Article Information

Authors: Steven Pettigrove, Jake Huang, Kelly Kim, Luke Higgins, Luke Misthos, Michael Bacina, Tim Masters
Service: Blockchain, FinTech
Sector: Financial Services, IT & Telecommunications

Blockchain Bites: ANZ and Chainlink forging blockchain real world asset strength, Bear market spirit: Latest from Token2049, MiCA stablecoins requirements on the horizon, Crypto comments from Gensler's SEC testimony, Stoner Cats NFT called securities by SEC, IOSCO Consultation on 2023 DeFi Report, Personal Transaction Data Dive Deep in Vitalik's Privacy Pools, US CFTC targets DeFi platforms, Rekt Test: building safety via security

Michael Bacina, Steven Pettigrove, Tim Masters, Jake Huang, Luke Higgins, Luke Misthos and Kelly Kim of the Piper Alderman Blockchain Group bring you the latest legal, regulatory and project updates in Blockchain and Digital Law.

ANZ and Chainlink forging blockchain real world asset strength with live transactions

ANZ Bank, one of Australia's "big four" banks, which has had a forward thinking posture towards blockchain and crypto-assets, has announced that it has completed a pilot building on lessons learned from a SWIFT blockchain interoperability test which took place earlier this year and followed an announcement by SWIFT late last year around the adoption of blockchain technology.

In a press release, Mr Nigel Dobson of ANZ said:

> *Banks are increasingly exploring use cases involving tokenised assets, with 93 per cent of institutional investors believing in their long-term value, according to a recent EY report.*

Mr Dobson cited the Bank of International Settlement's comments that a "unified ledger" representing a new kind of financial market infrastructure could enable the benefits of tokenisation "by combining central bank money, tokenised deposits and tokenised assets on a programmable platform".

By using Chainlink's Cross-Chain Interoperability Protocol (**CCIP**) ANZ worked:

> *to complete a test transaction to simulate the purchase of a tokenised asset, facilitated using A$DC and an ANZ-issued NZ-dollar-denominated stablecoin. This transaction involved technical integration of ANZ's digital asset services technology stack with CCIP to realise cross-chain settlement of tokenised assets securely and efficiently.*

This kind of TradFi usage of blockchain and crypto-asset technology are important steps to help move the industry past tired past narratives and truly unlock the benefits of tokenised real-world assets and upgrade our current financial infrastructure.

By Michael Bacina

Bear market spirit: Latest from Token2049

10,000 crypto developers, traders, builders, VCs, and a few lawyers descended on Singapore this week for TOKEN2049, reputedly the world's largest crypto conference. The conference hosted big name speakers such as Balaji Srinivasan, Chaoping Zhao, the Winklevoss twins, Jeremy Allaire, Rune Christensen and a who's who of the crypto world.

Last year's focus on DeFi and venture has given way to a focus on real world use cases, from Web3 gaming, Decentralised social media, tokenisation, data, digital ownership and stablecoins.

Regulation remained a central theme with the Securities and Exchange Commission (**SEC**) led crackdown on the United States crypto industry contrasted with more positive developments in Asia and elsewhere. In particular there was renewed energy from jurisdictions like Hong Kong, Singapore, Dubai and the United Kingdom as Governments and regulators adopt a more tech and innovation friendly approach.

Web3 Values

Putting financial speculation aside, a number of speakers refocused on the core values of Web3, what Balaji, the ex-Coinbase CTO and author of The Network State termed "internet values", such as transparency, democratisation, technology, freedom and entrepreneurship. Riffing on this theme, Cameron Winklevoss noted that crypto embodies many American values, although America seems to have taken something of a detour.

Business Fundamentals

There was a renewed focus on business fundamentals. Paul Veradittakit of Pantera Capital noted that we're:

> *Not investing into crypto, we're investing into companies, blockchain is the technology layer*

Infrastructure

There was much discussion on infrastructure and easier user experience. Robbie Ferguson from Immutable emphasised the importance of easy Web3 onboarding, noting Immutable's recent launch of its Passport wallet solution for gamers. Robbie was joined by James Tromans of Google Cloud who emphasised Google's focus on building infrastructure and great user experience in Web3. Arthur Hayes of Maelstrom and Bitmex trumpeted AI's need for decentralised storage and his bullishness on data focused decentralised storage protocols.

