural phenomenon beyond their financial aspects. While there is currently a strong focus on speculating on high-value NFTs, the concept of tokens connecting individuals to intellectual property is intriguing regardless of the token's price. They cautioned against regulating the technology solely from a financial standpoint and encouraged considering the utility that the technology can offer.

The regulator acknowledged the valid point raised by the industry representative and shared his observations during the development of MiCA, where he noticed that the market implementation of DLT was primarily focused on speculative activities rather than building useful applications. Many token issuers were more interested in the token's market value than in developing utility. He argued that building utility should be the primary focus, as the token's value would naturally follow. Moreover, he expressed regret over interesting ideas being abandoned because developers became too fixated on token value and market capitalization instead of infrastructure development.

As an illustration, the regulator mentioned the case of Maersk, a container company, which partnered with IBM to create a DLT-based tracking system for containers. However, despite the system's success, Maersk decided to discontinue it due to insufficient benefits compared to using a centralized database. The regulator recognized the inherent cost of innovation, where experimentation is followed by an assessment, and described this as the cost of innovation: Entrepreneurship involves taking calculated risks and making informed judgments.

While acknowledging the potential for disagreement among some of his colleagues, the regulator advocated the principle of "innovate first, ask for permission later". The US was described as having greater tolerance for risk compared to Europe, where there is less willingness to invest in untested ideas from both regulatory and business perspectives. The regulator lamented this cautious approach, considering that true success can only be determined by rolling out ideas in the market and observing their performance.

To this point, the industry representative replied that their approach was always to not seek funding unless they were confident that they could deliver on their promises, an attitude founded on their care for their community and unwillingness to mismanage their funds. The invited regulator praised this approach as it aligns with European values. The regulator mentioned that in contrast, American innovators are often willing to accept money without providing guarantees or ensuring much transparency, which according to the IOTA representative, is a clear mirror of the current industry situation in the EU and USA.

Final remarks for Chapter 4

The roundtable provided insights into the regulatory challenges faced by companies in the decentralized technology and cryptocurrency space. Participants underlined the importance of balancing innovation and regulation, as well as the potential impact on SMEs in the DeFi industry. The discussion emphasized the need for a dynamic and flexible regulatory regime that promotes innovation while ensuring necessary regulations are in place.

The industry representative emphasized the importance of balancing innovation and regulation, considering the potential impact of regulations on SMEs. The industry representative also outlined the need for transparency throughout the development process, from code reviews to public audits, as it builds trust and can lead to better outcomes. They also stressed the importance of understanding the legal landscape and conducting risk assessments to ensure that innovation fits into an existing system of regulation and behavior. Moreover, they emphasized the significance of aligning European values of mutual care to foster innovation, allowing entrepreneurs to make informed decisions based on their risk appetite and compatibility with their objectives.

The regulator emphasized the importance of building utility in decentralized technology rather than focusing solely on speculative activities and token value. Building utility should be the primary focus, as the token's value would naturally follow. The regulator expressed regret over interesting ideas being abandoned because developers became too fixated on token value and market capitalization instead of infrastructure development. The regulator's point of view is one of caution and balance, recognizing the potential benefits of decentralized technology but also the need for regulation to address potential legal issues and conflicts with legislation. In that

sense, the regulator advocates for a shift towards building useful applications rather than focusing solely on token value and market capitalization, as well as a cautious approach to regulation that acknowledges the cost of innovation and the competing objectives of government control and individual freedom.

Moreover, the sandbox is seen as a valuable tool for guiding innovators and promoting innovation, but it cannot protect against future regulations or changes in regulations. Innovators must evaluate risks and determine if pursuing certain endeavors is worth the potential legal consequences. The sandbox model aims to promote innovation while ensuring compliance with existing rules, and it provides an opportunity for innovators to demonstrate transparency and establish trust with regulators and society. The INATBA representative believes that the industry could assist regulators in navigating these complexities, and the sandbox's cross-sectoral and cross-border concept could facilitate connections with sandboxes in different countries.

Overall, the discussion emphasized the importance of collaboration and dialogue between innovators, regulators, and society to create a regulatory framework that fosters innovation while addressing societal concerns.

