Article Information

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

Blockchain Bites: ASIC targets onshore crypto promoters, Australia issues sanctions advice to Digital Currency Exchanges, Uniswap seeks to skewer the SEC on Wells Notice, Popular Ethereum trading tactic targeted by US DOJ

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

ASIC targets onshore crypto promoters

In recent years, ASIC has issued a number of warnings to so-called "finfluencers" who promote investment products or provide financial advice on social media without a financial services licence. ASIC's latest action shows that the risks of engaging in unlicensed financial services also extend to offshore cryptocurrency related offerings, following a guilty plea by an Australia-based promoter of the collapsed cryptocurrency platform, BitConnect.

On 16 May 2024, John Bigatton from New South Wales pleaded guilty in a Sydney court to providing unlicensed financial services on behalf of BitConnect contrary to section 911B(1) of the Corporations Act. Central to ASIC's case against Bigatton was the allegation that BitConnect carried on a financial service business, which Bigatton helped promote during his time acting as a "national promoter" for the platform.

According to ASIC, BitConnect offered investment opportunities through its website, including a financial product known as the Lending Platform:

> The Lending Platform was promoted as an investment opportunity and in order to participate, investors were required to acquire BitConnect coin (BCC), a cryptocurrency token offered by BitConnect through its website.

ASIC said the Lending Platform permitted lenders to invest or "loan" BCC for a fixed term in exchange for promised high interest rate returns. Investors did not control their loans once invested, nor could they withdraw their capital investment until the expiry of the lending period.

ASIC first charged Bigatton in 2020 and banned him from providing financial services for 7 years. ASIC alleged Bigatton undertook promotional activities for BitConnect and the Lending Platform on social media, including at seminars that he hosted around Australia, and through face-to-face meetings with investors. He promoted these products without an Australian Financial Services licence.

A sentencing hearing will take place on 5 July 2024 which will determine the penalty. A related charge of operating an unregistered managed investment scheme was withdrawn following Bigatton pleading guilty to the charge.

This case demonstrates ASIC's tough stance against finfluencers and promoters of financial services and crypto-related products. In 2022, ASIC issued an information sheet for social media about discussing financial products and services

online. The information sheet also emphasises that it is the influencers' obligation to ensure that any content they post complies with the law.

The case also highlights the risks of promoting offshore cryptocurrency related offerings that are on risk of being deemed financial products. To prosecute finfluencers and other promoters, ASIC must first demonstrate that the products or services they promote are financial products or services. Here, ASIC's case was made easier after the founder of Bitconnect was indicted in the US for allegedly running a USD$2.4 billion cryptocurrency Ponzi scheme.

Crypto-related product issuers need to carefully assess whether the functions and description of their products involve a financial product or service. Finfluencers and promoters should also carefully assess the products and services they promote. Even when a product issuer has collapsed or is based offshore, regulators may still try to find someone – such as a promoter of the product – liable. It is therefore vital for anyone involved in promoting products which could potentially be a financial product to have sound legal advice.

Written by Jake Huang, Michael Bacina and Steven Pettigrove

Australia issues sanctions advice to Digital Currency Exchanges

The Australian Sanctions Office (**ASO**) has issued an advisory for Digital Currency Exchanges (**DCEs**). The advisory underscores the importance of adhering to Australian sanctions laws, which are applicable not only within Australia but also extend to activities carried out by Australian citizens, registered entities overseas, and on Australian-flagged vessels and aircraft.

The advice contains a number of key takeaways:

1. **Adherence to Compliance Obligations:** Like all other Australian persons and entities, DCEs are required to abide by Australian sanctions laws and to prevent the criminal abuse of crypto-assets. These laws are not limited to activities within Australia but also encompass those undertaken by Australian citizens and entities overseas, as well as on Australian-flagged vessels and aircraft;
2. **Cryptocurrencies as Assets:** Under sanctions laws, cryptocurrencies are treated as assets. It is considered an offence to make these assets available to designated individuals or entities (a list of whom the ASO updates regularly), or to engage in transactions involving cryptocurrencies owned or controlled by such designated parties;
3. **Due Diligence Measures:** DCEs are expected to exercise reasonable precautions to prevent facilitating transactions involving designated entities. This includes freezing cryptocurrencies controlled by designated entities and reporting such instances to the Australian Federal Police (AFP) and ASO;
4. **Integration with AML/CTF Programs:** DCEs are required to integrate sanctions compliance into their Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) programs. This includes wallet and customer screening, transaction monitoring as part of ongoing due diligence, IP-based login restrictions and complying with reporting obligations under the Anti-Money Laundering and Counter-Terrorism Financing Act 2006;
5. **Risk Mitigation Strategies:** DCEs are advised to implement pre- and post-transaction screenings, monitor high-risk jurisdictions, and enhance due diligence for transactions potentially linked to sanctions evasion activity; and
6. **Penalties:** Violations of sanctions laws are considered serious criminal offenses, attracting penalties that include fines and imprisonment.