DeFi

The DeFi mood generally felt pretty somber, perhaps in light of recent US enforcement actions. Capturing the DeFi and macro zeitgeist, Paul Veradittakit noted tokenising the dollar (ie stablecoins) is the biggest thing happening in DeFi right now. In true Peter Thiel contrarian style, Joey Krug of Founders Fund opined that there is a lot more open things to build in DeFi.

Regulation

On the subject of regulation, speakers called on the wisdom of the great philosophers and theorists, channeling a sense of Zen. Richard Galvin of DACM cited the vaunted crypto manifesto, the Sovereign Individual, which noted that old laws seldom resist new technology, and expressing his view that technological change is likely to outpace and bend regulation in its image. Tyler Winkevoss evoked Ghandi's famous aphorism:

> *First they ignore you, then they laugh at you, then they fight you, then you win.*

We're in the fight phase he added.

On the question of US regulation, Brad Garlinghouse lamented the reported US$100m that Ripple has spent fighting the SEC in its battle to establish that the XRP token is not a security. His comment that his only regret being that he did not redomicile the company outside the United States from the beginning is a message that all regulators should consider given how mobile the blockchain industry is.

Cameron Winklevoss lamented the waste of public resources in regulators fighting the industry, a battle they are losing in some cases, rather than setting clear rules of the road for crypto which could embrace innovation.

Internationalisation

MC Lader of Uniswap Labs observedthat the developer of the eponymous Uniswap decentralised exchange is looking to internationalise its products, adopting new platforms and languages, while maintaining its United States presence. Coinbase is doing the same by pursuing its new International business, focused on derivatives, while maintaining its compliance focus and fighting SEC enforcement actions.

NFTs and Gaming

On the topic of NFTs and gaming, Yat Siu, Hong Kong's leading crypto identity, noted that his Web3 thesis remains consistent, the promise of digital ownership for gamers. Zedd Yin of Magic Eden cited the company's support for building consensus on creator royalties to help support the change for creators that Web3 represents. Alex Pack from Hack VC noted that Decentralised Social Media (DeSoc) continues to offer the promise of a whole new monetisation layer for the economy that fosters creativity and moves away from the winner take all Web2 model.

Market Structure

Diogo Monica of Anchorage Digital commented on shifts in market structure post the collapses of 2022, with many crypto market participants learning the lessons of past collapses and moving to a more disaggregated business model, noting the term "bankruptcy remoteness" had entered the lexicon among key concerns for crypto counterparties. Ouriel Ohayon of non-custodial wallet provider ZenGo, nevertheless noted that while it's important for the crypto space to mature, which will require some changes to risk and market structure, blockchain must retain its open, transparent, permissionless and global ethos to build a new paradigm. Amy Zhang of Fireblocks added "You can't fix people; you need technology and governance controls".

While for some it may seem like crypto is at something of a cross- roads after 2022, the mood at TOKEN2049 2023 underlined the core focus on building technology that empowers people and makes life better. With so many in attendance, the bear market spirits remain high. As MinTeo of Ethereal Ventures noted:

> *As we've seen in past cycles, crypto always finds a way.*

Or in the words of Sun Tzu;

> *He will win whose army is animated by the same spirit throughout the ranks. ("□□□□□□")*

MiCA – stablecoins requirements on the horizon

The EU's Markets in Crypto-assets Regulation (**MiCA** or **MiCAR**), one of the first comprehensive regulatory framework for crypto-assets, was adopted by the bloc on 20 April 2023 and is expected to apply in Q4 2024 across the EU.

Among the rules in MiCA, the provisions for stablecoins will start applying from 30 June 2024, six month ahead of other rules on licensing for crypto wallet providers and exchanges. Last month, European Banking Authority (**EBA**) published a statement saying that stablecoin issuers should start making preparation to comply with the requirements.

Below, we briefly introduce the requirements on stablecoin issuers. We have previously written about MiCA on MiCA covering its application to NFTs, public token offerings and crypto asset service providers (**CASPs**).