Full biographies of speakers and organizers

Policymakers and regulators:

Barbara Brandtner, Director for Financial Services- Directorate General for Competition (DG COMP). European Commission

Barbara Brandtner has more than 25 years of experience in the European Commission, of which close to 14 involve handling competition cases, with a particular emphasis on State aid and antitrust. She holds law degrees from the University of Vienna and the College of Europe and has an LL.M. from Michigan Law School. Following activities in the national Foreign Service and private practice, she joined the Commission's Legal Service in 1996 and held positions in several cabinets, including as Deputy Head of Cabinet of Competition Commissioner Neelie Kroes. Following assignments as Head of Unit for State aid enforcement and Procedural Reform (2008-2013), Resources, Ethics and Security (2013-2016) and State aid Strategy, including the implementation of the post-Modernization Partnerships with the Member States, Transparency and Evaluation, she is now Head of Unit for Markets and Cases III: Financial Services, Antitrust: Payments Systems at the Directorate General for Competition. This Commission department is responsible for EU policy on competition and for enforcing EU competition rules, in cooperation with national competition authorities.

[Ernst Ferdinandusse](), European Commission- DG Competition

Ernst Ferdinandusse is a Senior Expert in Antitrust at the Payment Systems Unit in DG Competition (DG COMP). Prior to DG COMP, he has been legal advisor at DG Research and Innovation. Ferdinandusse has vast experience in the European Commission, principally in the competition field where he has served as a Case handler of antitrust in the manufacturing and consumer goods sectors and mergers in the service sector. Ernst graduated in law and holds a Master's Degree in European Law from the College of Europe.

Joachim Schwerin, Principal Economist in the Unit responsible for the Digital Transformation of Industry within the Directorate-General Internal Market, Industry, Entrepreneurship and SMEs (DG GROW) - European Commission

Joachim Schwerin is the Principal Economist in the unit responsible for the Digital Transformation of Industry within the Directorate-General Internal Market, Industry, Entrepreneurship and SMEs (DG GROW) of the European Commission. He is responsible for developing the policy approach of DG GROW towards the Token Economy and Distributed Ledger Technologies as well as their applications for industry and Small and Midsize Enterprizes (SMEs). In 2020, he coordinated DG GROW's input into the Digital Finance Strategy, including the Markets in Crypto-Assets (MiCA) regulation. Previous responsibilities in the European Commission (which he joined in 2001) include the coordination of industrial and competition policy, the design of policy measures to improve SME access to digital finance and conceptual work on strategic aspects of the EU's competitiveness in the global economy. Joachim holds a PhD in economics from Dresden University of Technology and was Post-Doc Research Fellow at the London School of Economics.

Marius Kat, Head Parliamentary Assistant to MEP Paul Tang (SnD, NL), European Parliament

Marius Kat is the Head Parliamentary Assistant to Member of European Parliament (MEP) Paul Tang (SnD, NL) since 2019, focussing on matters linked to the Economic and Monetary Affairs (ECON) and Taxation (FISC) committees. Paul Tang is one of the leading voices in the parliament advocating for strict *de maximis* controls for crypto-assets and unhosted wallets. During the Transfer of Funds Regulation (TFR) negotiations both within the parliament and during trilogues, Marius assisted MEP Tang in hearing industry concerns, drafting the amendments and negotiating with the other MEPs in order to arrive to a final text. Prior to this, Marius was part of the campaign management team of the SnD from 2018 to 2019. Before this, he held roles in public affairs consultancies in the Netherlands. He holds a Bachelor of Arts from Oxford University and dual masters in Public Policy from Hertie School and Science Po Paris.

