Article Information

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

Blockchain Bites: Australia sanctions Zservers in coordinated ransomware sanctions, Australia passes sweeping Scam Prevention Act, HK Giants join forces on HK dollar-backed stablecoin

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.

Australia sanctions Zservers in coordinated ransomware sanctions

On February 11, 2025, the United States Department of the Treasury's Office of Foreign Assets Control (OFAC), the United Kingdom's Foreign Commonwealth and Development Office (FCDO), and Australia's Department of Foreign Affairs and Trade (DFAT) jointly sanctioned Zservers, a Russian-based bulletproof hosting (BPH) provider, for its role in facilitating ransomware attacks by the LockBit gang. LockBit has been one of the most active ransomware groups in recent years, targeting businesses, hospitals, and government entities worldwide. In 2022, LockBit was the most deployed ransomware variant across the globe.

The sanctions and their scope

Zservers and its operators have been added to sanctions lists in the US, UK, and Australia. The US designation includes two Russian nationals – Aleksandr Sergeyeevich Bolshakov and Alexander Igorevich Mishin – as well as three cryptocurrency addresses tied to Zservers. The UK also sanctioned four additional employees and a UK-based front company, XHOST Internet Solutions LP.

Australia has listed Zservers as well as the owners and a number of employees of the company, along with XHOST Internet Solutions LP. Certain owners and employees are known only by pseudonyms. Australia does not specifically list wallet addresses in its sanctions list, although dealings in a sanctioned person's crypto-assets will be covered by sanctions and subject to freezing and seizure.

The UK government described Zservers as "a key component of the Russian cybercrime supply chain," noting its role in providing essential infrastructure for ransomware attacks, including those targeting hospitals.

Australia's DFAT linked the action to its first cybercrime related sanctions issued last year against Aleksandr Ermakov over the Medibank Private cyberattack. The Zserver's action is Australia's first cyber sanction against a business and the first sanction for the provision of services or infrastructure used to engage in cybercrime.

How does Zservers work?

Zservers provides anonymous hosting services and operates data centers across various countries, such as Russia, Bulgaria, the Netherlands, the US, and Finland. While BPH services can be used for legitimate purposes, they are also attractive to cybercriminals due to their lenient policies on hosted content.

Zservers advertises its services openly, offering server administration, equipment rental, and custom configurations. This accessibility has made it a preferred choice for illicit actors seeking to conduct ransomware operations while evading law enforcement scrutiny.

Blockchain analysis firm Chainalysis has identified at least USD $5.2 million in on-chain transactions linked to Zservers, with direct connections to multiple ransomware affiliates beyond LockBit. These funds have been funnelled through sanctioned exchange Garantex and various decentralised and anonymous crypto services, highlighting the financial networks used to facilitate ransomware operations.

Conclusion

The coordinated sanctions against Zservers reinforce government efforts to step up action on ransomware and the importance of international collaboration in combating cybercrime. Last year's law enforcement action against LockBit disrupted its operations, and this latest move continues efforts to dismantle the infrastructure supporting ransomware groups.

While cybercriminal networks constantly adapt, targeting service providers like Zservers makes it more difficult for them to operate. By disrupting the financial and technical infrastructure behind ransomware, governments are increasing the cost and risk for those involved in these illicit activities.

Written by Steven Pettigrove and Luke Higgins

Australia passes sweeping Scam Prevention Act

Australia's Federal Parliament has passed the Scams Prevention Framework Act 2025, marking a major step in the country's fight against digital fraud. The new legislation imposes sector-specific obligations on designated sectors to detect, prevent, and disrupt scams impacting Australian consumers and small businesses. The legislation will take effect immediately upon Royal Assent subject to further Ministerial designations and codes.

The Scams Prevention Framework (**SPF**) is expected to impose additional regulatory oversight of and mandates on key sectors including banks, telcos, and digital platforms to play a proactive role in combating scams. The SPF is likely to be expanded to additional sectors (including the cryptocurrency sector) over time.

With its passage, the SPF introduces a multi-layered compliance structure, requiring businesses to:

- Prevent scams through internal governance policies.
- Detect fraudulent activity with actionable intelligence.
- Disrupt scams by blocking suspicious transactions and communications.
- Report scams to regulators and affected consumers.
- Respond effectively to consumer complaints and participate in external dispute resolution schemes.

The SPF primarily targets highly regulated sectors, which include banks, telecommunications providers, and digital platforms. These businesses must comply with new code-based obligations, which the Minister may introduce to address specific scam-related risks.

Failure to comply with the SPF may result in civil penalties, with regulators such as the ACCC and ASIC enforcing compliance.

Unlike previous approaches that largely relied on post-fraud enforcement, the SPF mandates upstream protections—forcing businesses to take preventative measures before scams occur. This shifts accountability onto service providers who facilitate digital transactions and communications.

The passing of the Scams Prevention Framework Act 2025 means affected businesses will need to review their compliance obligations and prepare for increased scrutiny. Expect further regulatory guidance, industry codes, and enforcement actions as the framework takes effect.

Written by Steven Pettigrove and Luke Misthos

HK Giants join forces on HK dollar backed-stablecoin

In a groundbreaking move, Standard Chartered Bank Hong Kong, Animoca Brands, and HKT have announced the formation of a joint venture to issue Hong Kong's first regulated HKD-backed stablecoin. This initiative marks a significant step in Hong Kong's ambition to cement its place as Asia's crypto hub, and as a global leader in regulated crypto assets.

The joint venture will apply for a license from the Hong Kong Monetary Authority (**HKMA**) under its new regulatory framework for stablecoin issuers. A bill issued in December is currently under review by the Legislative Council. This collaboration brings together three key players from Hong Kong's banking, Web3, and telecommunications sectors, each contributing their unique expertise to the project.

Standard Chartered, with its experience in stablecoin projects worldwide, will provide bank-grade global infrastructure and rigorous governance standards to secure compliance with regulatory obligations.

Animoca Brands, a global leader in the Web3 space, will leverage its industry expertise and extensive network to integrate the stablecoin into the broader digital economy. This includes adoption across metaverse applications, gaming, and decentralized finance (i.e. DeFi), thereby enabling innovative use cases and driving long-term growth.

HKT, a pioneer in technology, media, and telecommunications, will contribute its mobile wallet expertise to enhance real-world payment adoption. This will facilitate both domestic and cross-border transactions, providing greater benefits to consumers and merchants alike.

Bill Winters, Group Chief Executive of Standard Chartered, emphasized the importance of digital assets in the evolving financial landscape,

Digital assets are here to stay, and the development of different forms of tokenized money is integral to the advancement of this industry. We are introducing solutions and instruments that service this market and meet the growing client demand

The joint venture's licensing application with the HKMA is expected to progress in the coming months. Alongside the city's progress in regulated tokenisation, crypto asset trading, and digital bond issuance, the latest announcement represents broad institutional support for Hong Kong's ambitions as a global crypto asset leader.

Written by Jake Huang and Steven Pettigrove