Piper Alderman

Article Information

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

Blockchain Bites: Money laundering in the metaverse, Terraform settles for USD$4.5bn over Luna implosion, Mitigating settlement risks in Web3, Hydro execs damned over token price manipulation, SEAL launches Legal Defence Fund for Whitehat

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

Money laundering in the metaverse

Financial crime compliance company Elliptic has released the 2024 instalment of its annual report on 'Preventing Financial Crime in Cryptoassets', which sheds light on emerging trends in the use of cryptocurrencies to perpetuate financial crimes, including money laundering, fraud and scams.

Elliptic's report provides a comprehensive overview of a variety of financial crime typologies and potential red flag indicators that can help registered digital currency exchanges and other intermediaries mitigate the use of cryptoassets to perpetuate financial crimes. The report also identifies a number of emerging trends in relation to financial crime involving the use of cryptocurrencies.

Criminals are exploiting artificial intelligence (AI) techniques when perpetrating crimes involving cryptoassets, enabling them to scale their illicit activity.

While cryptocurrencies and AI have generally been viewed as distinct technologies, it appears that both developers and criminals are increasingly exploring the innovative potential of combining these technologies to very different ends. Elliptic's report identifies a marked rise in the use of artificial intelligence techniques in cyber crime. Criminals are using AI tools to make their illicit activity more immune to detection. For instance, some have generated deepfake images to lend authenticity to their scam messages and fabricate identification documents. Large Language Models (LLMs) have also been used to identify exploits in software code, and send scam messages to a greater number of victims.

Stablecoins have featured increasingly in crypto financial crime typologies.

Stablecoins enjoy greater price stability compared to other cryptoassets due to being pegged to traditional assets. This makes them an effective on-and-off ramp for threat actors to convert illicit fiat currencies into volatile cryptoassets like Bitcoin, often on non-compliant exchanges. From this point, they can sell those crypto assets and get 'clean' fiat currency back, concealing its illicit origin.

The red flag indicators associated with stablecoin-enabled laundering include: customers suddenly exchanging large volumes of funds for stablecoins with no clear explanation, and the use of exchanges or brokers that do not observe anti-money laundering and counter-terrorism financing (A**ML/CTF**) requirements.

As an example, the US Department of Justice seized $9 million worth of Tether/USDT in November 2023. This crypto had been bought using money stolen from victims of romance scams, using the 'chain-hopping' technique of swapping the fiat currency for a variety of cryptoassets. Later, a further $225 million worth of USDT was seized, with Tether cooperating with US law enforcement.

In January 2024, the United Nations Office on Drugs and Crime reported that organised criminal groups in Asia have been making increased use of the stablecoin USDT on the TRON blockchain to launder funds. Law enforcement reports from China and the US have also highlighted the prominence of stablecoins like Tether in the world of illegal online gambling and narcotics trafficking.

Cryptoasset exchanges located in high risk jurisdictions continue to offer an important lifeline to criminal actors seeking to convert funds from crypto into fiat currencies.

High-risk jurisdictions refer to those which are subject to sanctions and embargoes, on FATF's list of High Risk and Non-Cooperative Jurisdictions, and/or poor AML/CTF regulations. Exchanges located in these jurisdictions frequently have opaque ownership structures and no real KYC (**know your customer**) procedures in place, facilitating broader illicit activity involving cryptoassets.

Ransomware attackers and other cybercriminals continue to leverage elaborate money laundering schemes, involving privacy coins, cryptocurrency mixers, cross-chain services, and "peeling-chain" techniques.

Cryptocurrency mixing services pool illicit-origin cryptocurrencies together with others to obfuscate the trail back to the original source. "Peeling-chain" refers to the sending of funds through multiple intermediary wallets before reaching their final destination, which can serve to obfuscate their (illicit) source and destination. Cross-chain services allow movement between one blockchain and another.

Each of these methods shares the same objective of increasing the complexity of the chain of transactions from illicit funds to clean funds, to enhance the anonymity with which cryptoassets are already associated.

Money laundering in the metaverse

Metaverse platforms like the Sandbox and Decentraland offer users the ability to enter an immersive world and engage in an increasingly rich variety of experiences using avatars. Users can buy land, wearables, and other digital goods using ERC-20 and non-fungible tokens or even access DeFi protocols like lending platforms.