Peter Kerstens, DG FISMA, European Commission
Peter Kerstens is special advisor for Technological Innovation and Cybersecurity at the European Commission's financial services department DG FISMA). He led work on the European Commission's Fintech Action Plan and Digital Finance Strategy and co-chairs the European Commission's Fintech Taskforce. Kerstens has experience in a wide variety of fields, including single market, financial services, digitalisation, security, foreign policy sanctions, consumer protection as well as health and food safety. Earlier in his career, Peter was Finance

Counsellor at the EU Embassy in Washington DC. He has also been a member of the private offices of the Commissioner for the internal market and services (Charles McCreevy) and the commissioner for health and consumer protection (David Byrne). Before joining the European Commission in 1996, Kerstens advised major corporations on EU policy and regulatory affairs. Kerstens is a guest lecturer at the European University Institute in Florence, the European Law Academy in Trier and Georgetown Law. He is also Adjunct Professor at Vanderbilt Law School. He is a Dutch national and holds double magna cum laude master degrees in European affairs and political science from the College of Europe in Bruges and the University of Leuven, Belgium.

Industry experts outside of the IOTA ecosystem:

[Jan Klesla,](#) **Co-Founder, Blockchain Republic/ Advisor to the Czech Ministry of Industry and Trade/ Co-chair of the Finance sub-working group on DeFi and Web3, INATBA.** Jan is a co-founder of the Blockchain Republic, a non-profit organization that supports blockchain businesses in the EU and CEE. He is also a senior policy advisor to the Ministries of Economy and Finance in the Czech Republic, where he serves as the co-chair of the European Blockchain Partnership. Jan is also the co-chair of the Finance sub-working group at the International Association for Trusted Blockchain Applications (INATBA), a global forum for blockchain industry representatives. The SWG3 focuses on web3, DeFi, DAO, and the recently published series of policy papers on DeFi, DAO, NFTs, and regulatory sandboxes. Jan is a lawyer by training, worked as an IT/economic editor and policy commentator, and co-founded a fintech startup in New York City.

[Jeff Bandman](#), **Principal, Bandman Advisors and Member of the Consultative Working Group for ESMA's Financial Innovation Standing Committee, European Securities and Markets Authority (ESMA).** Jeff Bandman is Founder and Principal of Bandman Advisors, an advisory practice helping clients ranging from governments to start ups to global firms meet strategic innovation and regulatory challenges. He is COO and General Counsel of 6529 Holdings. He is also co-founder of the GBBC Digital Finance Initiative to establish an industry-driven global code of conduct for crypto assets and co-chairs its quarterly closed user group regulator forum.. At Yale University, he was a lecturer in Global Affairs on Cryptoassets, Blockchain, and Public Policy teaching a senior Capstone seminar in the Yale Jackson Institute for Global Affairs. Jeff was a senior official at the U.S. Commodity Futures Trading Commission from 2014-2017. As FinTech Advisor to Chairman Giancarlo, he was the Founding Director and architect of LabCFTC, the CFTC's hub for engagement with FinTech innovation. He chaired the CFTC blockchain, virtual currency, and FinTech working group from inception. He was Special Counsel to Chairman Timothy Massad, led the CFTC Office of International Affairs, & led the CFTC Division of Clearing and Risk, which oversees many of the world's largest clearinghouses. He led negotiations resulting in "Clearinghouse Equivalence" with the European Commission. Jeff worked in the financial industry in New York and London as an attorney and business executive. He led market structure initiatives and rebuilt Cantor Fitzgerald's market data business after the events of September 11, 2001. He graduated from Yale magna cum laude, with honors in History and English, and from Stanford Law School with honors as a member of the "Order of the Coif".

IOTA community industry experts:

BackupDev/Minted Vodka

BackupDev is a German company that builds and operates multi-chain NFT platform MintedVodka (https://minted.vodka). It focuses on innovation in NFT creation, interoperability and new use cases. Some of the innovations include software minted as NFTs and physical products/services represented and managed as NFTs.

- **Vitaly Semko, Founder, BackupDev/Minted Vodka.** Vitaly Semko has been working for over a decade as a freelance software developer and IT consultant. He has participated in dozens of high-profile projects from different industries/sectors: banking, health-care, retail, marketing research, telecommunications, governmental agencies, etc. Since 2017, Vitaly has been also involved in blockchain-related solutions development, such asProof of Concept projects for the energy sector or smart cities. Since 2021, Vitaly works on NFT-related innovations as a part of a small company in Leipzig, Germany.

Chunk Works and PIPE

Chunk Works (https://chunkworks.net/) provides people and organizations with the tools they need to retain control over their cloud data in a safe, reliable, and cost-effective way. Its goal is to contribute to a more secure and equitable digital future because data breaches and hacks are no longer a question of "if" but "when".