In conclusion, the advisory serves as a reminder for DCEs to remain vigilant and proactive in their compliance efforts, given the evolving landscape of digital currencies and sanctions laws. In addition to the existing regime and laws that apply to DCEs, the implicit additional scrutiny that the ASO (and presumably other regulators of Australia) is placing upon DCEs means that DCEs should assess their own level of exposure to Australian sanctions laws and ensure they have appropriate risk based processes in place to mitigate the risk of breaching sanctions regulations. If you are in doubt as to whether a particular transaction is permitted under sanctions regulations, DCEs are encouraged to seek professional advice.

Written by Luke Higgins and Steven Pettigrove

Uniswap seeks to skewer the SEC on Wells Notice

The clash between Uniswap Labs and the US Securities and Exchange Commission (**SEC**) continues for the future of financial innovation. In a recent blog post entitled "The fight for DeFi continues", Uniswap Labs has again responded to the Wells Notice that was issued against them by the SEC in April of this year, advocating for the recognition and support of

open source technologies that aim to enhance traditional financial systems, rather than disrupt. The blog post was accompanied by a link to Uniswap's formal submission to the Wells Notice.

Uniswap Labs argues that the SEC should embrace technologies like the Uniswap Protocol, which offer a secure, low-cost, and transparent infrastructure. These qualities align closely with the SEC's own mission to protect investors and maintain fair, orderly, and efficient markets:

> The Uniswap protocol is secure, low cost, transparent infrastructure that "protects investors and maintains fair, orderly, and efficient markets." Ironically, that's the SEC's mission.

The post argues that the SEC's current approach seems to extend its regulatory reach beyond traditional exchanges, targeting communication technologies and various market types. Uniswap argues that this expansion is an overreach, stating that some of the SEC's legal arguments have already been refuted in court. Unfortunately, no explicit case or proceeding is referenced by the SEC.

Coinbase's challenge to the SEC's enforcement powers over cryptoassets under the so-called "major questions" doctrine was rebuffed in an interlocutory judgment earlier this year. Interestingly, however, the FIT 21 bill has passed the House in the US and aims to grant the Commodity Futures Trading Commission (CFTC) robust authority over digital asset trading, indicating a potential shift in regulatory oversight that may curb the SEC's expansive ambitions.

Uniswap contend that their protocol represents a paradigm shift in how markets operate by allowing users to transact directly with one another without relying on centralised intermediaries (a core pillar of the thesis statement for blockchain technology). Decentralised models eliminate the need for middlemen, who often impose fees and hold users' assets, leading to higher costs and potential security risks. Uniswap argues that many traditional markets are inefficient or not transparent, operating on a limited basis (i.e., 9-5 hours on weekdays as opposed to 24/7).

Regarding the SEC's assertion that the Uniswap Protocol is an unregistered securities exchange controlled by Uniswap Labs (amongst other similar assertions), Uniswap contends that:

