Article Information

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

Blockchain Bites: Crypto crime as tech entrepreneurship, Australia Fights Crypto Scams, Ripple rides on as $2B SEC wave ebbs with $125M spray, UK draft bill proposes third category of personal property

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.

Defeating digital rogues: Crypto crime as tech entrepreneurship

The rise of crypto-assets and blockchain technology has brought innovation and disruption to global financial systems. However, alongside these advancements, a parallel ecosystem of criminal activity has emerged which often leverages the unique features of blockchain technology. In their SSRN working paper "Crypto Crime as Technology Entrepreneurship", Darcy Allen and Aaron Lane of the Royal Melbourne Institute of Technology (RMIT) argue that crypto criminals operate in a manner similar to conventional technology entrepreneurs.

The entrepreneurial landscape of crypto crime

Crypto criminals, just like legitimate entrepreneurs (at least, the successful ones), are adept at identifying opportunities within a given market.

> Similarly to conventional entrepreneurs, crypto criminal entrepreneurs allocate resources based on perceived opportunities and costs, adapting to shifts in regulation and technology.

The pseudonymity and censorship-resistance that is inherent to blockchain technology provides new ground for various illicit activities. However, these relatively new technologies also allow for greater opportunities for enforcement.

> …decentralised, immutable, programmable and transparent global technologies both provide new opportunities for constructing and executing crimes, but also create new opportunities for private and legal enforcement.

Allen and Lane outline what the various characteristics of crypto mean for crypto criminals. These are summarised as follows:

1. Global and interoperable: Crypto facilitates easier, cheaper, and faster value transfer globally, meaning criminals face less lock-in to specific institutional systems and lowering their exit costs. However, this also means increased competition and reduced rewards accumulated from each jurisdiction.
2. Open-source and transparent: Opportunities for exploitation (e.g., hacks) are more transparent as the entire history of blockchain networks and code is public. However, this transparency simultaneously aids law enforcement in tracking and detecting crimes. So-called "whitehat" hackers can use this information to recoup funds (read more about whitehat hacker initiatives here).

3. Censorship resistance and self-sovereignity: This ensures that transactions cannot be altered or reversed, providing security for criminals and allowing unprecedented control over crypto-assets. However, criminals must navigate a steep learning curve with experimental technology, and many secure storage devices (i.e., physical hardware wallets) can leave a trail of evidence if caught.

Taxonomy of crypto crimes

Allen and Lane propose a taxonomy of crypto crimes, noting that there are two primary ways in which crypto criminals can extract crypto-assets from victims. The first method is by theft, whereby criminals directly take the crypto-assets. The second method is via fraud, whereby criminals obtain crypto-assets by deception. Allen and Lane further state that there are three main types of crypto-crime within both theft and fraud: "conventional", "intermediary-enabled", and "decentralised". A taxonomy explaining this table is extracted below:

Table 2 – Taxonomy of Crypto Crime

	Conventional	**Intermediary-Enabled**	**Decentralised**
Theft	Stealing a Hardware Wallet Stealing/Copying Private Keys (or recovery phrases)	Stealing from a Digital Currency Exchange Misappropriation of assets under custody	Hacking of Decentralised Exchange Smart Contract Exploits
Fraud	Malware with Crypto as Payment Method Investment or Romance Scam with Crypto as Payment Method	Fake Initial Coin Offerings Pump and Dump Schemes	Rug Pulls in Decentralised Finance Flash Loan Attacks in Decentralised Finance

Source: Allen, Darcy W E and Lane, Aaron M., Crypto Crime as Technology Entrepreneurship (August 05, 2024). Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4915881

Economic perspectives on crypto crime and the role of the private sector

Allen and Lane propose that changes in technology and regulation can shift the costs associated with different types of crimes, prompting criminals to adapt their strategies. For instance, increased regulation in one area may lead to a shift towards more decentralised and harder-to-regulate activities.

> …it is possible that [anti-money laundering regulations, centralised exchange licensing and investments in traceability technology] don't decrease the level of crime, but rather change the allocation between different criminal activities.

The authors contend that the private sector will play a crucial role in addressing crypto crime in the years to come. Organisations are already developing sophisticated tools, such as blockchain analytics and tracking software, to enhance security and increase the transaction costs for criminals. These technologies not only aid law enforcement but also help legitimate businesses protect their customers and assets.