PIPE offers open source, decentralized data storage and transfers with a focus on user experience. This open protocol solves the problem of how to store and transfer immutable, decentralized data for millions of machines, messages, or megabytes. PIPE aims to transform online data ownership by putting control back into the hands of the users.

- **Bas van Sambeek, Communication Strategist, Chunk Works:** Bas specializes in high-tech startup positioning. He combines business development skills with storytelling to make a good product sell well. His interests in technology, privacy, and startups led him to the cryptocurrency world, where he is a part of the movement to elevate cryptocurrency beyond its speculative nature.

- **Dennis Schouten, Co-founder & Partner Manager, Chunk Works:** Dennis has been a business developer in the IoT/DLT industry since 2017. His career started within the IT/implementation industry, targeted towards retailers. His strong strategy and network-building skills help him identify common interests and align partners in the decentralized data ecosystem.

Firefly Wallet

Firefly (https://firefly.iota.org) is an open-source, secure and lightweight digital wallet for managing cryptocurrency tokens. With a mobile and desktop app, Firefly has ~50K users. Firefly allows users to send and receive tokens with zero fees in seconds, with a clean, minimalistic UI, seamless usability, and industry-leading security. Features extend beyond simple cryptocurrency payments to include staking tokens and participating in governance

decisions through a decentralized voting system. Future features include decentralized identity, NFT management and the ability to purchase cryptocurrency with a credit/debit card.

- **[Charlie Varley](...)**, **Director of Engineering, Firefly.** Charlie Varley has over five years' experience building wallet software within the cryptocurrency space. He is a Director of Engineering at the IOTA Foundation and envisions a not-so-distant future where digital wallets form a key component in finance and commerce, digital identity and peer-to-peer communication.

Nakama

Nakama (https://nakama.io/) is a thesis-driven, long-term focused web3 builder (inclusive of DeFi) and venture fund. They partner closely with the projects they invest in or incubate and actively participate in their governance, community-management and adoption. Their mission is to create value for all stakeholders and help crypto move away from value extraction, towards value creation and sustainable token economies.

- **[Rob Daykin](...)**, **Co-Founder, Nakama:** Robert has 15 years of experience in Fund Finance working across London and Jersey and has been actively involved in crypto since 2015, becoming interested in DeFi as an early investor in ETH Lend in 2017which later became Aave. He has since advised projects in DeFi focusing on creating fairer economic models for all stakeholders. He has also recently started advising the IOTA Foundation in creating a sustainable web3 ecosystem on their upcoming smart contract ecosystem.

SoonLabs

SoonLabs (https://soonaverse.com) is the creator of the Soonaverse, a platform for communities to create and manage DAOs, NFTs, projects, companies, and markets, on the feeless infrastructure of the Shimmer and IOTA networks. Any organization can launch and trade liquid assets through SoonLab's Marketplace, Launchpad, and Token Exchange products.

- **[Song Choi](...)**, **Head of Marketing/Founder, SoonLabs:** Song Choi is a marketing, sales and technology professional with over two decades of experience managing local, national and global brands. He has held key positions in a diverse set of industries, including the SVP of Marketing for a multi-billion dollar bank in the Pacific Region of the United States. He is the founder of several Web3 start ups including SoonStudios and the Token Exchange.

Zignar Technologies

Zignar Technologies (https://zignar.tech) is actively leading the development of the first Data Annotation and NFT Marketplace and decentralized autonomous organization- DAO to speed up the training of Artificial Intelligence. Annotated data sets are completed by users and consumed by researchers in a decentralized fashion. NFTs represent and trace the origin and ownership of these data sets to bring reliability to the input data for the training of Artificial Intelligence.

- **Gianfranco Campos, Co-Founder and CEO, Zignar Technologies:** Gianfranco Campos leads a distributed team around the world in six countries. Gianfranco has more than 15 years of action in the technology industry, with significant experience in Distributed Ledger Technologies, Coaching and Leadership, Investment Strategies, Project Management, Organization Transformation, and Agriculture. Gianfranco is an active member of the IOTA Evangelist Network and a Systems Engineer focused on providing solutions for the Systems Engineer focused on providing solutions for the machine economy.

