Article Information

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

Blockchain Bites: Crypto in limbo as ASIC calls for licensing obligations on tokens?, Policing the digital economy: Australia proposes sweeping scam prevention obligations, Coinbase takes rulemaking petition to Appeals Court, Alameda CEO sentenced over FTX fraud

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

Crypto in limbo as ASIC calls for licensing obligations on tokens?

The Australian Securities and Investments Commission (ASIC) is set to deliver a strong message to the cryptocurrency industry: prepare to be licensed under the Corporations Act. What's less clear is how ASIC says the Corporations Act will apply and how far that regulation will extend. ASIC Commissioner Alan Kirkland will address the Australian Financial Review Crypto and Digital Assets Summit today and is expected to signal that many crypto assets are considered by ASIC to be financial products under existing law.

What isn't expected to be addressed is how specific crypto-assets can comply with current financial services laws.

The move, part of a broader regulatory shift, will require cryptocurrency exchanges (currently registered with and regulated by AUSTRAC) to also hold Australian Financial Services Licences. Licensing has been sought by industry bodies and the industry for years, but in a manner tailored to give consumers the benefit of protections which well regarded crypto exchanges in Australia have provided, but without labelling all crypto assets as financial products.

Australia was a leader in implementing AML/CTF requirements for digital asset exchanges in 2018 but later years saw progress on tailored regulation pivot to repeated government consultations coupled with regulation by enforcement.

Imposing licensing requirements on a significant number of crypto-asset exchanges on the basis that widely traded crypto assets are financial products, while simultaneously abstaining from providing clear guidance on how these tokens are financial products and how they can comply with licensing and disclosure obligations causes confusion and uncertainty, and risks doubling up of licensing obligations on exchanges as they must seek both a digital asset exchange licence for non-financial product tokens plus licensure for tokens which are financial products.

Many of those exchanges have taken significant steps to ensure regulatory compliance by obtaining and maintaining strong protection of client assets, KYC and AML/CTF policies, and receiving legal advice regarding their products.

While ASIC is expected to update its main regulatory guidance note for crypto-assets (INFO225) later this year, its latest comments leave critical questions unanswered, absent ASIC committing to providing a pathway to compliance, including:

- which tokens are financial products?
- what kind of financial products are they?
- and what kind of disclosure of licensing will those products need?
- can those products possibly meet that disclosure and licensing requirements?

There are tokens which nearly all lawyers in the industry agree are likely financial products, which are already caught in the existing financial service regime, but there are a great many which do not meet the traditional definitions of a financial product, and provide utility to users beyond any kind of speculation or investment.

Shoehorning these innovations into a licensing regime that was created over a decade before the first bitcoin was mined will have serious and ongoing ramifications for the industry. The reality of such a regime is that the overwhelming majority of tokens will not meet the heavy compliance burden that Australian financial products face, which will likely stifle innovation and encourage Australians to access offshore and decentralised platforms (in conflict with ASIC's focus on consumer protection). Token projects will continue moving offshore to jurisdictions that provide certainty and scams may proliferate more broadly, as licensed exchanges delist tokens which cannot meet licensing requirements and consumers go looking for them.

Globally, crypto firms face similar challenges, with the US Securities and Exchange Commission (**SEC**) taking action against major platforms like Coinbase for offering what they assert are unregistered securities under US law. Similar to the proposed approach for Australia, no pathway to compliance has been proposed by the SEC for token issuances.

At the same event Fred Schebesta, founder of Finder, which found itself on the wrong end of regulation by enforcement said:

> It would be a really good idea to try and update the law, as opposed to suing organisations and crushing the Australian economy and killing our innovation.

The USA and SEC has been seen as hostile to crypto and ASIC's position on crypto as financial products risks Australia also being seen as an unfriendly jurisdiction. Meanwhile, jurisdictions seeking to lead in crypto, including the United Kingdom, the European Union, Singapore, and Dubai, are grappling more directly with the global nature of crypto-assets and are seeking to attract new businesses to be based within their borders.