MiCA sets governance and reserve requirements for two types of stablecoins:

1. crypto-assets purports to maintain a stable value by referencing the value of one official currency (**Electronic Money Tokens** or **EMT**), and
2. crypto-assets purports to maintain a stable value by referencing another value or right or a combination thereof, including one or more official currencies (**Asset-referenced Tokens** or **ART**).

Likely prompted by the infamous collapses of Terra (UST) – an "algorithmic stablecoin" and the collapse of cryptocurrency exchange FTX, EBA said it published the recent statement to:

encourage timely preparatory actions to MiCAR application, with the objectives to reduce the risks of potentially disruptive and sharp business model adjustments at a later stage, to foster supervisory convergence, and to facilitate the protection of consumers.

The EBA also warned that issuers of EMT and ART should start adhering to MiCA's "high standards" of disclosure to potential users sooner rather than later. Such standard is higher compared to the general disclosure requirements (e.g. issuing a whitepaper) on non-ART and non-EMT issuers. ART and EMT issuers also face other strict requirements in addition to disclosure.

Requirements on issuers of ART

Issuers of ART in the EU need to:

- meet certain capital requirements;
- obtain permission from a competent authority;
- not only publish a whitepaper, but also get it approved by the competent authority;
- notify holders adequately, such as publishing and updating the exact number of ART in circulation and the value and composition of the reserve assets on its website at least monthly;
- comply with requirements relating to the maintenance and custody of reserve assets, such as separating reserve assets from the issuers' assets and securing prompt access to such reserve assets.

Under MiCA, a permission to issue ART is valid for the entire EU. However, supervision remains with the competent authority of the EU member state in which the issuer is domiciled.

Requirements on issuers of EMT

Issuers of EMT in the EU also face enhanced requirements. First of all, EMT may only be issued by credit institutions and e-money institutions. In addition:

- a white paper must be published and presented to the competent authority, as with ART issuers;
- issuers of EMT must ensure an immediate repayment of funds at the demand of holders at par value, and a clear statement on conditions of redemption;
- Issuers of EMT are prohibited from paying interest on the tokens.

Issuers of ART and EMT (as well as CASPs), when providing crypto-asset services should not grant interest to users of ART or EMT for the time such holders are holding those tokens.

Significant ART/EMT

If an ART or EMT is determine by the EBA to be significant, more stringent requirements apply. EBA will then perform supervision on the tokens.

Additionally, the EBA is mandated to develop 17 technical standards and guidelines under MiCA to further specify the requirements for ARTs and EMTs, and an additional 3 mandates jointly with European Securities and Markets Authority (**ESMA**), EBA's counterpart for securities markets. Publication of technical standards is expected in Q2 2024.

The news comes on the same day that ESMA issued its first batch of proposed MiCA rules detailing how CASPs seeking a license to operate across the bloc will obtain authorisations – the proposals are set out in a 160-page and include how crypto firms should handle user complaints and manage conflicts of interest.

While there is still some time before MiCA comes to full effect and more technical guidelines are in train, MiCA already represents a game-changer for token issuers and CASPs, as the regime offers the promise of a regulated, relatively light touch, pathway to issuing tokens and performing crypto-asset related services. We anticipate that lawmakers around the world will be reviewing MiCA with interest as they craft their own regulatory regimes.

By Michael Bacina, Steven Pettigrove and Jake Huang

Guidance or grievance? Breaking down the crypto comments from Gensler's SEC testimony

SEC Chairman Gary Gensler's recent testimony before US congress provides clearer insight into the views of the controversial chairman. Gensler spoke as a witness before US Senators Sherrod Brown and Tim Scott and other members of the United States Senate Committee on Banking, Housing, and Urban Affairs overseeing the activities of the SEC.

Chair Gensler spoke at length on a number of different focus areas for the SEC, including the proposed use of Artificial

Intelligence as potential data analytic and tracking tools for use across the economy.

