Article Information

Author: Michael Bacina, Steven Pettigrove
Service: Blockchain, FinTech
Sector: Financial Services, IT & Telecommunications

Blockchain Bites: The Merge is here, Black Market for Stolen NFTs, ATO (air)drops new guidance, Gensler urges crypto registration, Coinbase insider pleads guilty, KKR jumps into Avalanche for PE offering

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

The Merge is here!

The Ethereum Merge has finally arrived following months of upgrades, developments, and a first-of-its kind transition on a blockchain of this size. The Merge is designed to offer a more-sustainable future for the second largest (by market cap) cryptocurrency, Ethereum, by substantially reducing the energy it takes to verify transactions.

The old Ethereum Blockchain has 'merged' with the Beacon Chain which was launched in 2020 to test the proof-of-stake system. This evolution has been in the works since the start of Ethereum and fits into a broader roadmap of ongoing improvements to Ethereum.

The old Ethereum Blockchain used a consensus model similar to Bitcoin, with nodes verifying transactions using a proof-of-work (**PoW**) model. Proof of work uses energy intensive computers to solve complex mathematical problems in order to verify transactions. Before the Merge, Ethereum was estimated to be using as much electricity as the Netherlands.

In an ambitious move to redevelop the software without ceasing trading, in a move said to be similar to be akin to changing out a petrol engine for an electric motor while a car is driving, Ethereum is now running on proof-of-stake (**PoS**), which requires validators to hold and stake tokens. Validators are selected at random to mine the next block and once a designated number of validators have verified the block is accurate, the next block will be created.

Validators receive rewards proportionate to their staked tokens, without having to expend large amounts of energy and makes participation in the consensus nodes cheaper and easier.

Holders of ETH and ERC-20 tokens do not need to do anything for their tokens to continue to function as normal, but a raft of scams are expected to try and trick people into handing over their private keys or transferring their tokens to scammers.

The Merge has not only revamped thousands of decentralised apps that rely on the Ethereum Blockchain, but potentially reduced the overall energy usage of the entire world by 0.2%.

Merge parties were held around the world, luckily in Australia the merge time was about 5pm AEST but many stayed awake to watch history be made:-

The network will be watched closely for any bugs or unexpected operations in the coming days but so far the Merge is being considered one of the greatest open source software successes to date.

The Black Market for Stolen NFTs: Elliptic Report

The rise of non-fungible tokens (**NFTs**) with secure ownership on the blockchain has been followed swiftly by scams

seeking to steal NFTs and flip them for a profit, leading to a distinct economy for the stolen goods. Thanks to the traceable nature of blockchains, however, that economy can be identified and studied faster than would be the case for a traditional black market.

A new report from blockchain analytics' company Elliptic gives us an update on NFT-based scams, sanctions risks, market manipulation and money laundering. The risk to marketplaces and exchanges is presently small but significant and growing. Some exchanges have been subject to lawsuits over their management of stolen assets, alleging that marketplace operators have failed in a duty to flag or freeze onward sales. In particular, marketplace operators need to be vigilant at all times for scammers within the NFT community, as it only takes seconds of complacency or accidental clicks to result in losses which can run into the millions of dollars.

How are scammers operating?

Scammers often use social media to steal NFTs using phishing links and impersonate NFT marketplace support staff. Scammers often then list stolen NFTs at very low prices, taking advantage of bots deployed by other NFT traders on marketplaces which are designed to detect and acquire NFTs at cheap prices.

In February 2022, a phishing attack occurred where over 200 NFTs worth USD$5.1 million were stolen and represented the single largest NFT phishing heist on record. The scammer ended up returning two thirds of the stolen NFTs back to their owners but kept the higher-value NFTs. The scammer sold the remaining assets across 3 NFT marketplaces. Of those, 45 were purchased and sold by their buyers within 5 days of the attack. The scammer gained USD$1.42 million from the 45 stolen NFTs, for around 8% lower than their total floor price at the time (USD$1.54 million). All but 10 of these were flipped for a profit by the subsequent buyers who grossed USD$1.77 million from their sales, meaning that 13% of the monetary gains were made by the initial buyers rather than the scammer. This demonstrates the attractiveness of this emerging black market of stolen NFTs. Additionally, one user minted an NFT and sent it to the scammer with a note saying:

> *Hello, I am interested in buying the NFTs you have on you [right now]. I can buy them in bulk at 50% of floor price.*

Nevertheless, buyers often purchase stolen NFTs without realising their stolen nature, and on becoming aware of the theft, these buyers prefer to sell them at a loss rather than flip them for a profit. The reasons for this include avoiding negative publicity in the NFT community or disposing of stolen assets as quickly as possible to mitigate the risk of complicity. The community actively calls out users interacting with stolen NFTs and openly urges the return of the NFTs or sale back to the victims, as is what happened to the 3 stolen Mutant Apes which were subject of a phishing scam on 20 February of this year. Two of the stolen Apes were sold by their initial buyers at a loss as a result.