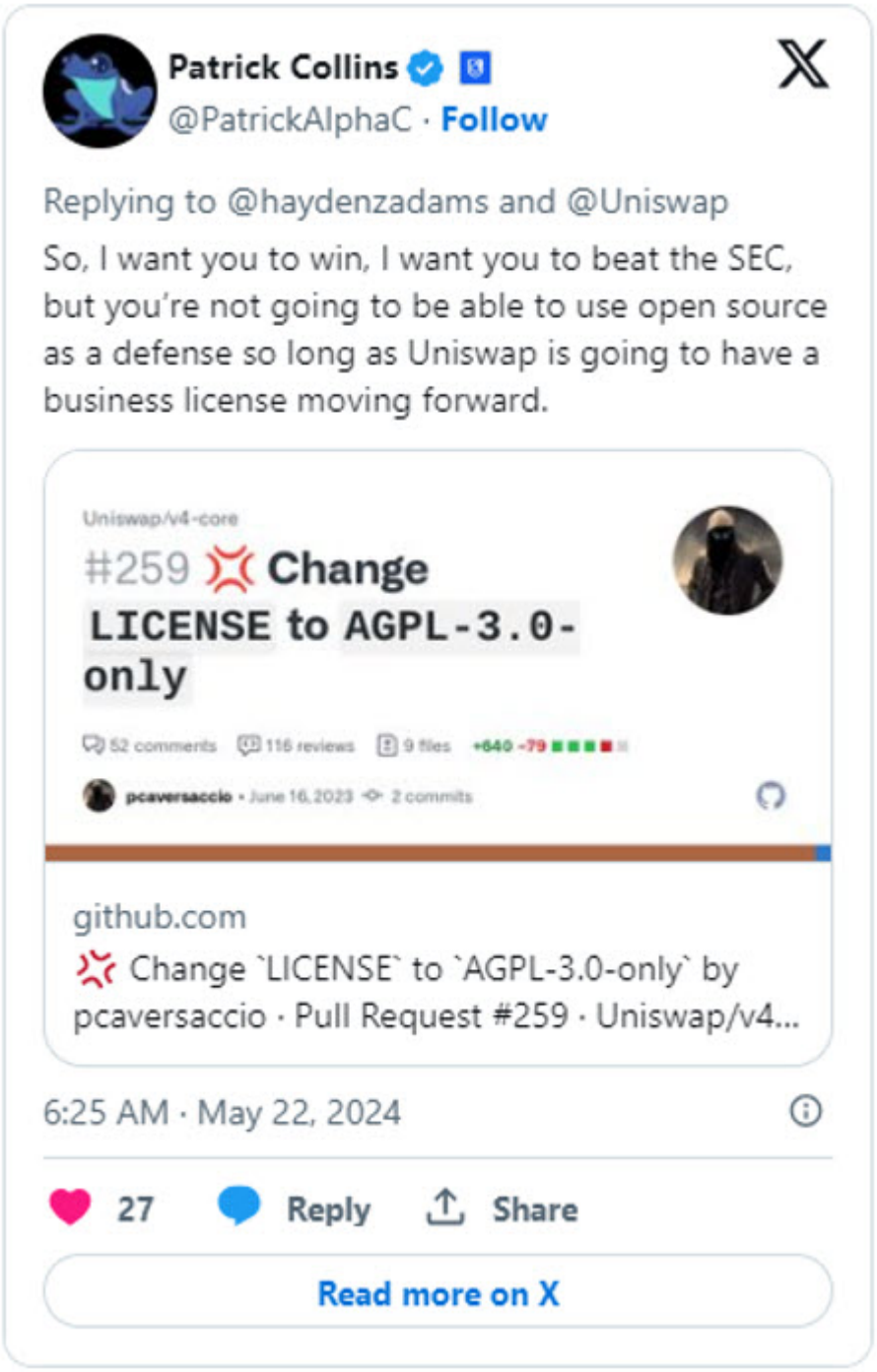
> [t]hese assertions assume that value represented in a specific digital file format is a security – and that the SEC can unilaterally extend the definitions of exchanges, brokers and contracts to the point of meaninglessness.

Uniswap likens crypto-assets and tokens to file formats akin to PDFs, with the Uniswap Protocol operating like a general-purpose internet protocol. Uniswap further contends that the distribution of UNI tokens to early adopters and testers of the Protocol involved no contracts or profit expectations based solely on Uniswap's efforts, undermining the SEC's assertion of these tokens as securities.

Uniswap remains steadfast against contrary claims to the legitimacy of its operations and is prepared to defend its approach. Uniswap argues that the SEC should not expend taxpayer resources on litigating against technological advancements that challenge and improve outdated systems. Uniswap's legal team, with a proven track record against the SEC in the Ripple and Grayscale cases, is ready for the fight.