Unfortunately, according to Elliptic, enterprising criminals are also setting up shop in the metaverse. While instances of metaverse-related crime remain "relatively small", Elliptic identifies the metaverse as an emerging area for money laundering. Potential techniques including use of phony NFTs, theft of or ransomware attacks on virtual goods, drug dealing through illegal storefronts and terrorism financing.

The Elliptic report highlights the ever evolving threat of financial crime with new developments in technology. Ironically, the nature of this threat is revealed by the very transparency of the blockchain which criminals seek to exploit. Digital currency exchanges should continue to keep these typologies under review, consider them as part of their ongoing AML/CTF risk assessment and ensure that their AML/CTF program has systems and process in place to address these emerging threats.

Written by Michael Bacina, Steven Pettigrove and Anson Lee

Terraform settles for USD$4.5bn over Luna implosion

Terraform Labs and its former CEO Do Kwon have agreed to pay USD $4.47bn to settle civil charges brought by the US Securities and Exchange Commission (**SEC**). Terraform was the developer behind the $40bn meltdown of the TerraUSD (**UST**) "stablecoin" in 2022, setting off several subsequent collapses and a prolonged "crypto winter".

According to court documents filed on 12 June 2024, the settlement has been approved by District Court Judge Jed Rakoff of the Southern District of New York. The steep penalty is slightly lower than the SEC's first settlement offer of $5.3 billion in fines, but much higher than a virtual slap on the wrist. Kwon must pay at least USD$204,320,196 out of his own pocket for distribution to harmed investors.

Despite the legal settlement, the battle between the US and South Korea for Kwon's extradition continues, with the Montenegro Supreme Court considering conflicting requests from Kwon's home country and the US on criminal charges including fraud and market manipulation. Remarkably, Kwon remains on bail in Montenegro despite being convicted on charges of using a false passport to attempt to flee the European country for Costa Rica.

The agreement comes after a jury handed down a verdict in April that the collapsed stablecoin operator and its former CEO were liable for securities fraud by misleading investors, which led to billions of dollars in losses. Central to SEC's civil case was that Kwon and Terraform Labs had deceived investors and consumers about the nature of the algorithm that pegged UST to the US dollar. The SEC alleged that Do Kwon implied to the public that the algorithm underpinning the peg operated independently of human interference.

Some commentators have argued that the collapse of Terra/Luna and TUSD was attributable to a "complex phenomenon that happened across multiple chains and assets", rather than concentrated market manipulation by a third party. However, the jury determined that the claim that the algorithm was immune from market manipulation (i.e. human interference) was fraudulent on the part of Kwon and Terraform Labs.

SEC Chair Gary Gensler stated in a Thursday press release following the settlement,

This case affirms what court after court has said: The economic realities of a product — not the labels, the spin, or the hype — determine whether it is a security under the securities laws.

Before the settlement was approved, lawyers for the SEC also filed a letter saying that:

the proposed judgment will send an unmistakable deterrent message to not only those who engage in brazen misconduct, but also to all those who seek to evade the requirements of the federal securities laws by crafting new standards of behavior for crypto assets that fall under the purview of the federal securities laws.

Terraform Labs is currently in Chapter 11 bankruptcy protection and, according to current CEO Chris Amani's trial testimony, has approximately $150 million in assets on hand. It is currently unclear how the company will pay the hefty fines. While the settlement is another milestone in the cleanup from the heady COVID crypto boom, Kwon continues to await final judgment for his role in the Luna fiasco.

Written by Jake Huang and Steven Pettigrove

New market paradigms: mitigating settlement risks in Web3

As the use of public blockchains in financial transactions continues to grow, it is crucial to address the settlement risks associated with these decentralised systems. Traditional financial markets benefit from the assurance of central bank money and government-backed insurance schemes, which provide a sense of security and trust. However, some believe that public blockchains lack these safety nets, leading to uncertainty and potential principal risk for market participants. Understanding and mitigating these risks is essential for the future of decentralised finance (**DeFi**) and the broader adoption of blockchain technology.

Leading Web3 venture capital, Paradigm, has issued a report written by Natasha Vasan which dives into the intricacies of settlement risks in hybrid transactions—those involving both public and private blockchains or a mix of on-chain and off-chain components. The paper explores various technical, legal, and market-based solutions to enhance settlement finality and reduce risks, making DeFi a more reliable and attractive option for financial institutions and individual traders alike.