What can marketplaces and exchanges do to combat this?

Some ways in which marketplaces and exchanges can fight these types of scams:

- Have procedures in place to flag, freeze or delist stolen assets once a credible theft report has been made.
- Scammers risk being banned from major marketplaces and potentially be left with unsellable assets if a report is made. Therefore, encouraging scam victims to report and lock NFTs during negotiations with scammers, even offering to buy back their assets at reduced prices is a successful strategy for that reason.
- Highly public campaigns through the use of social media and other channels frequented by the NFT community can be a huge success in being able to block sales on major NFT marketplaces at once. An example is the Calvin Becerra campaign on Twitter in regards to stolen BoredApeYC NFTs. Successful campaigns such as this leave scammers and potential onward buyers with no avenue to sell stolen assets, with the only viable option being the return of the stolen NFTs at a negotiated ransom.

NFT marketplaces and exchanges need to be proactive in reporting and responding to theft reports and detecting malicious activity through their services, including using wallet screening and transaction monitoring tools like Elliptic, Chainalysis or TRM Labs.

Red flags for exchanges to consider include:-

- where an NFT has been sold in quick succession over several marketplaces and swap services;
- where an NFT has been sold at well below the floor price;
- where NFTs that have been quickly sold have been bought by the same set of users who may be running bots;
- if funds have gone into Tornado Cash or other mixers shortly after NFTs have been exchanged;

- the transaction wallet has numerous comments on its blockchain explorer page about being involved in prior hacks or scams; and
- a search of the associated wallet address on a search engine or social media reveals that it has been implicated in prior hacks or scams.

The key for exchanges is to act swiftly, be vigilant and on alert with action plans in place and ready to be implemented as soon as potential scam activity is detected. Scam reports may originate from numerous sources so NFT marketplaces and crypto exchanges alerted can act swiftly to block suspect addresses identified through different platforms. The more marketplaces which do this, the more scammers can be prevented from easily cashing out the stolen assets, decreasing incentives for NFT theft overall.

Australian Tax Office (air)drops new airdrop guidance

The Australian Taxation Office (**ATO**) has issued new guidelines on how Australia's tax regime applies to cryptocurrency rewards and new tokens earned from staking crypto assets.

There is a wide variety of what constitutes staking in the crypto market, but the ATO has provided the following high-level definition:

> *Staking involves locking your existing crypto asset tokens to validate transactions on the blockchain and create new blocks. The users who create new blocks in this system are known as forgers.*

The ATO views 'forgers' who create new blocks should treat the tokens they receive as ordinary income and to declare that on their tax return.

The guidance also looks at the proof-of-stake consensus mechanism – where forgers hold units of a crypto asset to validate transactions to create new blocks. Upon the verification of a transaction on the network as valid, there is a consensus.

The ATO then takes the opportunity to look at other consensus mechanisms that reward existing token holders for their role in maintaining the network and which also have the same tax outcome. Rewards received through: i) proof of authority and proof of credit mechanisms by validators; ii) agent nodes and guardian nodes; and iii) premium stakers and other entities performing comparable roles, will also be treated as reportable ordinary income.

A forger or miner will also receive ordinary income equal to the monetary value of the tokens they receive as a reward for participating in proxy-staking or voting with their tokens in a consensus mechanism. The key is that the staker has received something with a known market value.

Importantly, when a token holder disposes of a crypto asset earned through any of the above staking processes, they will also need to work out whether they have made a capital gain or loss for the purposes of CGT.

In relation to 'airdrops' – a tool used to distribute crypto assets to a group of people (whether they want it or not) to try and increase the adoption of a token, the ATO has now said the monetary value of an established token received in an airdop is also reportable ordinary income at the time of receipt.

Thankfully, where a crypto project has made an initial airdrop of tokens that is the very first distribution of its tokens, and where there has been no trading in the project's tokens prior to the airdrop, that is there is no market value, the ATO will consider that the token holder does not derive ordinary income or make a capital gain at the time of receipt, but if the tokens are free (which is usually the case under an airdrop), they have a cost base of zero and the whole of any subsequent sale or swap for any amount above zero will trigger a CGT event, but the tokens will be eligible for a normal 50% CGT discount if the assets are held for longer than 12 months.

This guidance follows the repeated requests from the industry for clearer guideance from regulators in the absence of legislative reform. In June this year, federal Treasurer Jim Chalmers issued a statement confirming that the Labor government planned to introduce legislation clarifying the tax treatment of digital currencies.