Amy-Rose, CEO of the Digital Economy Council of Australia, said:

> Our start-ups are innovating in stealth mode behind closed doors so that they're not targeted… Then once they build product, they plan to go to Singapore or Dubai or even the US, depending on the election outcome

Samira Tollo, CTO and Cofounder of exchange elbaite said:

> Australia is stuck in an echo chamber. For years, we've been calling for clear regulation to define digital assets, trying to fit them into existing frameworks.

In choosing a path similar to the SEC journey, ASIC will still have to grapple with the key questions on how decentralised tokens can comply with laws made for centralised issuers, plus a potential about face at the SEC if Trump wins the presidency and keeps his promises, and traditional financial product issuers will likely object to any lighter touch regime while they themselves face ongoing burdensome compliance obligations for products.

One upside of this approach is that it may drive a harder examination of existing disclosure and licensing, and real world asset tokenisation may become even more attractive to exchanges who will push their superior automation and systems into greater competition with traditional financial services businesses.

By Steven Pettigrove, Michael Bacina and Luke Misthos

Policing the digital economy: Australia proposes sweeping scam prevention obligations

Australia is stepping up its fight against scams announcing a consultation on legislation to introduce a "Scams Prevention Framework" (SPF), which aims to protect Australians, visitors, and small businesses (defined as SPF consumers) from the threat of scams in the digital economy. With the growing sophistication of scam operations targeting individuals and businesses alike, the Australian government hopes to take proactive measures to disrupt, detect, and prevent scams by imposing new obligations on digital platform and infrastructure providers in key sectors with tough penalties for non compliance.

The SPF is intended as a holistic and agile response to evolving scam threats focusing on industries that the Australian Treasury has identified as key in addressing scam risks. As formulated, the SPF would impose a significant compliance burden on designated sectors to identify and disrupt scams. It represents the latest example of Governments imposing increasing obligations on digital platforms as gatekeepers in policing the digital economy.

Key features of the Scams Prevention Framework (SPF)

The SPF introduces broad protections aimed at safeguarding Australians and businesses by requiring regulated entities to take certain actions against scams. Initially, three service sectors will be designated under the framework and will need to meet several key obligations under the SPF:

- banks;
- telecommunications providers; and
- digital platform services (including social media platforms, paid search engine advertising, and direct messaging services).

Scam Definition and the Nature of Scam Activities

An essential aspects of the SPF is its expansive definition of "scam." Under the framework, the definition intends to capture:

> conduct involving an attempt, successful or otherwise, to deceive the consumer into performing an action that results in a loss or harm to the SPF consumer

This broad definition is intended to captures a wide array of scam activities, ensuring that scam attempts are addressed at all stages of their lifecycle. However, there is also concern that its breadth will extend to a wide variety of market behaviour already regulated under Australian consumer laws and impose a significant burden on regulated platforms to identify conduct that may be labelled deceptive or cause "harm".

Interestingly, the SPF distinguishes scams from other forms of fraud, such as cybercrime or unauthorised hacking, which do not involve consumer deception but may still lead to unauthorized payments. This distinction focuses the framework on the particular tactics used by scammers to trick victims into compliance.

It is specifically contemplated that the regime will cover scams involving cryptocurrency, loyalty and rewards points.

Obligations for regulated entities

The SPF imposes a number of principle-based obligations on regulated entities to protect consumers at various stages of scam activity. These principles include:

1. **Prevent**: regulated entities must take steps to prevent scams from reaching or affecting SPF consumers. This includes implementing robust systems to block scammers from accessing platforms and services and educating staff and consumers on identifying scams.
2. **Detect**: entities must monitor for potential scams and identify affected consumers. This applies not just to scams in progress but also to previous scams, even if a loss hasn't yet occurred. For example, banks are tasked with developing processes to flag suspicious activity, such as large cash transactions with new payees, or payments into a crypto-asset.
3. **Disrupt**: entities must take reasonable steps to disrupt suspected scams in progress. This could involve adding friction or validations to prevent the scam from succeeding. The framework includes a 28-day safe-harbour period, allowing entities to take proportionate actions while further investigating scam activities.
4. **Report**: entities are required to report actionable scam intelligence to the Australian Competition and Consumer Commission (ACCC) and, if requested, share scam reports with the ACCC or other regulators. This obligation is likely to sit alongside existing obligations for reporting entities to report suspicious activity to AUSTRAC, the anti-money laundering regulator.
5. **Respond**: entities must provide accessible mechanisms for consumers to report scams and establish internal dispute resolution (IDR) processes. Additionally, all entities covered by the framework must be part of an external dispute resolution (EDR) scheme, such as the Australian Financial Complaints Authority (AFCA), ensuring consumers have independent avenues for redress if they feel their complaints are not adequately addressed.
6. **Governance**: entities must also implement governance policies and procedures to manage scam risks effectively.

Sector-specific codes and regulatory oversight

To address the unique challenges different sectors face, the SPF will introduce sector-specific codes that provide tailored obligations. These codes will be flexible in an attempt to allow adaptation as scam tactics evolve, and will include minimum standards to address sector-specific harms.

The multi-regulator model of the SPF means that the ACCC will oversee obligations in the primary law of the framework and the digital platform services sector, while the Australian Securities and Investments Commission (ASIC) and the Australian Communications and Media Authority (ACMA) will enforce codes for the banking and telecommunications sectors, respectively. This coordinated approach aims to maximise regulatory expertise and ensure a comprehensive, ecosystem-wide response to scam activity. However, it is important that the SPF functions in a way that does not cause unnecessary inefficiencies within the system – for example – in circumstances where administrative processes with one regulator lead to roadblocks in complying with the requirements of another.

The proposal includes tough new penalties for corporates and individuals who fail to implement the principles based obligations to prevent and disrupt scams and applicable industry codes comparable to breaches of civil penalty provisions under other laws.

Future expansion of the SPF

While the initial focus is on banks, telecommunications, and digital platforms, the SPF is designed to evolve over time, with additional sectors expected to be designated in the future. These may include superannuation funds, digital currency exchanges, and online marketplaces.

Conclusion

The SPF is another step in Australia's increasing efforts fight against scams. The proposal would cast significant responsibility for that fight on platforms in the designated sectors imposing tough new obligations to identify and disrupt scam activity.

The consultation period is open until 4 October. The Treasury is specifically seeking feedback on the compliance burden which would be imposed on industry, and interested parties are encouraged to contribute to the consultation.

As the Government has made fighting scams a key policy priority, it is likely that the SPF will be imposed in some form. Entities that operate within the designated sectors should consider the framework's obligations, and begin preparing to take increasing measures to combat scams in the digital economy.

Written by Luke Higgins and Steven Pettigrove

Coinbase takes rulemaking petition to Appeals Court

The ongoing battle between Coinbase and the US Securities and Exchange Commission (**SEC**) entered a new phase this week, as the exchange giant continued its push for clearer rules in the crypto-asset space. The case, which stems from Coinbase's call for the SEC to establish specific regulations for cryptoasset securities, is now before the US Court of Appeals for the Third Circuit.

Coinbase had previously petitioned the SEC to create a tailored regulatory framework for the industry. When that petition was denied, the company took legal action, claiming that the SEC's refusal to engage in rulemaking was both arbitrary and harmful to innovation.

Coinbase's legal team told the US Appeals Court on Monday that the SEC had failed to provide a pathway for businesses and industry participants to progress in the crypto-asset space. In a series of posts on X, Coinbase's Chief Legal Officer, Paul Grewal, expressed frustration, stating that the SEC "refuses to provide a reasonable explanation for its barebones denial" while simultaneously carrying out what the company describes as an aggressive and unclear enforcement strategy.