Despite the looming legal battle, Uniswap is undeterred in its mission to innovate, which has proven inspiring for blockchain enthusiasts and industry members alike with many taking to social media to express their support:

This is not to say that Uniswap's approach has not been met with some *healthy* criticisms. In response to the [founders' posts on X announcing their reply to the Wells Notice and the blog post], many expressed their concerns with some of Uniswap's arguments:


Patrick Collins
@PatrickAlphaC · Follow
Replying to @haydenzadams and @Uniswap
So, I want you to win, I want you to beat the SEC, but you're not going to be able to use open source as a defense so long as Uniswap is going to have a business license moving forward.
Uniswap/v4-core
#259 Change LICENSE to AGPL-3.0-only
52 comments
116 reviews
9 files
+640 -79
pcaversaccio · June 16, 2023
2 commits
github.com
Change `LICENSE` to `AGPL-3.0-only` by pcaversaccio · Pull Request #259 · Uniswap/v4...
6:25 AM · May 22, 2024
27
Reply
Share
Read more on X

The unfolding conflict between Uniswap Labs and the SEC represents a critical juncture in financial regulation. Embracing blockchain technology and open source innovation can lead to more robust and equitable financial systems. It is imperative for regulators to support these advancements rather than stifle them through litigation. This case will not only shape the future of Uniswap, but also the broader landscape of financial technology.

Written by Luke Higgins, Steven Pettigrove and Michael Bacina

Popular Ethereum trading tactic targeted by US DOJ

The US Department of Justice (**DoJ**) has turned its attention to popular MEV trading tactics unsealing an indictment against brothers, Anton and James Peraire-Beuno, who face up to 20 years in prison over an "MEV attack" on the Ethereum blockchain that netted the pair USD$25 million worth of cryptocurrency.

In the indictment unsealed by the DoJ, the brothers have been charged with conspiracy to commit wire fraud, wire fraud, and conspiracy to commit money laundering after their 12-second attack took advantage of normal trading practices.

MEV, or maximal extractable value, is a software used by a majority of Ethereum validators to verify transactions on the Ethereum blockchain. Validators can use the MEV system to see transactions before they are officially verified and added to the blockchain. Traders can leverage this information to prioritise transactions with higher fees and inserting their own transactions ahead of others such that it affects the market price of the asset and gaining value from buying or selling based on the price movement. Some compare the practice to front running in traditional markets.

The process works as follows:

- Transactions are submitted by Ethereum users which are added to a "mempool", a digital area where transactions sit briefly before being validated and added to a block in the chain;
- Bots set up through the MEV (called "Searchers") access the mempool and assess which transactions could result in profitable trades;
- In order to bundle the potentially profitable transactions together, the Searchers validate a target transaction, a signed transaction before the target transaction, and a signed transaction after the target transaction;
- The Searches employ a range of tactics, for example rearranging certain transactions to make a trading profit;
- The transactions are then verified by Ethereum validators and become part of the irreversible blockchain.

The whole process usually takes a few seconds and enables MEV Searchers to benefit from transactions at the expense of Ethereum users.

The Ethereum community more or less accepts these practices, due to the difficultly in eradicating it and where the profits

are relatively insignificant. However, the Peraire-Bueno brothers alleged exploit went far beyond what many in the community consider to be reasonable.

In order to effect the attack, the brothers allegedly targeted the MEV Searchers when they sought to validate the three transactions (being the target, before signed and after signed transactions). The DoJ allege the brothers set up validators designed to entice the MEV Searchers into honeypot transactions, and using 'false signatures' were able to receive the full content of the proposed block, including private transaction information.