Last week, Treasury released an exposure draft of the legislation which seeks to clarify that digital currencies will not be taxed as foreign currency under Australian law, in line with the Administrative Appeals Tribunal's decision in *Seribu v Federal Commissioner of Taxation*. That submission process continues and with the Board of Taxation continuing their review, we expect to see more clarification of the Australian tax position regarding crypto in coming months.

Square peg round hole: Gensler urges registration of crypto-assets despite regulatory mismatch

The Chairman of the United States Securities and Exchange Commission (**SEC**), Gary Gensler, has reiterated his reductive approach to the regulation of cryptocurrency and digital assets in a speech titled '*Kennedy and Crypto*'.

Presented as part of 'SEC Speaks', Gensler opened by recognising past leaders of the US and its landmark investor protection legislation: The Securities Act of 1933, the Investment Company Act of 1940 and the Securities Exchanges Act of 1934. Gensler repeated his previous views that he considers that almost all crypto-asset tokens are 'securities' (noting the speech does not purport to be official SEC policy) and that:

> *Nothing about the crypto markets is incompatible with the securities law. Investor protection is as relevant, regardless of underlying technologies.*

Few could disagree with the second sentence, but the first sentence raises serious concerns. Despite instructing his SEC staff to encourage entrepreneurs to have their tokens registered and regulated under existing securities law, only a tiny 'handful' of crypto tokens have managed to be registered as securities, which suggests some incompatibility must exist. Indeed, in many cases, the nature of and rights attaching to crypto-assets are quite different from traditional securities. In the years since the SEC's Munchee Order, the DAO Report and other 'regulation by enforcement' actions have hit US crypto projects, standing in stark contrast to Gensler's invitation to projects to 'come in' and register.

Interestingly, Mr Gensler's approach is also at odds with a number of significant bipartisan reform proposals currently making their way through the US Congress, including the draft Responsible Innovation Act and the draft Digital Commodities Consumer Protection Act.

Despite the reality of crypto-asset regulation not being fit for purpose in the US becoming increasingly clear, Gensler remains steadfast in his view that:

Not liking the message is not the same as not receiving it

It appears that Mr Gensler, unlike other Commissioners, wants innovation in digital assets only to occur in the narrow ways that laws designed for a centralised financial system will permit. Commissioner Pierce has been praised for calling out the lack of regulatory fit in the US, and pressing for sensible reforms and Commissioner Uyeda in a recent speech also said:

> *Rulemaking can be challenging and time-consuming. It may be tempting to develop "new" interpretations of existing statutes and rules and apply them through enforcement action. This temptation should be avoided.*

He continued in noting the two key issues are:

> *does the crypto asset constitute a security and, if so, h**ow do market participants comply with the federal securities laws and the Commission's rules**. To date, the Commission's views in this space have been more often expressed through enforcement action. This is an example of a situation where regulation through enforcement does not yield the outcomes achievable through a process that involves public comment. (emphasis added)*

Many jurisdictions face similar problems, with a substantial education gap meaning that often the suggestion is made that cryptocurrencies should be simply regulated like a "normal" financial product. The fundamental differences between centrally issued and controlled financial products with walled markets permitting trading only under strict rules with carefully admitted participants, and the freeflowing nature of global permissionless blockchains prevent an easy fit.

Few major regulators have set out for crypto projects a path by which they can comply with securities laws and overcome requirements which are entirely sensible for a centralised system but become illogical when applied to a decentralised system. The current approach of some is to suggest that there is only decentralised theatre at work, and in truth small groups of centralised individuals operate crypto projects. While that may be true for some projects (a great number in the early stages of a crypto project as they journey towards fully decentralised decision-making), it is not the case for many more established projects.

The SEC has a history of crypto 'regulation by enforcement', launching a range of investigations and lawsuits against crypto projects such as Coinbase and Uniswap Labs. This is despite concerns voiced by the industry as to the lack of clear guidance as to what features the SEC will or will not regard as indicative of whether a crypto-asset is a security and

examples of how a crypto project can register under existing US securities laws. Coinbase's General Counsel recently called out the regulatory mismatch and suggested a proper fit for purpose regime be developed.

To date, there is no example provided by the SEC as to how a decentralised crypto project could comply with US securities laws, and projects are left with a choice to try and register their tokens as securities (and accept the significant costs, delays, practical limitations and uncertainty as to how or whether they can in fact comply), avoid the US market entirely, or risk being the next target of the SEC.

At some point, the "technologically neutral" approach taken by regulators in relation to crypto-assets may need to be revisited. Laws have had to address specific technologies of cars, radio, mobile phones, tv and the internet, and it seems increasingly likely that the activity based regulation of financial services will need to evolve to accommodate both investor and consumer protection and the technological innovations brought by decentralised technologies.