The SEC's position, however, is firm. In its arguments, the regulator made it clear that dissatisfaction with existing regulations does not give Coinbase or other crypto companies special treatment under the law. Moreover, the SEC maintains it is not obligated to create new rules specifically for the cryptocurrency industry as the existing laws are sufficient.

The central question in this legal standoff is whether crypto-tokens – like those traded on Coinbase's platform – should be classified as securities (i.e., whether they meet the so-called "Howey" test). SEC Chair Gary Gensler has repeatedly stated that the majority of cryptocurrencies fall under this category (despite recently acknowledging a misnomer in its use of the term "crypto-asset securities" for several years), and has called on exchanges like Coinbase to "come in and register" under existing securities laws. Coinbase, however, argues that the current legal framework is unworkable and that there is no way for exchanges to comply with the current law. This sentiment is shared by many businesses operating within the sector who point to example of firms who have sought registration either being denied or met with regulatory enforcement action.

This legal skirmish is not the only one between the SEC and Coinbase. In a separate case, the SEC sued Coinbase in June 2023, accusing the company of operating as an unregistered broker, exchange, and clearing agency. The regulator also claims that 13 cryptocurrencies available on Coinbase, including SOL, ADA, and MATIC, are securities. That lawsuit is currently in the discovery phase.

For the crypto-asset industry, the outcome of Coinbase's legal efforts could be significant. Coinbase and many others in the sector argue that existing regulations, which were crafted decades ago for traditional financial instruments, are ill-suited to digital assets. Without a clearer framework, they warn that innovation could be stifled, and the US may lose its competitive edge in emerging technologies.

At the heart of this debate is a critical question for regulators, lawmakers, and industry participants alike: how should crypto-assets be classified, and what rules should apply to their issuance and trade? As the case between Coinbase and the SEC moves forward, the answers to these questions will shape the future of cryptocurrency in the US – and determine whether the country embraces blockchain technology or whether developers seek more friendly emerging regulatory regime in Asia and Europe.

While there are a number of legislative proposals under debate in the United States, the legislative process has been slow and the battle over crypto regulation is increasingly playing out in the Courts.

Written by Luke Higgins and Steven Pettigrove

Alameda CEO sentenced over FTX fraud

Caroline Ellison, a top executive of Alameda Research, the FTX group's trading arm, has been sentenced to two years in

prison over her involvement in the collapse of FTX and related financial frauds.

Ellison was a co-CEO of Alameda Research and chief lieutenant to Sam Bankman-Fried (commonly known as SBF). Earlier this year, SBF received a 25-year prison sentence for stealing over USD$8 billion from customers of the exchange in order cover trading losses at Alameda and other investments.

Ellison struck a plea deal with the prosecutor by admitting to charges including wire fraud and money laundering, and testified against SBF. She was also ordered to forfeit more than USD$11 billion to the court, with the possibility of additional restitution payments.

Ellison was facing a potential maximum sentence of 110 years in prison, which is 55 times longer than the sentence she received.

Judge Kaplan described her cooperation with prosecutors as “remarkable” but emphasized that her significant culpability and remorse for the crimes should not serve as a “get out of jail free card,” according to Reuters.

In court, Ellison expressed her apologies to the victims of the scheme, as reported by US media. She said:

> On some level, my brain can’t even comprehend the scale of the harm that I caused

FTX was founded in 2019 and quickly grew to become the third-largest crypto exchange globally, valued at USD$32 billion within just two years. The success of FTX turned SBF into a billionaire and a prominent business figure. However, in 2022, rumours of financial woes led to a run on its deposits, triggering the firm’s collapse and ensuring a prolonged crypto winter. SBF and his associates immediately fell under investigation with SBF convicted by a New York jury last year on charges including wire fraud and conspiracy to commit money laundering, following a trial that detailed his misuse of customers’ funds for property purchases, investments, and political donations. SBF is now appealing the sentence.

Written by Jake Huang and Steven Pettigrove