Article Information

Authors: Steven Pettigrove, Jake Huang, Jordan Markezic, Michael Bacina
Service: Blockchain
Sector: Financial Services, FinTech, IT & Telecommunications

Blockchain Bites: Tornado Cash winds pick up, ASIC target Crypto Target Market Determinations, Cross chain crime, EU offers token regulation path

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

Tornado Cash winds pick up: Coin Center sues OFAC over privacy concerns

Coin Center – a crypto policy not-for-profit organisation – has brought proceedings against the US Treasury Department's Office of Foreign Asset Control (**OFAC**). Coin Center claims that OFAC unlawfully overreached its authority when it criminalised interactions with Tornado Cash – a privacy enabling Ethereum coin mixing facility which had been used by bad actors.

The action follows Coin Center's threat raised immediately after the ban that it would challenge the OFAC decision in Court. Coin Center's Executive Director, Jerry Brito, said on Twitter:

> *Not only are we fighting for privacy rights, but if this precedent is allowed to stand, OFAC could add entire protocols like Bitcoin or Ethereum to the sanctions list in future, thus immediately banning them without any public process whatsoever. This can't go unchallenged.*

At the time of the ban, OFAC argued that Tornado Cash had been used to launder money by bad faith actors, including North Korean-sponsored hacking organisation, Lazarus Group.

By banning Tornado Cash, the US Treasury has been accused of 'declaring war' on privacy. Coin Center made the following observations in a press release on their website:

> *Privacy is not the default on Ethereum. If you do your job on Ethereum, your co-workers can see your salary. If you donate to a political cause on Ethereum, the enemies of your cause can see your contribution. If you are a celebrity on Ethereum, your fans see not just your publicized activities but also your private personal accounts. Privacy is normal for a salaried employee, a charitable donor, even a celebrity, but privacy is not normal if you do these things on Ethereum unless you use Tornado Cash.*

Of course there are other privacy centric mixers which are not subject to sanctions, but the action by OFAC, which is an administrative decision, and not a policy or judicial decision, could extend easily to other privacy enabling software.

Coin Center's action against OFAC is similar to the lawsuit filed against OFAC by Coinbase last month, alleging OFAC's action in banning an unaffiliated piece of open-source software overstepped the law. The claim is technical but OFAC is entitled to act against persons and entities and the core argument is that a piece of software is not a person or entity.

Coin Center's action, argues that OFAC's powers are given to it by the *International Emergency Economic Powers Act* only by allow OFAC to block domestic users from:

> *transacting with a foreign person or majority foreign entity or the property of that person or entity.*

Coin Center are making the matter squarely about privacy, observing:

> *Privacy is normal, and when we win our lawsuit, using Tornado Cash will be normal again.*

If Coinbase or Coin Center prevail in their actions, the victory will be seen as a substantial win for the privacy rights of people, as well as giving more confidence to American citizens to use privacy tools.

Crypto Target Market Determinations Targeted by ASIC

On Monday, ASIC announced that it had made interim stop orders preventing Holon Investments Australia Limited (**Holon**) from offering or distributing three funds to retail investors because of allegedly non-compliant target market determinations (**TMDs**). Each fund – the Holon Bitcoin, Ethereum and Filecoin funds – offers retail investors exposure to a single crypto-asset, being BTC, ETH or FIL, respectively.

Target Market Determinations are required to be published by the providers of financial products to retail customers under the Design and Distribution Obligations set out in Pt 7.8A of the *Corporations Act 2001 (Cth)*. ASIC states that the Design and Distribution Obligations are intended to require providers to "design financial products to meet the needs of consumers and to distribute their products in a more targeted manner". Once an issuer has prepared and issued a TMD, they are required to notify ASIC if they have significant dealings inconsistent with the TMD and there may be consequences for that dealing.

ASIC argues that the Holon funds are "not suited to the wide target market defined" in the TMDs, which it says includes investors:

- with a potentially medium, high or very high risk and return profile; and
- intending to use the fund as a satellite component (up to 25%) of their investment portfolio; and
- intending to use the fund as a solution/standalone component (75-100%) of their investment portfolio.