Coinbase Insider Trader Pleads Guilty

Earlier this week, Nikhil Wahi, the brother of a former Coinbase product manager, has pleaded guilty to one count of conspiracy to commit wire fraud in connection with a scheme to commit insider trading in crypto assets. The charge carries a maximum sentence of 20 years.

Nikhil Wahi was arrested in July this year, after being alleged to have used confidential Coinbase information about which crypto assets were about to be listed on Coinbase. Nikhil Wahi had transferred funds, crypto assets and proceeds through multiple anonymous Ethereum blockchain wallets.

Damian Williams, the United States Attorney for the Southern District of New York, said:

> *Less than two months after he was charged, Nikhil Wahi admitted in court today that he traded in crypto assets based on Coinbase's confidential business information to which he was not entitled.*
>
> *For the first time ever, a defendant has admitted his guilt in an insider trading case involving the cryptocurrency markets.*
>
> *Today's guilty plea should serve as a reminder to those who participate in the cryptocurrency markets that the Southern District of New York will continue to steadfastly police frauds of all stripes and will adapt as technology evolves. Nikhil Wahi now awaits sentencing for his crime and must also forfeit his illicit profits.*

Coinbase employees were frequently exposed to confidential and privileged information prior to the public being informed about tokens to be listed on the exchange. For almost a year, Nikhil Wahi used unanimous Ethereum blockchain wallets to buy up crypto-assets after being tipped by his brother Ishan Wahi before they were publicly listed on Coinbase. The crypto assets were then sold for a profit.

Coinbase had a strict internal process that prohibited its employees from sharing any confidential information with others, as this could impact the market price. Nikhil Wahi's charge was one of three that were the first ever crypto insider trading tipping scheme prosecuted in the US. Ishan Wahi, a former Coinbase product manager and Nikhil's brother, was charged for allegedly tipping off Nikhil Wahi and Sameer Ramani (who was a friend of Ishan Wahi) about upcoming token sales, making profits of USD$1.1M by front running listings in over 25 tokens.

As part of the prosecution, the SEC had made allegations that the tokens involved in the insider trading scam were securities under US law. At the time Coinbase was critical of the SEC investigation, citing the lack of clear guidance and rules for defining cryptocurrencies as securities under US law.

Coinbase's Chief Legal Officer, Paul Grewal said to Coindesk:

> *We are confident that our rigorous diligence process – a process the SEC has already reviewed – keeps securities off our platform, and we look forward to engaging with the SEC on the matter.*

Nikhil Wahi is scheduled to be sentenced in December for his crimes and the prosecution of the others continues. The question of whether the tokens involved in the trading scandal are securities or not will not be decided by the guilty plea, but will have to wait for another case as the SEC continues "regulation by enforcement".

KKR jumps into Avalanche for PE offering

On Tuesday, global investment firm, KKR & Co, announced a partnership with digital asset management firm, Securitize, to tokenise its private equity fund "Health Care Strategic Growth Fund II" on Avalanche, a public blockchain network. KKR offers alternative asset management, capital markets and insurance solutions to its clients. Securitize manages and tokenises institutional-grade products, leveraging blockchain based capital markets and financial solutions.

Commenting on the development Securitize CEO, Carlos Domingo, said:

> *'This new fund is an important step toward democratizing access to private equity investments by delivering more efficient access to institutional-quality products…Tokenization has the potential to address many of the biggest challenges for individual investors seeking to participate in private market investing by enabling technological and product innovations that were not possible before'.*

The Health Care Strategic Growth Fund II is a $4 billion fund and invests in growing healthcare companies in North America and Europe. The development is facilitated by Avalanche, an eco-friendly smart contract platform based on proof of stake technology. Investors in the new fund will have to hold the security for at least a year prior to selling it to other qualitied purchasers on a secondary market managed by Securitize. Tokenising private equity investments should allow individuals to access investments in smaller amounts, enhance operational efficiency and facilitate greater liquidity.

Managing Director and Co-Head of KKR, Dan Parant, commented on the partnership:

> *'With its ability to digitize operational inefficiencies and increase ease of use for individual investors, blockchain technology has the potential to play an important role in the future of private markets… We're excited to be working with Securitize to be an early adopter of this technology and look forward to opening our investments up to a new audience of investors'.*

KKR's new partnership follows a string of recent announcements by institutional players who are looking to leverage the benefits of blockchain technology for clients and enhance their digital assets offerings, such as State Street, Blackrock and Barclays. Despite the onset of crypto-winter, institutional interest in blockchain technology continues to grow unabated.