FTI Consulting coordination team:

Adriana Torres Vergara, Senior Consultant FTI Consulting, Brussels. Adriana is experienced in Political Intelligence and Public Affairs, having worked in International Organizations, Public Bodies and Consultancies in Europe and in Latin America delivering strategic analysis and Public Affairs counsel. Her main policy focus is on Digital Finance, having provided strategic advisory work in the field of Crypto regulation. She works with a number of financial services and crypto industry clients on developing and implementing their EU public policy strategies

Dea Markova, Managing Director, Forefront Advisers, Brussels. Dea led advocacy campaigns for the centralized and decentralized industry during the EU crypto rulebook negotiations. She moved back to the EU from the FinTech team of the Monetary Authority of Singapore. Prior, she headed programmes for Innovate Finance, the UK FinTech trade association. She has 12 years of experience in financial services and regulation.

Kristina Budrytė-Ridard, Managing Director FTI Consulting, Brussels. Kristina has 10+ years of consulting experience both advising clients on public affairs as well as on legal issues. She works with a number of financial services and crypto industry clients on developing and implementing their public policy strategies at EU and national level.

Maxime Malherbe, Director FTI Consulting, Brussels. Maxime advised public and private sector actors on public affairs and communications during the EU Crypto Framework and Anti-Money Laundering package negotiations. He works with several DeFI clients on developing public policy strategies in preparation of upcoming legislation.

IOTA Foundation's Team:

Mariana de la Roche, Senior Regulatory Affairs Expert, IOTA Foundation / Board of Directors and Co-chair of the social impact and sustainability working group, INATBA. Member of the Expert Panel, EUBOF.

Mariana de la Roche is the Senior Regulatory Affairs Expert of the IOTA Foundation and a member of the Board of Directors of INATBA. She is a Colombian human rights lawyer with a law degree obtained with academic excellence, a specialization in human rights and humanitarian law, and a master's degree in public administration. Since 2021 Mariana has been leading the actions of the social impact and sustainability working group of INATBA. Mariana is also part of the leading team coordinating BC100+, an initiative supported by the UN's General

Assembly to advocate for BC for the UN Charter Values and the 2030 Agenda. Lastly, since 2023 she is part of the Expert Panel of the EUBOF and one of the ambassadors of the Global Blockchain Business Council (GBBC).

Laura Kajtazi, Project and Regulatory Affairs Manager, IOTA Foundation. Member of the Expert Panel, EUBOF.

Laura Kajtazi is Project and Regulatory Affairs Manager at the IOTA Foundation and member of the Identity Working Group at INATBA. Before joining the IOTA Foundation, Laura completed her Master Programme in International Economics and Management at the University of Paderborn, Germany. In her studies, she discovered her passion for entrepreneurship and macroeconomics and began to work in the crypto area from an entrepreneurial and monetary policy perspective. During her Master studies, she was employed by the IOTA Foundation as a working student where she gained insights into the benefits of Distributed Ledger Technologies for different sectors such as health technology, sustainability, global trade and supply chains.

David Phillips, Editor, IOTA Foundation

David Phillips is an editor at the IOTA Foundation, where he develops content, communications, and messaging that engages audiences and conveys the story of IOTA. David has a diverse background in print and online editorial work, corporate communications and event producing, social media management and content creation.

Tom Jansson, Head of Legal & Regulatory Affairs, IOTA Foundation

Tom Jansson is Head of Legal and Regulatory Affairs at the IOTA Foundation. He is a qualified lawyer with extensive in-house and private practice experience and advises the foundation on a wide range of legal and regulatory topics, including the Markets in Crypto-assets Regulation (MiCA) and other regulatory initiatives related to the crypto-asset industry.

Dr. Anja Raden, Executive Director of Legal and Regulatory Affairs, IOTA Foundation

Anja Raden is responsible for the Legal and Regulatory Affairs Department of the IOTA Foundation. She is a fully qualified lawyer with over 15 years of work experience in the public and private sectors. She has been actively involved in Crypto since 2018 and is a board member of Blockchain Bundesverband.