The final point is unclear, as Holon's published TMDs relating to these funds already excluded investors who intend to use the fund as a solution/standalone component (75-100%) from the target market.

The wording of ASIC's press release infers that ASIC believes exposure to a concentrated single asset crypto fund will only be appropriate for retail investors who have a relatively high risk appetite and that the products would be suitable for retail investors in small concentrations (potentially well below 25% of total portfolio) only.

ASIC's press release states:

> *ASIC made the interim orders to protect retail investors from potentially investing in funds that may not be suitable for their financial objectives, situation or needs….Crypto-assets are highly volatile and complex, making concentrated investments in individual crypto-assets very risky and speculative. Investors are likely to experience significant price volatility and deep negative returns in periods of asset price decline.*

ASIC also acknowledges that Holon warns investors of the potential of a total loss of value in its product disclosure statement. Its TMD also emphasizes the high risk of short term losses occurring.

ASIC's interim orders are valid for 21 days unless revoked earlier. Holon will have the opportunity to make submissions to ASIC. Final orders will be made if ASIC's concerns are not addressed in a timely manner. With continued rising numbers of Australians holding crypto-assets directly, and regulated funds arguably providing a safer way for some Australians to access crypto-assets, this move could lead to a dispute which may touch on the fundamental freedoms Australian retail investors should have to invest in their choice of assets.

In the meantime, any licensed providers which offer retail products involving crypto-assets would be wise to urgently review their TMDs and other disclosure documents for compliance and seek competent legal advice from lawyers with deep crypto experience.

Cross chain crime: wild west or totally trackable?

Decentralised Exchanges (**DEXs**), Cross-chain Bridges and Coin Swap Services have been used by criminals and high risk entities to obfuscate at least USD$4 billion-worth of illicit crypto proceeds, according to a report by Elliptic.

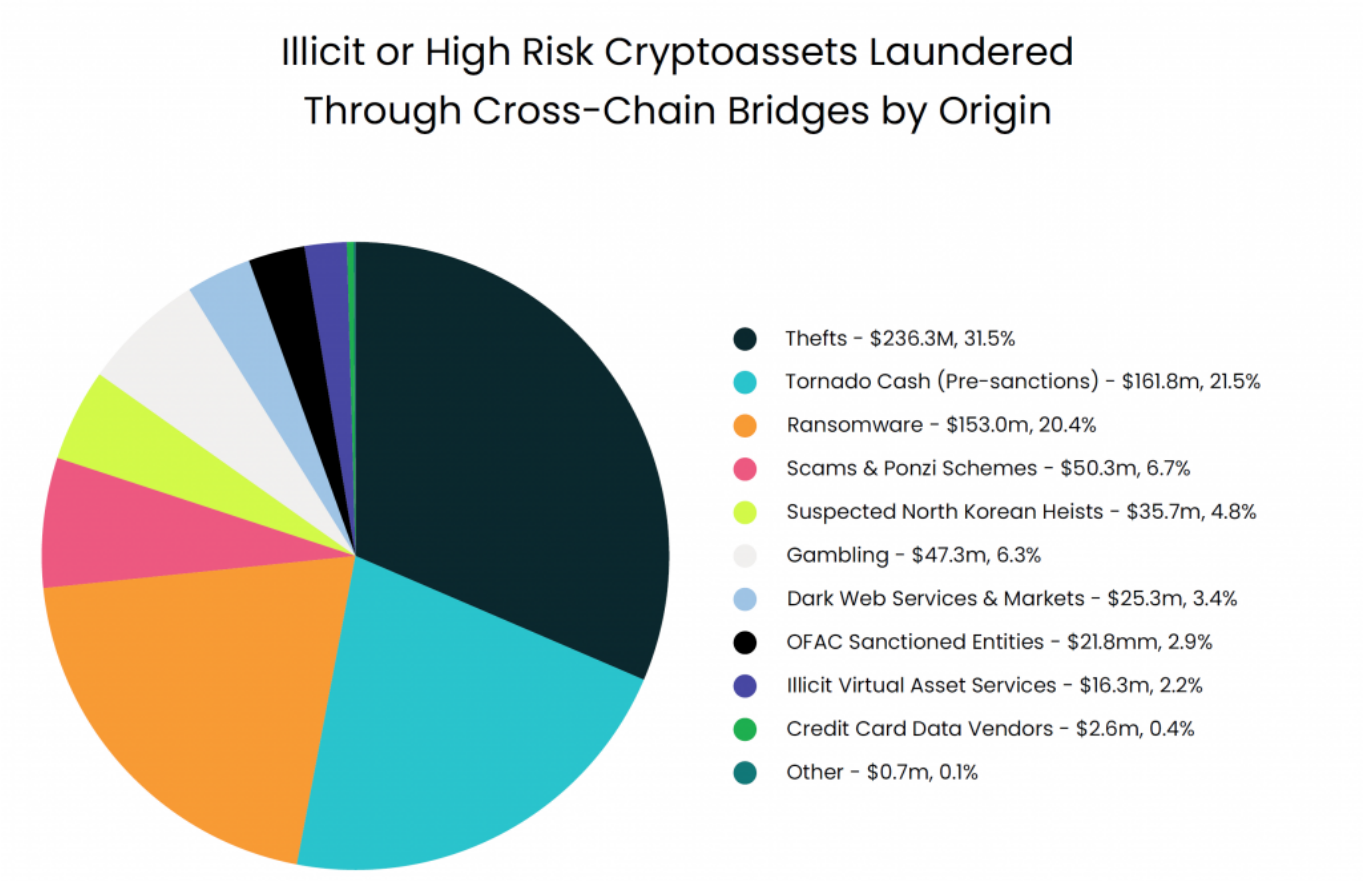
The Elliptic Cross-Chain Report 2022 analyses a range of crypto-related illicit activity to determine the ways in which these services have been exploited. The criminal activity mentioned includes hacking, dark web markets, online gambling, Ponzi Schemes, ransomware attacks and illicit virtual asset services.