Key takeaways from the report:

1. **Understanding Settlement Risks**: Despite immutability being one of the selling points of blockchain technology, public blockchains like Ethereum do not guarantee that transactions are final and irreversible as central banks do in traditional finance. This means there is a risk that transactions could be undone or disputed, especially if someone gains control of the network (although it is worth noting that this is unlikely for a mainstream blockchain such as Ethereum). Without a central authority to ensure transaction finality, the report states this creates uncertainty and potential financial risk for users. Unlike traditional financial systems, where government guarantees and insurance schemes protect consumers within the system, DeFi operates without these safety nets. This increases the need for proper risk management strategies.
2. **Decentralised Settlement Insurance**: Implementing decentralised settlement insurance could provide a safety net for users. This mechanism would use incidental funds that are burnt by blockchains as part of its mechanism of action (i.e., slashed funds) to compensate victims of settlement issues or disruptions. This proposed insurance system could operate similarly to traditional depository insurance but would be managed through decentralised governance mechanisms, adding extra layers of security and trust to the particular blockchain ecosystem.
3. **Central Counterparty for Hybrid Transactions**: Exploring the creation of "decentralised central counterparties" (CCPs) can help mitigate credit risks in hybrid transactions. These CCPs could pool resources and risk exposure, functioning similarly to traditional financial institutions like the Depository Trust Company (DTC). A decentralised CCP could manage settlement risks and provide compensation for victims of transaction issues, thereby reducing the principal risk for users and enhancing the reliability of hybrid transactions (i.e., part blockchain and part tradfi transactions).

4. **Standardised Legal Contracts**: Adopting standardised contractual frameworks, akin to the ISDA Master Agreement for OTC derivatives, could provide consistency and legal certainty for hybrid transactions. These contracts would define the moment of settlement finality, specify remedies in the case of settlement disruptions, and integrate contract logic into self-executing smart contracts, thereby reducing the risks associated with hybrid transactions and promoting greater trust and adoption in DeFi.
5. **Public-Private Blockchain Communication**: Developing solutions to enable seamless communication between public and private blockchains is essential as we move towards an increasingly tokenised future. This includes addressing the unique risks associated with transactions involving regulated financial institutions or national governments. Collaborative efforts, such as the SWIFT and Chainlink Cross-Chain Interoperability Protocol (CCIP) project, are exploring ways to ensure regulatory compliance and settlement finality in public-private blockchain communications.
6. **Legal Interventions and Industry Self-Regulation**: External legal interventions may be necessary to ensure institutional adoption and to promote trust in public blockchains as a settlement option for financial transactions. Defining a legally recognised moment of settlement finality and providing a legal basis for recourse in case of disruptions is a useful starting point. Through the development of baseline standards and best practices, industry self-regulation can complement legal mandates and enhance interoperability and trust across different blockchains.
7. **Managing Operational Risks**: Addressing operational risks, such as settlement delays due to network congestion or inflated gas fees is crucial for the smooth execution of hybrid transactions. Placing certain legal requirements on off-chain agents involved in hybrid transactions, such as ensuring timely conclusion of transfers on public blockchains, can help mitigate these risks and enhance the overall efficiency and reliability of DeFi.

As the use of blockchain technology in financial markets increases, Paradigm's report highlights the importance of understanding the underlying technology and the ability to craft unique solutions to address market risks. Adopting strategies to address these risks will be important as mainstream institutions increasingly enter these markets and expect a level of assurance on par with traditional markets. Proactively addressing critical settlement risks may be the difference in ushering in the future of markets.

Written by Luke Higgins and Steven Pettigrove

Hydro execs damned over token price manipulation

Two executives of Hydro Technology – the company behind the cryptocurrency HYDRO – have been sentenced to jail for defrauding investors by manipulating the price of the token. Michael Kane, the CEO of Hydro Technology, was sentenced to 3 years and 9 months, while Shane Hampton, the company's Head of Financial Engineering (being his official title), was sentenced to 2 years and 11 months.