> Just as we saw private orderings and private governance solutions emerge to crime in the early days of the internet…we anticipate greater investment within the cryptocurrency industry itself to suppress criminal activities in order to reduce transaction costs and expand the cryptoeconomy.

Conclusion

The analogy of crypto criminals to entrepreneurs provides a valuable framework for understanding the dynamic nature of illicit blockchain activities. As technology and regulations continue to develop, so too will the strategies used by these nefarious actors. Allen and Lane's paper highlights that effective interventions will require a collaborative effort between regulators, law enforcement, and the private sector to mitigate the risks and impacts of crypto crime. By recognising the entrepreneurial aspect of crypto crime, perhaps we can better anticipate and respond to the challenges posed by this ever-evolving threat.

Written by Luke Higgins and Steven Pettigrove

Operation Spincaster: Australia Fights Crypto Scams

The Australian Federal Police (AFP) has stepped up its efforts to combat cryptocurrency scams with the launch of Operation Spincaster, a global initiative aimed at disrupting criminal activities targeting crypto users.

Australia is continuing its war against scams, following the National Anti-Scam Centre's efforts to reduce scams, and the recent overall decline in scam losses, the AFP's initiative is timely.

In collaboration with the blockchain data platform Chainalysis, the AFP has identified over 2,000 compromised crypto wallets belonging to Australians, shedding light on the tactics used by cybercriminals in a scam known as "approval phishing."

Approval phishing is a sophisticated scam technique where criminals trick victims into signing a malicious blockchain transaction. Once the transaction is approved, the attacker gains access to the victim's crypto wallet, allowing them to siphon tokens at will.

This scam has been responsible for stealing over $4 billion in cryptocurrency worldwide since May 2021 and is prevalent in both investment scams and romance scams. Despite the recent drop in scams in Australia, the AFP remains vigilant.

Operation Spincaster has seen participation from digital currency exchanges and public agencies across the US, UK, Canada, Spain, Netherlands, and Australia. In June 2024, the AFP-led Joint Policing Cybercrime Coordination Centre (JPC3) hosted a workshop with Chainalysis, digital currency exchanges, and law enforcement agencies to share intelligence on compromised wallets, train in tracing stolen funds, and discuss real-time scam detection.

AFP Detective Superintendent Tim Stainton emphasised the necessity of a collaborative approach.

> Working together and sharing knowledge with industry, government, and law enforcement partners is crucial.

The operation has received significant support from major digital currency exchanges, including BTC Markets, Binance, Crypto.com, Ebonex, Independent Reserve, OKX, SwyftX, and Wayex. These platforms have committed to identifying Australian victims, providing support, and preventing further victimisation.

Operation Spincaster is a significant step forward in the fight against crypto scams, and with continued collaboration and vigilance, we can protect the community from these growing threats.

Written by Michael Bacina, Steven Pettigrove and Luke Misthos

Ripple rides on as $2B SEC wave ebbs with $125M spray

A United States federal judge has ordered Ripple Labs to pay a $125 million civil penalty for breaching US securities laws. The judgment, issued by Judge Analisa Torres of the US District Court for the Southern District of New York, also

permanently restrains Ripple from violating US securities laws.

The ruling stems from a lawsuit filed by the Securities and Exchange Commission (SEC) in December 2020, alleging that Ripple raised funds through the sale of XRP tokens as unregistered securities. The SEC initially sought up to USD $2 billion in civil penalties and disgorgement, while Ripple argued for a maximum penalty of $10 million.

In July 2023, Judge Torres ruled that XRP is not a security in the context of programmatic sales on exchanges, but that institutional sales did amount to unregistered securities transactions under US law.

Judge Torres found that 1,278 transactions violated Section 5 of the Securities Act. This led to the imposition of a USD $125 million civil penalty, which Ripple is required to pay within 30 days. The judge found that it was not open as a matter of law to order disgorgement in the circumstances.

Despite the substantial fine, Ripple's leadership views the outcome as a positive development. CEO Brad Garlinghouse described the ruling as a "victory for Ripple, the industry, and the rule of law," noting that the penalty was significantly reduced from the SEC's initial demand.

Ripple's chief legal officer, Stuart Alderoty, echoed this sentiment, stating that the company respects the court's decision and is now better positioned to continue its growth.

