## Article Information

Authors: Michael Bacina, Steven Pettigrove, Jade McGlynn, Jordan Markezic, Luke Misthos
Service: Blockchain, FinTech
Sector: Financial Services, IT & Telecommunications

---

# Blockchain Bites: US Treasury releases responsible crypto regulation framework, US Fed Vice Chair pushes for crypto reform, Shanghai's new metaverse development fund, Celsius plunges into bankruptcy, NFTs stolen in phishing attack

***Michael Bacina, Steven Pettigrove, Jade McGlynn, 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.***

---

**U.S Treasury releases framework for responsible development of digital asset regulation**

The United States Treasury has issued a framework on crypto-assets designed to assist US government agencies to work with foreign regulators.

This globally focused framework follows an executive order on digital assets made by President Joe Biden back in March, which focused on the coordination and consolidation of various government agencies under a national policy. The Treasury's recent framework order appears to be an internationalisation of the governments efforts to ensure the responsible development of digital assets under the executive order. According to the Treasury the framework aims to:

> *ensure that, with respect to the development of digital assets, America's core democratic values are respected; consumers, investors, and businesses are protected; appropriate global financial system connectivity and platform and architecture interoperability are preserved; and the safety and soundness of the global financial system and international monetary system are maintained.*

The government department cites that due to the risks posed to investors by the uneven regulation, supervision, and compliance across jurisdictions international cooperation among public authorities, the private sector, and other stakeholders is critical. This could be seen as a dig at the highly centralised Chinese central bank digital currency.

To elaborate on the nature of the issue, the report continues:

> *Inadequate anti-money laundering and combating the financing of terrorism (AML/CFT) regulation, supervision, and enforcement by other countries challenges the ability of the United States to investigate illicit digital asset transaction flows that frequently jump overseas, as is often the case in ransomware payments and other cybercrime-related money laundering.*

To promote these aims of international co-ordination and cooperation the Treasury will continue to engage with international policy makers at G7 on topical matters related to digital assets payments, including the implications of: new technologies on the international monetary system, the creation and movement of money in public and private sectors and central bank digital currencies, it says.

In addition, the country will work with G20 members to: reduce the challenges presented by the use of digital assets for cross-boarder payments and financial stability due to digital assets, push for better digital asset regulations, and speak

over any remaining macro-financial challenges.

It remains to be seen if the bold statement of "inadequate anti-money laundering" is evidenced by the data, as the regular Chainalysis Crypto Crime reports continue to show that crypto-assets are not used in illicit activity in a substantial proportion relative to total transaction volume (and well below the levels of illicit use of cash).

**US Fed's Vice Chair pushes for crypto regulation**

Speaking at the recent Bank of England Conference, the Vice Chair of the Federal Reserve, Lael Brainard, has urged crypto regulation as a necessary step to combat weighty risks such as fire sales, deleveraging and contagion in the crypto markets, and to promote competition, efficiency and speed.

The news comes amid a recent number of collapses in the crypto industry following the Terra/Luna meltdown, Three Arrows liquidation and Celsius' freezing transactions as the largest casualties of the crypto winter so far. Despite significant losses occurring, Ms. Brainard says the crypto system is not yet so interconnected with traditional finance to be considered a systemic threat.

Although she did not disclose much relating to potential policy, Ms. Brainard did confirm the future of crypto involves regulation:

> *Future financial resilience will be greatly enhanced if we ensure the regulatory perimeter encompasses the crypto financial system and reflects the principle of same risk, same disclosure, same regulatory outcome.*

While praising the benefits of crypto and digital assets generally, the Vice Chair sought to draw a distinction as to whether lower costs were delivered by genuine innovation, or cost savings by non-compliance with existing laws. This is a curious point to make, given that crypto businesses have been clamouring for clear paths to regulation which can be complied with using decentralised technology.

Crypto has headlined US regulatory conversation in the finance space for the past few months, most recently with the Securities Exchange Commission (**SEC**) confirming bitcoin as a commodity and inferring ether is a security for regulatory purposes.

As the US continues to traverse the crypto winter, those in charge of inciting and enacting policy, such as Ms. Brainard, seem to believe it is a global process instead of something that must be tackled by each individual country:

> *Due to the cross-sectoral and cross-border scope of crypto platforms, exchanges, and activities, it is important that regulators work together domestically and internationally to maintain a stable financial system and address regulatory evasion.*

This is spot on, as highly mobile crypto businesses with young staff will move to jurisdictions which have supportive frameworks for regulation, and rely on the borderless nature of blockchain networks to deliver their innovation. This poses a significant challenge to traditional financial services regulation, which has traditionally enjoyed a clear enforcement path and a gatekeeper model to ensure compliance. Designing laws which must balance incentives and costs more carefully than ever before is a difficult task.

**Shanghai Govt launches $1.5B Metaverse Development Fund**

The Shanghai Government has announced the launch of a US$1.5 billion Metaverse Development Fund as part of measures designed to boost its post-pandemic economy recovery.