DEX platforms use smart contracts to enable cross-asset swaps, so users can move assets across different blockchains efficiently. These users may use the swapping services for legal or illegal uses. Swapping stolen assets for a token with higher trading volumes, such as Ethereum using a DEX is the most common swap used by criminals.

A Cross-chain Bridge is another service which enables users to exchange tokens from one blockchain to tokens on another. For example, a user can exchange Bitcoin from the Bitcoin Blockchain to Wrapped BTC (wBTC), which is on the Ethereum Blockchain enabling value in BTC to be used with ETH compatible services.

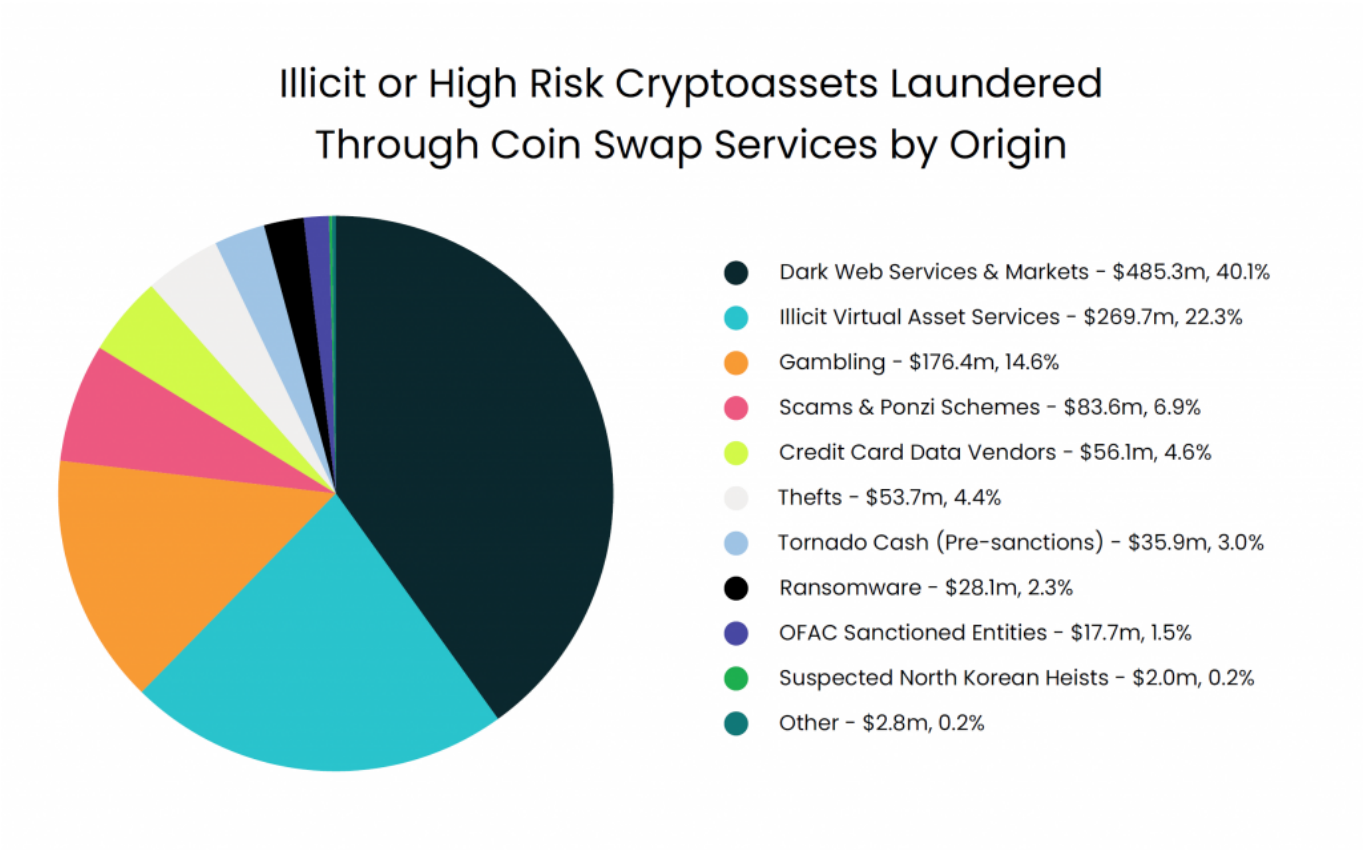
From January to July 2022, USD$1.2 billion worth of cryptoassets were stolen across eight cross-chain bridge exploits. Bridging has been used by criminals to add another level of transactions to seek to disguise their activities and to access services not available on the blockchain where the criminal proceedings originated. Of course the publicly visible nature of the blockchain means tracking services like Elliptic and Chainalysis can identify these movements in aggregate and hone in on illicit wallets and the identity of criminals over time.

More than USD$750M of illicit funds has been laundered through cross-chain bridges, according to Elliptic, with thefts comprising the largest amount.



Finally, Coin Swap Services allow users to swap cryptoassets for other tokens, which may be either on the same or on a different blockchain. Coin Swap Services generally do not require users to create accounts, nor do they verify customer identities. Many are advertised on illicit cybercrime forums.

Elliptic say that Coin Swap Services have been used to launder more than USD$1.2B of illicit crypto assets and are mainly utilised by dark web services and illicit virtual asset services.



Currently, Virtual Asset Service Providers (**VASPs**) use screening services like Elliptic and Chainalysis to determine whether tokens they receive originate from a wallet addresses associated with illicit activity, a form of "know your transaction" which may prove more effective than existing "know your customers" since it is impossible to hide the history of public blockchain assets.

Legacy screening solutions such as "know your customer" do not permit this level of monitoring at all, and holistic screening is used to monitor multiple chains and identify illicit cross-chain hops.