Critical for the blockchain space were Chair Gensler's comments about crypto-asset regulation:

> *There is nothing about the crypto asset securities markets that suggests that investors and issuers are less deserving of the protections of our securities laws [...] given that most crypto tokens are subject to the securities laws, it follows that most crypto intermediaries have to comply with securities laws as well.*

Chair Gensler's speech speech Washington DC in September last year saw sweeping statements made that the Chair considers:

> *Without prejudging any one token, most crypto tokens are investment contracts under the Howey Test.*

The inference Gensler makes in his most recent testimony is clear: the SEC continues to position itself as "the cop on the beat watching out" while furiously avoiding any engagement with the rulemaking which Coinbase has been seeking. Focusing on enforcement priorities without providing meaningful rule-making to enable a pathway to compliance remains the chief criticism of the SEC's approach, with Chair Gensler saying:

> *Given this industry's wide-ranging noncompliance with the securities laws, it's not surprising that we've seen many problems in these markets. We've seen this story before. It's reminiscent of what we had in the 1920s before the federal securities laws were put in place.*

Gensler stops short of delving into some of the specific ongoing litigation the SEC is involved with and he naturally did not connect the making of rules in response to the issues of the 1920 as a solution to rules not being fit for purpose. Proposals in place to update the US custody rules for investment advisors to cover all crypto-assets have been heavily criticised by major financial businesses as being unworkable.

Chair Gensler's views on crypto-assets don't seem likely to change and the absence of clear rules and a path to compliance in the US appears likely to keep headwinds against innovation in crypto-assets in that country.

By Michael Bacina and Tim Masters

Don't get high on your NFT supply? Stoner Cats called securities by SEC

The SEC has taken action against Stoner Cats 2 LLC, alleging that the company conducting an unregistered offering of crypto-asset securities disguised as NFTs. The offering, which purportedly aimed to finance the creation of an animated web series known as "Stoner Cats" (currently rated lukewarm 4.7/10 on IMDb), managed to roll up a cool USD$8 million from collectors (or "investors" as the SEC likes to call them) in an offering that was allegedly a total buzzkill in terms of meeting the necessary exemption criteria for registration under US law.

According to the SEC's order, on 27 July 2021, Stoner Cats initiated the sale of more than 10,000 NFTs, each priced at around USD$800 and the initial supply sold out in 35 minutes. The SEC alleges that both prior to and following the sale of the Stoner Cats NFTs to the public, the company was sky high, extensively marketing the financial benefits of ownership of the Stoner Cat NFTs, emphasising the potential for resale on the secondary market.

The SEC order also alleges that the marketing campaign prominently featured the company's Hollywood expertise, familiarity with cryptocurrency projects, and the involvement of well-known actors in the web series. A quick google search of "Stoner Cats" will reveal various articles linking famous actors Mila Kunis and Ashton Kutcher to the project.

The SEC further alleges that the company had lit up the Stoner Cats NFTs to grant the company a 2.5% royalty on each secondary sale, with the company actively encouraging individuals to toke transactions of the Cats and leading to a dank USD$20 million or so in fees across at least 10,000 transactions. Gurbir S. Grewal, Director of the SEC's Division of Enforcement, emphasised the SEC's 'substance over form' approach:

> *Regardless of whether your offering involves beavers, chinchillas, or stonerific NFTs, under the federal securities laws, it's the economic reality of the offering – not the labels you put on it or the underlying*

objects – that guides the determination of what's an investment contract and therefore a security

Without admitting or denying the SEC's findings, the company has consented to a cease-and-desist order and agreed to pay a doobie of a civil penalty of USD$1 million. Additionally, the SEC order required the establishment of a 'Fair Fund' to reimburse collectors who say they were burned by holding the NFT too long while the price burned down. The order states that the company has also agreed to green out and destroy all NFTs in its possession and control.

Twitter users was also quick to comment on the SEC order, memeing the project and Mila Kunis and Ashton Kutcher alike, and creating a memorable #Cats #Compliance hashtag combo.

In an interesting twist, secondary sales of Stoner Cats on platforms such as OpenSea have surged since the SEC's action against the company. No word on whether the royalties will be making their way on those sales back to the company.

This enforcement action by the SEC serves as a dank reminder of the regulatory haze surrounding crypto-asset offerings, particular those that blur the line between collectibles and securities. In an industry marked by rapid innovation and continuously evolving legal standards, it is easy for participants to get lost in the smoke. Despite the similarity between NFTs and other collectibles, and the absence of any enforcement against baseball card sellers, it seems the collectibles NFT world is not as safe a place as many had previously thought.

