Article Information

Authors: Jade McGlynn, Michael Bacina, Tudor Filaret
Service: Blockchain, FinTech
Sector: Financial Services, IT & Telecommunications

Blockchain Bites: $8M stolen from Aussie Hedge fund, China pushing CBDCs, Gaming Blockchain Boost, Hong Kong digital exchange crackdown

Michael Bacina, Tudor Filaret, and Jade McGlynn of the Piper Alderman Blockchain Group bring you the latest legal, regulatory and project updates in Blockchain and Digital Law.

Fake zoom invite leads to $8m being stolen from Aussie Hedge Fund

On Monday, the Australian Financial Review reported that Levitas Capital, a Sydney-based hedge find, was the target of a fake Zoom invite that was opened by one of the fund's co founders Michael Fagan or Michael Brookes. After sending the fake Zoom invite on 10 September 2020, the hacker was able to install a malicious software program that gave them access to the funds email system. Amongst other things, the hackers used to send off fake invoices and approve unauthorised transactions.

Between 10 to 23 September 2020, the hackers siphoned off money in a number of ways, including:

1. a payment of a fraudulent invoice for $1.2 million to an Australian company;
2. a payment of $2.5 million to the Bank of China in Hong Kong (the payment was eventually stopped by one of the co-founders);
3. a payment of $5 million to East Grand Trading at the United Overseas Bank in Singapore (the payment was eventually stopped by one of the co-founders);
4. a withdrawal of $240,000 via at an ANZ branch in Bankstown
5. a further withdrawal of two bank cheques of equal value of $240,000; and
6. a further 64 withdrawals from the ANZ account totalling $300,000.

One of the co-founders, Michael Fagan, commented:

There were so many red flags which should have been spotted

Michael Fagan's comments that the red flags should have been spotted are correct. Basic training on awareness on brand impersonation and phishing would have prevented these issues from happening in the first place. This is not the first time an AFS licensee has had a similar mishap. Earlier this year, a hacker gained remote access to an AFS licensee, RI Advice Group, and spent more than 155 hours logged onto the server. The hacker did so simply through "brute-force" – attempting

to log on using an employee login 27,814 times unsuccessfully from 10 different countries. It is astounding that AFS licensees cybersecurity systems were not adequately prepared for such an attack.

Levitas Capital was forced to close following its September attack after one of its largest institutional clients, Australian Catholic Super, withdrew its money out of concerns triggered by the cyberattack. Prior to the attack, Levitas Capital has $75 million under management.

We are yet to see whether ASIC will commence proceedings against Levitas Capital. Earlier this year in August, ASIC commenced proceedings for pecuniary orders against RI Advice Group following the 'brute-force' cybersecurity attack.

Getting paid with bitcoin: BitPay launches a new payroll service

Bitcoin payments provider BitPay recently announced a new service: "BitPay Send", a neat new way for businesses to pay employees, contractors, customers and vendors all at once with cryptocurrency.

Bitpay describes the new service as "ideal for companies looking for a fast, efficient, and secure way to send mass payouts anywhere in the world, on any day of the week, and at any time".

As one of the oldest and most respected bitcoin companies in the world, Bitpay has already raised $72.5 million in investment. Considering BitPay Send's so-far positive reception, who's to say what's next as they continue working to transform how businesses and people send, receive, and store money around the world.

No word yet on whether tax reporting compliant with Australian laws applies to the use of Bitpay's payroll service. Currently Australia has some services like Get Paid In Bitcoin of which the level of uptake is unclear.

China challenges G20 to charge on with CBDC co-operation

Last week, China's President Xi Jinping urged G20 meeting attendees to support digital currency and advised that member countries should support the growth and implementation of their own central bank digital currencies (CBDCs) if they aim to stabilize and restore economic growth.

Unlike Australia, the Chinese government feels the case for a retail CBDC is strong as a means to stimulate the economy. When you consider recent predictions that China's planned digital yuan will account for 15% of total consumption payments in 10 years, it's clear to see why the government would want to ensure stability in a new form of digital money.

Game on! Regulatory relief granted for gaming token VCOIN by US SEC

The SEC Division of Corporate Finance recently granted a welcome 'no action position' for Delaware Corporation IMVU Inc in relation to an in-game blockchain currency. This published position allows IMVU's digital asset/stablecoin VCOIN to be sold on their virtual world platform without registering the offer and sale of a security under the *Securities Act of 1993* and *Securities Exchange Act of 1934*. Put another way, it enables the VCOIN to be used without fear of SEC prosecution.

VCOIN is a tangible example of how an appropriately structured digital asset can use the power of blockchain without falling within the definition of a security. This is not a binding ruling for ASIC but may help provide some indicia for local blockchain developers seeking to utilise tokens in their products.

Chainalysis code to catch and keep captive seized digital assets

Recently, blockchain analysis firm Chainalysis announced it was launching a program designed to manage and store cryptocurrency seized during criminal investigations.

Coining it an "asset realisation program", Chainalysis explained that its new software will empower law enforcement agencies to handle, hold, and track seized assets, including cryptocurrencies such as Bitcoin (**BTC**), Ethereum (**ETH**), and other "alt coins".

In its 12 November announcement, the company whittled down its value proposition in as many words as:

> When law enforcement discovers and investigates illicit cryptocurrency assets, they need to seize and store them until they can be legally forfeited. As such, government agencies and insolvency practitioners — licensed professionals who advise on insolvency matters — need a safe way to track, store, and ultimately

sell seized cryptocurrency assets for fiat currency.

Right now there seems no greater time for Chainalysis to champion its new program, seen in the US government's announcement they had seized BTC worth $1 billion in the largest confiscation of digital coins recorded to date.

Chainalysis was involved in that investigation as well as the recent Welcome to Video take down, works with the US agency FinCen to investigate financial crimes, and has been involved in other recent probes into North Korean hacking activities and terrorism financing.

Hong Kong set to introduce robust digital currency exchange regulations

Taking yet another step away from mainland China and its aggressive posture towards digital currency trading platforms, Hong Kong has announced an expansion of monitoring and overseeing the activities of digital currency exchanges.

Hong Kong has historically supported digital currency exchanges businesses, welcoming exchanges into the provincial sandbox as long as they adhere to laid down rules and regulations. In doing so, the Securities and Futures Commission (**SFC**) had previously put in place an 'opt in' regulatory framework for digital currency trading platforms which allowed platforms that didn't deal in securities to be exempt from these laws.

In efforts to improve protections for digital currency exchanges users, the SFC has recently announced new plans to regulate all digital currency exchanges regardless of whether they list "security tokens". According to BTC manager, the security watchdog is now looking to adopt the Financial Action Task Force (**FATF**) recommendations for guidance on how to tighten HK oversight.

The SFC has always been of the opinion that instead of imposing an outright ban on digital currency exchanges like China, Hong Kong authorities should continue working towards creating a regulated environment for digital currency commerce in the city. This led to the introduction of policy requirements like its 2019 demand for all exchanges to have full deposit insurance, and now the SFC's latest directive. As Chinese law enforcement is continuously investigating principal actors at many major digital currency exchanges and effectively tightening the regulatory noose around smaller exchanges, the two jurisdictions seem increasingly taking divergent approaches to this growing sector.