The US Department of Justice (**DOJ**) brought the charges against the two Hydro executives, alleging that they orchestrated a scheme to manipulate the price of HYDRO. It was alleged that, from October 2018 to April 2019, the two executives and their co-conspirators engaged Moonwalkers Trading Limited to use an automated trading system, or "bot" to execute fraudulent trades.

In this process, they carried out approximately $7 million in wash trades and over $300 million in spoof trades on a cryptocurrency exchange in the US – flooding the market with fake and fraudulent orders. These trades aimed to create a misleading market for HYDRO, enticing retail investors to purchase the cryptocurrency, which allowed the accused and their associates to sell their holdings for over $1.5 million.

Kane pleaded guilty in November 2023 to several criminal counts including conspiracy to commit securities price manipulation, conspiracy to commit wire fraud and wire fraud. As for Hampton, in February 2024, a federal jury in the Southern District of Florida found him guilty on counts of securities prices manipulation and conspiracy to commit wire fraud.

According to the DOJ, the case represents the first time a jury in a federal criminal trial found that:

> a cryptocurrency was a security and that manipulating cryptocurrency prices was securities fraud.

The DOJ added:

> The Criminal Division will not hesitate to use all tools at its disposal—including the federal securities

laws—to protect the integrity of cryptocurrency markets.

Last year, Hydrogen Technology was fined just under USD$2.8 million and Kane USD$260,206 by the US District Court of the Southern District of New York for violating securities law in a case brought by the Securities and Exchange Commission.

This case and other similar cases, such as the complaints involving the Mango Markets exploit, show that US regulators are going beyond using general fraud charges to prosecute market misconduct in relation to cryptocurrencies, increasingly pursuing securities fraud and market manipulation charges, even if the latter requires satisfying the threshold question of the underlying cryptocurrency being a security.

Written by J Huang and S Pettigrove

SEAL launches Legal Defence Fund for Whitehats

The Security Alliance (**SEAL**), the coalition behind a number of leading security initiatives for the Web3 ecosystem, has launched its latest initiative, the first Legal Defence Fund for Whitehats hackers in Web3. The Fund is intended to provide financial assistance to good faith security researchers who face legal action in connection with research activity. The fund has been launched in collaboration with the Security Research Legal Defence Fund (the **SRLDF**).

Whitehats are security researchers who engage in ethical hacking in order to identify and secure computer systems. Security researches who identify or expose vulnerabilities in software can face legal threats or prosecution over their work, including allegations of unlawfully accessing computer systems or misappropriation of data or assets. Since 2022, the official policy of the US Government is not to prosecute “good faith” security researchers. However, this does not mean that researchers will not face legal threats from the company which published the software or users, or allegations which call their good faith into question. Legal threats can have a chilling effect on good faith security research.

SEAL’s Legal Defence Fund complements its broader toolkit for Web3 security researches.

The Whitehat Safe Harbour Agreement is intended to incentivize Whitehat hackers to rescue funds by offering agreed rewards and pre-emptive legal releases from the protocol and its users, and reducing the risk of criminal prosecution. The new Legal Defence Fund will assist eligible Whitehats who use the Whitehat Safe Harbor Agreement in good faith to protect the crypto ecosystem.

Whitehats that face legal threats or lawsuits due to good faith security research can apply for grants from the Security Research Legal Defense Fund to offset the cost of legal representation. The eligibility criteria are set out on the Fund's website. The SEAL Whitehat Safe Harbor Agreement is now included in the grants that can be made under the SRLDF.

As part of this initiative, SEAL is also making an initial donation to the fund thanks to its donors including Paradigm, a16z, Electric Capital, Framework, Dragonfly, Paperclip, E-girl Capital, the Ethereum Foundation, and the Filecoin Foundation.

The Security Alliance is the coalition behind several other security initiatives, including the Whitehat Safe Harbor, SEAL Wargames, which allows developer teams to simulate security incident scenarios, and the SEAL 911 Emergency Hotline, which enables users, developers and security researches who need access to urgent security advice, help with disclosing a critical vulnerability, or to connect with a team of carefully vetted expert volunteers. SEAL 911 has helped disrupt, intercept, and remediate several hacks, recovering over USD 50 million in crypto-assets. SEAL has also built the world's first crypto ISAC or information sharing and analysis centre to enhance real time sharing of threat intelligence, and combat cyber hacks and financial crime in Web3.

Written by Michael Bacina and Steven Pettigrove