By Michael Bacina and Luke Higgins

IOSCO Consultation on 2023 DeFi Report

On 7 September 2023, the International Organization of Securities Commissions (**IOSCO**) released a Consultation Report, introducing 9 policy recommendations for decentralised finance (**DeFi**) (**Report**). The Report seeks consultation on, and builds further on, the IOSCO DeFi report of 2022, and proposes updated recommendations based on discussions with "academics, data analytics firms, researchers, and technologists" noting distributed ledger technology based applications have significantly expanded since the 2022 report.

The Report acknowledges:

> *DeFi is an important, evolving, and expanding technological innovation. The use of DLT may have the potential to foster financial innovation, increase efficiencies, and improve access to financial products, services, and activities.*

However, the word "risk" is mentioned 20 times for each mention of "benefit" in the Report. IOSCO Board Chair, Jean-Paul Servais confirmed that the new recommendations complement the Crypto and Digital Assets Recommendations (**CDA**) released earlier this year by IOSCO:

> *Once finalised, the two sets of Recommendations will provide a first clear, interoperable, and globally consistent policy framework for crypto and digital assets, including DeFi.*

The paper defines DeFi as:

Financial products, services, arrangements, and activities that use distributed ledger or blockchain technologies (**DLT**), including self-executing code referred to as *smart contracts.*

In discussing DAOs, the Report links DAOs to people, not self-executing code, asserting that:

> *DAO's are, at their essence, organizations of humans*

and that:

> *In theory, a DAO's governance rules could be encoded in smart-contracts on the blockchain on which it depends and all on-chain activity associated with a DAO could be immutably recorded on the blockchain, providing transparency to observers. In practice, however, DAOs rely critically on input from human actors for their operation, including through activities that occur off-chain.*

Recommendations

The 9 policy recommendations follow a 'lifecycle' approach and are 'principles-based' and 'outcomes-focused' and include:

1. Regulators are encouraged to analyse DeFi at a functional, technical and economic reality, enterprise level for a holistic understanding.
2. Identifying responsible persons – Regulators should look beyond decentralisation and identify natural persons and entities involved in the DeFi arrangement that could be subject to applicable regulatory framework including for example, founders and developers, issuers and holders of governance tokens and custodians.
3. Achieving common standards of regulatory outcomes – Regulators should avoid regulatory arbitrage between traditional financial markets and DeFi markets.
4. Requiring identification and addressing conflicts of interest – especially for Responsible Persons.
5. Requiring identification and addressing of material risks, including operational and technology risks.
6. Requiring clear, accurate and comprehensive disclosures – transparency is necessary for investor protection and market integrity.
7. Enforcing applicable laws – this will include obtaining appropriate crypto-asset and blockchain data, tools and expertise to conduct investigatory and enforcement activities.
8. Promoting cross-border cooperation and information sharing.
9. Understanding and assessing interconnections among the DeFi market, the broader crypto-asset market, and traditional financial markets.

The Report seeks to 'harmonise' the way crypto-asset markets and securities markets are regulated, following the oft-repeated principle 'same activity, same risk, same regulatory outcome'.

The approach, particularly when coupled with Recommendation 2 seeking to find responsible persons, may be met with submissions noting the operation of self-executing code does not usually involve responsible persons and given the recent decision in the Uniswap case, there's a risk that Courts might recognise the reality of smart contracts in a way which is not

consistent with IOSCOs recommendation.

In addition to the recommendations, the Report contains a list of recent crypto-failures, including the Terra USD/Luna Collapse, the FTX Insolvency and USDC Depeg. These centralised business failures but are said to have "reportedly" impacted DeFi, with reference to liquidity pools and price action, with the Report noting:

> *These events also illustrate how investors may tend to migrate assets from a centralized platform to DeFi when they lose confidence in the centralized platform,*

The Report also summarises theft of assets which has occurred from DeFi protocols, highlighting the risk of smart contract failure which is unique to DeFi. It also includes several graphs from the 2023 Crime Report from Chainalysis but omits data on the total illicit usage (which sits around 0.15% of volume across all crypto-assets), risking that a casual reader will be left with the impression that DeFi is a growing and risky dangerous area of loss.