The ruling also addressed future compliance, with Judge Torres suggesting a reasonable probability of future violations by Ripple. Nonetheless, her Honour noted that Ripple's sales after the SEC complaint may not have breached federal law.

The judgment brings this round of the protracted legal battle between Ripple and the SEC to an end. The SEC is expected to appeal the judge's ruling with respect to the programmatic sales of XRP.

Following the announcement of the ruling, the price of XRP surged by approximately 24%, reflecting investor optimism about Ripple's future prospects.

Highlights of her Honour's reasoning to substantially reduce the civil penalty payable by Ripple are as follows:

- although Ripple's conduct was egregious, the Court found that a first-tier penalty was appropriate for Ripple as there had been no allegations of "fraud, deceit, [or] manipulation," and no conclusively established "deliberate or reckless disregard of a regulatory requirement" [p 14];
- the Court found that the SEC failed to establish that Ripple's failure to register the sales of XRP with the SEC caused substantial losses (or the risk thereof) to investors [p 15]; and

- Ripple did not contest the SEC's contention that its current financial condition did not merit a reduced penalty [p 15].

The SEC contended that Ripple's actions were motivated by profits and to avoid the costs of registration. However, her Honour found that this did not support the corresponding inference that Ripple recklessly disregarded regulatory requirements in making its business decisions.

The Court considered evidence of two conflicting opinions obtained from a US law firm, the latter of which concluded that there was a compelling argument that XRP tokens are not securities. To that end, the case again emphasises the importance of obtaining legal advice before launching crypto asset offerings in an uncertain regulatory environment.

While the ruling imposes a significant penalty on Ripple, it also affirms the company's stance that the XRP token is not inherently a security. The ruling comes however at substantial cost to both sides with Ripple having reportedly spent in excess of $100 million defending the SEC action. Given these costs, and the fact that the action could still drag on to appeals, legislation seems like a relatively cheaper and more efficient means of bringing regulatory clarity to crypto-asset markets.

Written by Luke Higgins and Steven Pettigrove

UK draft bill proposes third category of personal property

On 30 July, the UK Law Commission published a supplementary report and draft Bill which would legislate a third category of personal property, which digital assets such as cryptocurrencies and non-fungible tokens (**NFTs**) could fall into. If taken up by Parliament, the new legislation would pave the way for courts to definitively treat digital assets as personal property, ending a longstanding debate in the UK. The issue of whether digital assets are a type of personal property has repeatedly been argued by litigating parties and discussed in UK courts and beyond. This debate is largely due to attributes of digital currencies that do not neatly fit into either traditional category of personal property, being:

- a chose in possession which is a tangible thing over which the owner has actual enjoyment (e.g. cars or jewelleries), or
- a chose in action which is an intangible thing of which a person lacks present enjoyment, but has a right to sue to recover it (e.g. debts or financial securities).

The Commission, in its June 2023 report, concluded that certain digital assets are capable of being personal property. However, because they are fundamentally different from both traditional categories, the Commission suggested the existence of a "third" category of personal property called "digital objects". The report has been cited by subsequent UK higher court decisions, which has further influenced other common law jurisdictions such as Australia, New Zealand and Singapore.

Extrajudicially, Justice Jackman of the Federal Court has commented that recognition of a third category of property is not necessary for recognition of digital assets as property under Australian law. The judge's comments were endorsed in a recent Federal Court decision regarding a freezing order sought by the Australian Securities and Investment Commission, which found that cryptocurrency is capable of being "property" for the purposes of granting an interlocutory injunction.

The Commission recommends that the law not define the boundaries of this third category, rather that legislation should confirm its existence and keep the boundaries open to accommodate the recognition of new forms of property.

> The draft Bill makes clear that a thing is not prevented from being the object of personal property rights merely because it is neither a thing in action nor a thing in possession. This reflects the trajectory of recent case law, but removes the lingering uncertainty that remains in the absence of a definitive statement from the appellate courts.

If the draft Bill becomes law, it will pave the way for digital assets to be definitively recognised as personal property, which may also influence other common law jurisdictions. The proposed Bill and the Commission's report last month on Decentralised Autonomous Organisations show that the UK Law Commission remains at the forefront of legal reform with respect to digital assets.

Written by Jake Huang and Steven Pettigrove