This kind of monitoring will undoubtedly help in dispelling the persistent but mistaken myth that crypto-assets are a 'wild west' and filled with fraud and scams. The crypto-asset space continues to grow and be used, in over 99% of transaction volume, for entirely legitimate purposes and pending regulation of centralised entities should only help dispel this myth further.

EU offers path to regulated token offerings

On 10 October 2022, the European Parliament Committee on Economic and Monetary Affairs endorsed the full text of the Markets in Crypto Assets Regulation (**MiCA**), which was previously approved by the European Council. MiCA is now one step closer to becoming law. The next stage is for the European Parliament plenary to vote and formally adopt MiCA, which could happen as early as November. If approved, MiCA will likely come into force in 2024.

MiCA is set to shape the regulatory landscape for how crypto-assets, crypto-asset issuers and crypto-asset service providers (**CASPs**) will be regulated in the European Union (**EU**) member states. This article is the second in our series of posts discussing the full text of the regulation approved by the European Counsel. Our first post addressed the extent to which NFTs are regulated under MiCA. This post discusses the pathway for regulated token offerings under MiCA.

MiCA lays down separate regimes for issuing:

- electronic money or e-money tokens (i.e. stablecoins which purport to maintain a stable value by reference to one official currency),
- asset-referenced tokens (crypto-assets which purport to maintain stable value by reference to something else, including one or more official currencies); and
- crypto-assets other than the first two categories (**crypto-assets**).

This post will focus on the third category being the rules applicable to offerings of crypto-assets generally. Special rules apply to e-money tokens and asset referenced tokens given the particular risks which relate to tokens which purport to maintain stable value. We will address these rules in a separate post.

MiCA applies to persons and other undertakings that are engaged in the issuance, offer to the public and admission to trading of crypto-assets or that provide related services in the EU (Art 2). Offerors are those who offer crypto-assets to the public, including issuers (Art 3 (7a)).

"Offer to the public" means:

> *a communication to persons in any form and by any means, presenting sufficient information on the terms of the offer and the crypto-assets to be offered, so as to enable potential holders to decide whether to purchase those crypto-assets.*

Generally under MiCA, if a person or entity offers a crypto-asset to the public, or seeks admission of a crypto-asset to trading on a trading platform, MiCA will require them to, among others:

1. be a legal person;
2. have a white paper for the crypto-asset;
3. notify their crypto-asset white paper to the competent authority of their home EU state;
4. publish the white paper.

Issuers of crypto-assets, unlike e-money or asset referenced tokens or CASPs, are not required to have or establish a legal entity within the EU. In that context, a token offeror's home EU state will be the State in which the crypto-asset is first offered or admitted to trading.

Specific obligations apply to the content and form of white papers and marketing communications relating to crypto-asset offerings. All information must be "fair, clear and not misleading" and include basic risk disclosures. Offerors may be liable to purchasers for failing to comply with disclosure requirements and the regulation contemplates a 14 day cooling off period for retail purchasers during the offer period and prior to admission to trading.

A crypto-asset whitepaper must be notified to the offeror's home EU state. Token issuers will also need to provide an explanation of why the relevant crypto-asset is not a financial instrument or other regulated product.

MiCA provides for certain exemptions from these requirements (e.g if the crypto-assets are offered for free, in the context of small or low value wholesale offers, or where crypto-assets are created as a reward for maintenance of a distributed ledger or validation of transactions).

MiCA also provides for transitional and grandfathering arrangements in respect of existing crypto-assets (Art 123). If a crypto asset's offer to the public ended before MiCA comes into effect, it will be exempted from the offering requirements. If a crypto-asset was admitted to trading on a trading platform before MiCA comes into effect, it will be exempted from admission requirements but remain subject to certain disclosure requirements. The grandfathering provisions under MiCA are likely to create an incentive to issue and obtain wide admission of crypto-assets to trading on exchanges prior to the regulation entering into force.

The token issuance provisions under MiCA represent a potential game changer for token issuers globally as they offer the promise of a regulated, relatively light touch, pathway to issuing tokens to the public. We anticipate that lawmakers around the world will be reviewing MiCA with interest as they craft their own regulatory regimes.