IOSCO represents a range of financial regulators around the world and the Report says it represents a 'significant step forward in achieving regulatory outcomes for investor protection and market integrity'.

In light of the coverage of 130 jurisdictions and regulation of over 95% of the world's securities markets by IOSCO members, once finalised, these recommendations will be likely to lead the approach by regulators concerning digital assets around the world.

IOSCO is receiving public comments on the paper until 19 October 2023 via email DeFiconsultation@iosco.org. and given the nature of the recommendations, it is important that all those involved in DeFi projects ensure that their voices are heard, so that recommendations can capture the benefits of DeFi while addressing risks in a way that accommodates the risk that DeFi actually poses.

By Steven Pettigrove and Kelly Kim

Vitalik's Privacy Pools: Where Personal Transaction Data Can Dive Deep!

In a paper published 6 September 2023, the Ethereum co-founder Vitalik Buterin, along with four industry leaders and academics, introduced a new smart contract-based protocol named 'Privacy Pools'. Proposed as an alternative to the sanctioned cryptocurrency mixer Tornado Cash, Privacy Pools leverage advanced cryptographic techniques, including zero-knowledge proofs, to verify the legitimacy of funds, without needing to expose the whole transaction history for a user. Through the new Privacy Pool protocol for Ethereum, users are able to 'generate a brand new Ethereum address that is completely unlinkable to any prior transaction history'. The Protocol is described as:

> *A first step towards a future where people could prove regulatory compliance without having to reveal their entire transaction history.*

The paper acknowledges the inherent privacy concerns arising from the easily accessible and transparent nature of transactions on the public blockchain, which share significant metadata in a permanent and very public way. Privacy-enhancing protocols have previously sought to address this by breaking the link between a 'particular deposit and its withdrawal counterpart' but the way that has occurred has created opportunities for bad actors to also use those tools. The paper identified the 'critical issue with Tornado Cash' as:

> *Legitimate users had limited options to dissociate from the criminal activity the protocol attracted.*

In contrast, Privacy Pools offer 'membership proofs' and 'exclusion proofs' functions, which allow users to confirm whether or not their withdrawals come from the pool of 'good' deposits. This is said to be designed with an aim of enabling users to fulfil their 'desire for privacy' as well as their 'desire to avoid suspicion'. By pooling honest transactions together, users are able to confirm the legitimacy of their transactions by proving that their transactions came from the 'good' deposits. As good actors are incentivised to distinguish themselves from the 'bad' deposits, bad actors will face difficulties with proving their membership in a "good"-only association set.

This approach is aimed at maintaining separation between the pools. However, the paper recognises that in reality, due to

societal perspective and jurisdictional differences, there may be cases where there is 'no global consensus' on which funds are 'good' or 'bad'. In such cases, users are able to exclude withdrawals that are non-compliant with their jurisdiction or issue a membership proof against the 'intersection' of both association sets to demonstrate compliance with numerous jurisdictions. The protocol is 'very flexible' in this way and 'censorship resistant'.

Privacy Pools come at an important time where ongoing data breaches highlight the need to ensure greater baked-in privacy for users and less exposure of personal information, but with governments historically used to using the collection of personal information as a means of tracking down bad actors and prosecuting law breakers.

The paper makes a bold prediction about Privacy Pools:

> *In many cases, privacy and regulatory compliance are perceived as incompatible…this does not necessarily have to be the case.*

To realise this vision of a 'potential future' where 'financial privacy and regulation can co-exist', the paper requests for cooperation from 'practitioners, academics…policymakers and regulators', and if this vision can be brought to reality, perhaps users can truly have the benefits of strong privacy protection without the stigma of bad actors also using those same tools.

By Michael Bacina and Kelly Kim

US CFTC targets DeFi platforms: Commissioner dissents noting impossibility of compliance

The Commodity Futures Trading Commission (**CFTC**) has issued orders against three decentralised finance (**DeFi**) companies for alleged violations of the Commodity Exchange Act (**CEA**) and CFTC regulations. The companies in question are Opyn, Inc., ZeroEx, Inc., and Deridex, Inc., all registered in Delaware but operating out of California and North Carolina.

