Article Information

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

Blockchain Bites: Taking notes: PRC Minister says China should study crypto, FTX reorganisation secures major creditor support, North Korean hackers target crypto projects

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.

Taking notes: PRC Minister says China should study crypto

China's former Minister of Finance, Zhu Guangyao, recently urged Beijing to pay closer attention to cryptocurrencies during a speech at a summit hosted by Tsinghua University.

Zhu emphasized the need for the government to recognize the risks and potential harm that cryptocurrencies pose to capital markets, but also highlighted the importance of

> studying the latest international changes and policy adjustments, because cryptocurrencies are the most vital aspect to the development of digital economy.

Zhu cited the United State's change of rhetoric in relation to crypto – the US had focused on the challenges that cryptocurrencies may bring to international anti-money laundering and counter-terrorism financing efforts, and to international capital markets. However, the US's stance had changed significantly this year, especially in light of remarks made on the US campaign trail.

Zhu pointed directly at comments made by Republican candidate Donald Trump as a reason for further action by Beijing. At the Bitcoin Conference in Nashville in July, Trump stated that the U.S. must fully embrace the crypto industry, warning that if America does not take the lead, China will.

Trump compared the crypto industry to the steel industry of a century ago, predicting that it might one day surpass gold:

> One day, it probably will overtake gold. There's never been anything like it.

Zhu also noted that despite initial opposition, the U.S. Securities and Exchange Commission had approved Bitcoin and Ether exchange-traded funds (or ETFs).

The state of cryptocurrency is interesting in China. While mainland China remains cautious about cryptocurrencies and has placed a ban on them, the government has continued to make forays into digital asset by launching its own NFT marketplace, building a new blockchain network and issuing a retail central bank digital currency.

On the other hand, Hong Kong has taken a more welcoming stance in recent years, establishing a licensing framework for virtual asset service providers, promulgating regulations for stablecoins and tokenisation, listing Bitcoin and Ether ETFs and actively encouraging the industry to set up operations in the city.

Written by Jake Huang and Steven Pettigrove

FTX reorganisation secures major creditor support

The collapsed crypto exchange FTX has taken a big step forward in its bankruptcy process, with over 94% of its "Dotcom" creditors voting in favour of a reorganisation plan. These creditors, primarily clients of the offshore FTX.com exchange, represent approximately USD $6.8 billion in claims.

The plan, spearheaded by restructuring agent Kroll, promises to return 118% of claims in cash to most creditors – a rare offer in bankruptcy cases, where returns are rarely above or even close to 100%. The approval is a significant milestone for the company, which filed for bankruptcy following its dramatic collapse in 2022. Almost all creditor classes supported the plan, while two creditor groups didn't return ballots but are presumed to accept.

A hearing to confirm the plan is set for 7 October in the US Bankruptcy Court. However, potential hurdles remain. The US Securities and Exchange Commission (SEC) has previously raised concerns about using stablecoins for repayments (document filing number 24028). Whether these objections will influence the court's decision remains to be seen.

The reorganisation plan has been widely backed by Dotcom customers, with 94% of ballots cast in favour. US creditors were slightly less supportive, with 89% voting yes on claims totalling USD $60.99 million. Other creditors, like those with smaller Dotcom convenience claims, showed overwhelming approval, with nearly 96% backing the plan.

While the plan offers some hope for FTX's battered customers, the situation underscores the broader risks tied to the crypto industry's regulatory challenges. As the 7 October court date approaches, all eyes are on the SEC and the bankruptcy judge's final decision. If confirmed, the reorganisation plan could offer a win for FTX creditors—many of whom were left in financial limbo when the exchange imploded in late 2022.

Written by Luke Higgins and Steven Pettigrove

North Korean hackers target crypto projects

A recent investigation by CoinDesk has uncovered that more than a dozen crypto companies, including well-established blockchain projects like Injective, Fantom, and Cosmos Hub, unknowingly hired IT workers from North Korea.

This covert operation, orchestrated by the Democratic People's Republic of Korea (**DPRK**), poses significant cybersecurity and legal risks to the companies involved, many of which have subsequently suffered from hacking incidents linked to these employees.

The workers from North Korea operated under false identities, using forged documents, fake IDs, and resumes that showcased impressive technical skills and GitHub histories. These individuals were hired remotely, often through informal channels such as Telegram and Discord, and were able to pass standard background checks due to the sophistication of their forged credentials.

According to CoinDesk's report, several North Korean IT workers were able to secure employment at prominent blockchain firms like Sushi and Yearn Finance, with some even maintaining positions at multiple companies. One of the most significant vulnerabilities of the crypto industry is its reliance on global, remote workforces, which allowed DPRK workers to exploit the hiring processes, especially among smaller teams that lacked thorough vetting protocols.

Hiring DPRK workers comes with serious cybersecurity risks. CoinDesk identified multiple cases where companies that hired North Korean IT workers later became targets of cyberattacks. In one instance, the decentralised finance (**DeFi**) platform Sushi fell victim to a $3 million hacking incident in 2021, which was traced back to two North Korean developers. These workers had embedded malicious code into Sushi's platform, allowing them to redirect funds to wallets controlled by North Korean agents.

In another case, the crypto company Truflation, founded by Stefan Rust, unknowingly employed five North Korean developers. This included one employee, "Ryuhei," who initially posed as a Japanese national but was later revealed to be part of a North Korean scheme to funnel earnings back to Pyongyang. Rust's company later suffered a significant breach, with millions of dollars stolen from his personal and company wallets.

The U.S. Department of the Treasury's Office of Foreign Assets Control (**OFAC**) has been closely monitoring these activities, linking blockchain payments from North Korean developers to sanctioned entities utilising blockchain's

traceability. While no crypto companies have been prosecuted yet, the strict liability imposed by US sanctions means that businesses hiring DPRK workers, knowingly or not, could face legal repercussions.

CoinDesk's investigation highlighted the sheer scale of North Korea's infiltration into the crypto industry. Zaki Manian, a prominent blockchain developer, claimed that over 50% of the job applications in the crypto sector are suspected to come from North Korea. The challenge lies in identifying and filtering out these applicants, as they often possess legitimate technical skills and present convincing backgrounds.

Startups and smaller firms are particularly vulnerable, as they often lack the resources to conduct in-depth background checks. CoinDesk found that these companies are more likely to hire workers via informal channels, without verifying their true identities.

While North Korean IT workers may deliver satisfactory work, the legal and ethical implications are severe. Hiring DPRK workers violates international sanctions and contributes to the exploitation of these individuals, who are forced to send the majority of their earnings back to the North Korean regime. These wages, while high by North Korean standards, only enrich the oppressive government and its illicit and repressive activities.

As more stories come to light, developers must tighten their hiring processes and increase scrutiny of remote applicants, especially in a rapidly evolving industry that thrives on decentralised teams and remote workers. The risks extend well beyond one bad hire, and could extend to violations of international sanctions and the risk of cyber breaches and theft of digital assets.

Written by Steven Pettigrove and Luke Misthos