According to Hong Kong-based media outlet, the South China Morning Post, the fund will help Shanghai foster 10 "leading" companies, and 100 small firms which could launch at least 100 "benchmarking products and services". Head of Shanghai's Economy and Information Technology Committee, Wu Jincheng, commented that:

> *The Metaverse will drive the transformation and upgrading of various industries in the real economy.*

The Shanghai Government is also backing investments in low-carbon energy projects and small terminal technology. Jincheng added that there was "huge market value" in the three sectors, which are estimated to be worth approximately

US$224 billion by 2025. The Shanghai Government has also identified the metaverse as one of its four 'frontiers for exploration' in its five year plan published in December 2021.

Shanghai's announcement follows a tumultuous period for Web3 technologies in China. In September 2021, the Central Government launched a crackdown on trading cryptocurrencies and Bitcoin mining. In recent times, State-run media outlets and regulators, such as the China Banking and Insurance Regulatory Commission, have issued several warnings with respect to illegal fundraising schemes associated with the metaverse and various cryptocurrencies.

Notwithstanding these developments, a consortium of Chinese companies with links to the Government has reportedly been building a Blockchain-based Service Network (**BSN**) targeted at companies offering computing infrastructure services. China is also pushing ahead with the development of its CBDC, the eCNY, and has re-emerged as a leading Bitcoin mining center trailing only the United States.

Mirroring its approach to the early days of the Internet, China's apparent strategy is to seek to secure the economic and technology benefits associated with blockchain and Web3 technologies while maintaining control over markets and data. It remains to be seen how this will play out in the Web3 era with its focus on the benefits of decentralisation and permissionless systems.

**Celsius files for bankruptcy, under investigation**

Embattled crypto lender, Celsius Network (**Celsius**), has filed for bankruptcy in New York. The filing follows a statement issued by the US State of Vermont's Department of Finance Regulation (**DFR**) earlier this week labelling the firm 'deeply insolvent'.

According to Reuters, Celsius estimated its assets and liabilities as between US$1 billion to US$10 billion and has US$167 million in cash on hand. It has more than 100,000 creditors.

In its statement on Tuesday, the DFR stated that Celsius:

> *deployed customer assets in a variety of risky and illiquid investments, trading, and lending activities. Celsius compounded these risks by using customer assets as collateral for additional borrowing to pursue leveraged investment strategies. Additionally, some of the assets held by Celsius are illiquid…*

In June, Celsius suspended withdrawals, cut its workforce and engaged restructuring experts following the downturn in crypto markets.

On Wednesday, it was reported that Celsius had paid off its debt on the DeFi protocol, Aave, which freed up US$26 million in tokens in its restructuring strategy. Celsius also moved US$418 million in staked ether (stETH) to an unknown wallet. Last week, Celsius paid off a loan on Maker, another DeFi protocol, releasing US$440m in collateral. The pay-offs sparked controversy in some quarters that Celsius was apparently paying third party loans while customer withdrawals remained suspended. However, the pay-offs were presumably intended to release more funds from overcollateralized loans to repay creditors.

Meanwhile, Celsius is reportedly under investigation in a number of US States along with other failed crypto-lenders. In its statement, the DFR alleged that Celsius engaged in unregistered securities offerings by offering cryptocurrency interest accounts to retail investors. The DFR also noted that Celsius lacked a money transmitter license, meaning that Celsius operated largely independent of regulatory oversight.

Celsius is also currently subject to proceedings in the New York State Supreme Court brought by KeyFi for breach of contract and fraudulent misrepresentation. The proceedings commenced by KeyFi allege Celsius had been:

> *leveraging Celsius' customer deposits to manipulate crypto-asset markets, had failed to institute basic accounting controls which endangered those same deposits, and had failed to carry through on promises that induced the Plaintiff to undertake various trading strategies.*

The lawsuit also levels allegations of gross mismanagement at Celsius and that Celsius become a Ponzi scheme after suffering heavy losses in early 2021.

Despite today's filing, the ramifications of Celsius' collapse are likely to reverberate for some time to come.

**NFTs stolen in Phishing Attack on Uniswap v3**

A group of hackers has pulled off a major phishing scam on a Uniswap v3 liquidity pool, making off with NFTs worth roughly US$3.56m in ETH. The hackers impersonated Uniswap's website and deceived liquidity providers into signing malicious transactions.

Positions in Uniswap v3 liquidity pools are represented as NFTs which liquidity providers can use as collateral for loans paid out in stablecoins and other assets.

On chain data tied to the scammer's account reveals that all but 70 ETH of the amount stolen has already been transferred through a cryptocurrency mixing service, Tornado Cash, in an attempt to obscure the destination of the stolen digital assets.

The hack follows not long after a much wider attack against Uniswap users. According to MetaMask security analyst Harry Denley, a malicious actor targeted over 73,000 wallet addresses by sending them a token under the guise of a UNI airdop, hoping to steal the credentials of those who logged in to inspect the free token.

Following the latest incident, Hayden Adams, founder of the Uniswap protocol, confirmed in a tweet that the loss of NFTs was the result of a phishing attack which was:

> *totally separate from the protocol (and) a good reminder to protect yourself from phishing and not click on malicious links.*

These incidents demonstrate the increasing sophistication of phishing scams where bad actors seek to deceive users by impersonating well known websites and offering seemingly plausible inducements to gain access to users' accounts.