The CFTC's enforcement action focuses on several key areas:

- **Failure to Register:** Both Deridex and Opyn are charged with failing to register as a swap execution facility (**SEF**) or designated contract market (**DCM**), as well as failing to register as a futures commission merchant (**FCM**).
- **Bank Secrecy Act Violations:** All three companies are accused of failing to adopt a customer identification program as part of a Bank Secrecy Act compliance program, a requirement for FCMs.
- **Illegal Offerings:** ZeroEx, Opyn, and Deridex are charged with illegally offering leveraged and margined retail commodity transactions in digital assets.

The companies have been ordered to pay civil monetary penalties ranging from $100,000 to $250,000 and to cease and desist from further violations.

In a press release, CFTC Director of Enforcement Ian McGinley took a swipe at DeFi operators for failing to comply with laws that were drafted before DeFi existed and are virtually impossible for DeFi companies to comply with:

> *Somewhere along the way, DeFi operators got the idea that unlawful transactions became lawful when facilitated by smart contracts…they do not.*

Interestingly, CFTC Commissioner, Summer Mersinger has dissented against the enforcement actions against Opyn, Deridex and ZeroEx. In a statement of the same date as the press release, Ms Mersinger noted that the handling of these three cases through enforcement:

obscures that one of the cases before us is not like the others

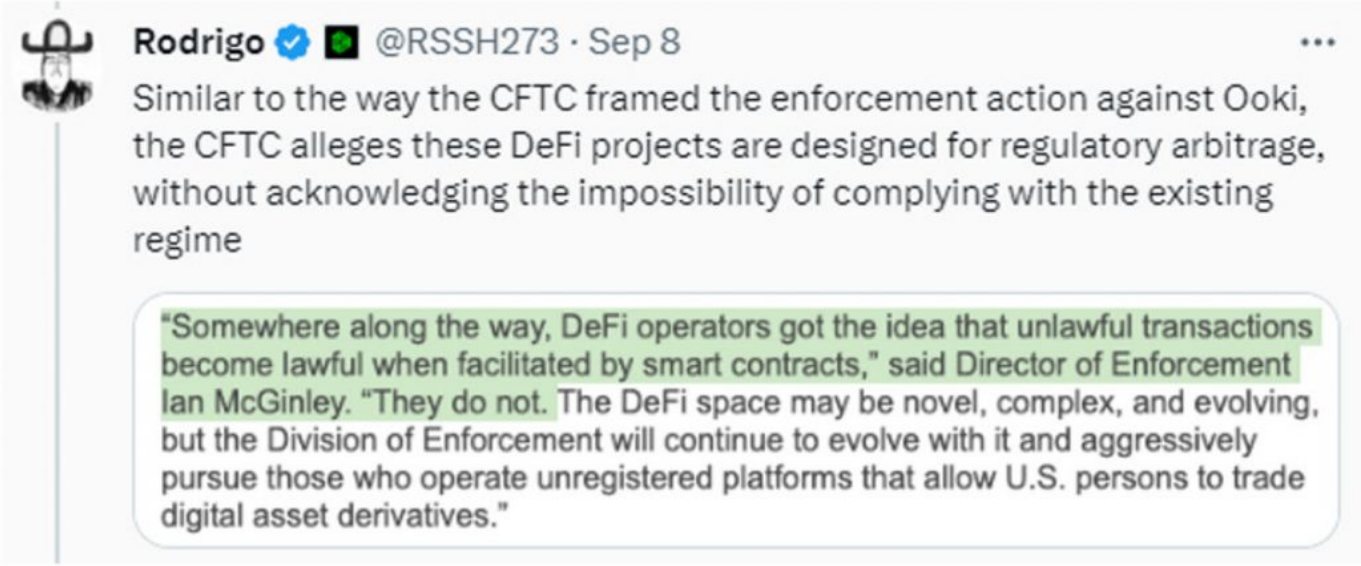
With respect to the ZeroEx charge, Ms Mersinger rightly outlines that ZeroEx's offering enabled users to execute spot trades in different digital asset pairs and that the CFTC does not have regulatory jurisdiction over spot trading, which is lawful under the CEA.

The CFTC nonetheless proceeded with this charge because the ZeroEx protocol, Matcha, was used to trade leveraged digital assets issued by unaffiliated third parties through smart contract technology developed by other unaffiliated third parties and automatically executed on other DeFi lending platforms.