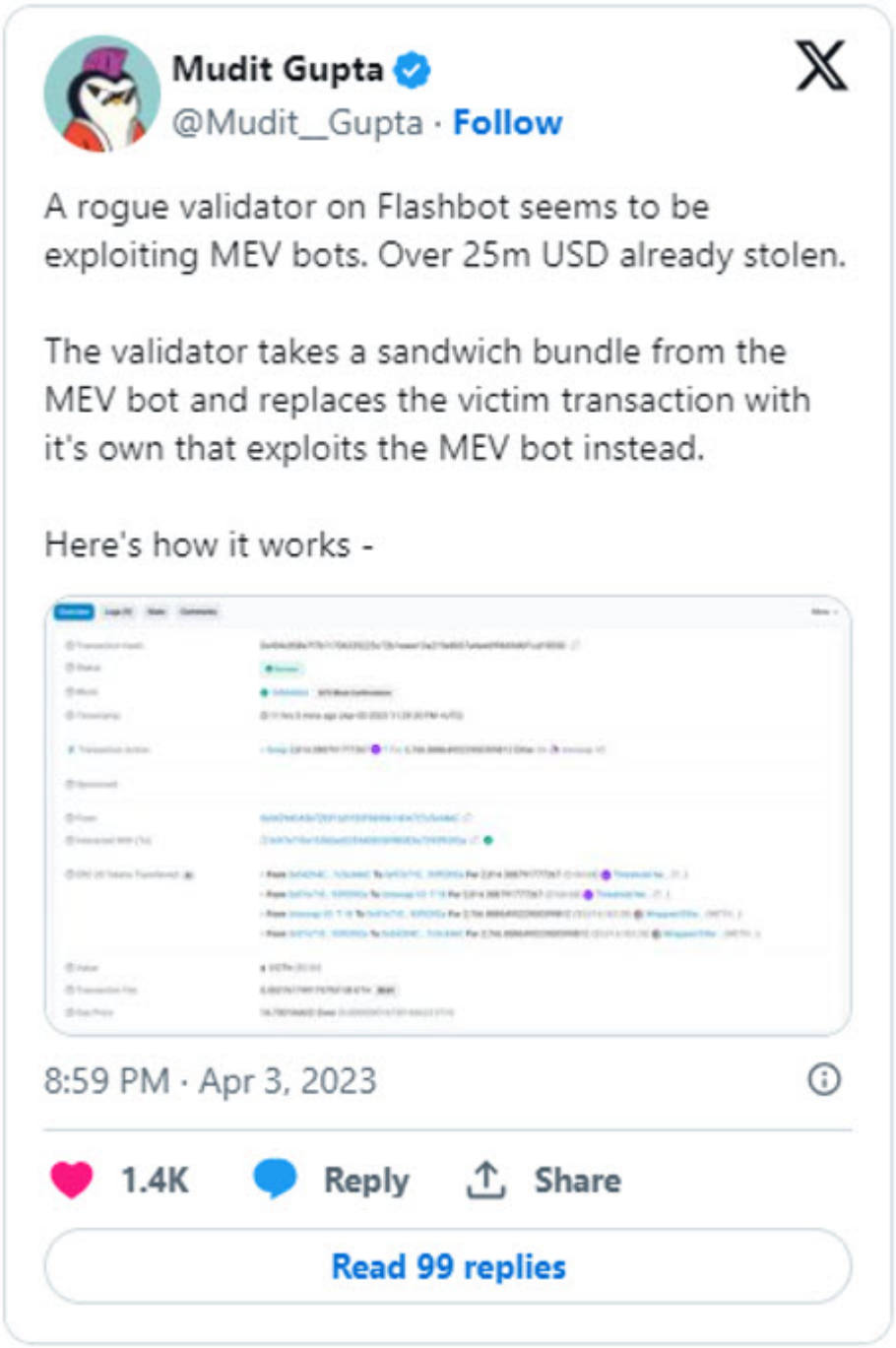
The attack has raised a number of questions in the Ethereum, and broader crypto communities. Namely, it has re-enlivened the "code is law" discussion, where one side believe stealing is stealing irrespective of how it comes about, and the other side contend that if the code allows an exploit, then the practice is acceptable at law.

The debate also made rounds when the DOJ indicted Avraham Eisenberg who drained USD$110 million from Mango Markets by exploiting the perpetual futures market. In that instance, Eisenberg bought perpetual futures referencing Mango's governance token, before initiating a large volume of buy orders on multiple crypto exchanges, resulting in a price increase which he cashed in on without proceeding with the buy orders.

For the two brothers, however, prominent community members (for example MetaMask's lead product manager Taylor Monahan) believe this particular exploit crossed the line of what is generally allowed.

In its press release, the DoJ claimed the attack "exploited the very integrity of the Ethereum blockchain", a statement that lends itself to the overarching sentiment by the DoJ that blockchains are inherently vulnerable.

Crypto community members, specifically those who are in tune with the Ethereum ecosystem, quickly recognised the attack for what it was, which is an exploit of a bug in the code, something made technically possible by the Ethereum code. As it was happening, X user "Mudit Gupta" laid out (in code) how the attack works:



With the brothers now facing up to 20 years in prison, the US Courts look likely to decide their fate and the boundaries of fraud and legitimate arbitrage activity in the context of blockchain validator networks and MEV trading.

Written by Michael Bacina, Steven Pettigrove and Luke Misthos