Ms Mersinger plainly and bleakly points out the reality of the continued enforcement by the CFTC:

> *Enforcement is inherently ill-suited to balancing our competing mandates of protecting customers and promoting responsible innovation. By contrast, that is the essence of agency rulemaking.*
>
> *Customers, market participants, stakeholders, and the Commission itself benefit from clear, transparent, and comprehensible rules adopted with public engagement through a notice-and-comment rulemaking process. Yet, today's actions do not promote responsible innovation – they shut it down, banishing innovation from U.S. shores.*

The general incoherence of the charges were neatly summarised by X user 'Rodrigo' in a thread, which noted that Opyn was charged despite taking steps to excluding United States customers and that the CFTC's reasoning is inconsistent with the recent opinion dismissing the Uniswap class action where Uniswap was not found liable for the actions of third parties using their technology for activities which Uniswap did not control.



US Crypto litigator Jason Gottlieb said:

In Australia, the similar risk of companies leaving the country in search of digital asset regulatory clarity exists, but for different reasons. The industry has been patiently waiting for centralised exchange custody and licensing consultation from Treasury while a private member's bill seeking to licence exchanges being rejected by a Senate Committee any many other jurisdictions are moving ahead with licensing and clarity for projects.

There is a clear opportunity for DeFi guidance to be issued by regulators in Australia, informed by the substantial learnings from overseas actions. Unfortunately, current consultation from IOSCO is treating DeFi as if it was not decentralised, with recommendations proposed that responsible persons be sought and held responsible for DeFi protocols.

This enforcement action also is worthy of note as the most recent move in the tug-o-war for digital asset regulatory jurisdiction between the CFTC and the Securities and Exchanges Commission and marks a continuation of regulation by enforcement that has targeted innovative Web3 companies who as a result are travelling to greener pastures.

By Michael Bacina, Steven Pettigrove and Luke Misthos

Pass or Fail? Avoiding being rekt with the Rekt Test: building safety via security

At the Gathering of Minds conference earlier this year, a group of blockchain industry leaders led by Trail of Bits CEO Dan Guido met to discuss and workshop a simple test for profiling the security of blockchain projects with a view to help address and reduce security failures and build trust in the ecosystem. Although the number of hacks decreased in 2022, the amount stolen cost users approximately $3.8 billion. The result was the Rekt Test.

As a blockchain version of the the Joel Test (a famous and very simple checklist created in 2000 by Joel Spolsky to determine the maturity and quality of a software team) the Rekt Test is designed to assist Web3 projects to objectively assess their security posture and measuring their risk profile against bad actors.

The test focuses on simple and universally applicable security controls to inform Web3 projects that otherwise may lack guidance and structure to their security operations.

The 12 questions comprising the Rekt Test are as follows:

1. *Do you have all actors, roles, and privileges documented?*
2. *Do you keep documentation of all the external services, contracts, and oracles you rely on?*
3. *Do you have a written and tested incident response plan?*
4. *Do you document the best ways to attack your system?*
5. *Do you perform identity verification and background checks on all employees?*
6. *Do you have a team member with security defined in their role?*
7. *Do you require hardware security keys for production systems?*
8. *Does your key management system require multiple humans and physical steps?*
9. *Do you define key invariants for your system and test them on every commit?*
10. *Do you use the best automated tools to discover security issues in your code?*
11. *Do you undergo external audits and maintain a vulnerability disclosure or bug bounty program?*
12. *Have you considered and mitigated avenues for abusing users of your system?*

Projects will need to consider these questions in depth and reflect on their current operations. Each question is a starting point to unpack into a range of more detailed questions applicable to a project and conducting a risk analysis. The list is of course not designed to be definitive, but a way to start informed discussions about important security controls.

Hacks, scams, social engineering, lack of documentation, and the absence of security roles are common points of risk in the blockchain ecosystem and industry participants need to go beyond just improving smart contract code or enlisting white hats to test systems as the industry matures.

Having a clear response to the Rekt test could be a great framework for blockchain projects and businesses, and even developers, to help ensure that aren't the victim of accidental loss or a cyber attack.

By Michael Bacina and Luke Misthos