Article Information

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

Blockchain Bites: Australia and Singapore Govt blockchain trials, The Mt Gox Saga continues, Tips for Data protection, The flight from Macau

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

Cross border modernisation: Australian Border Force launches blockchain trial

The Australia-Singapore Digital Economy Agreement (**DEA**) entered into force on 8 December 2020 bringing with it global benchmarks for trade rules and a range of practical cooperation initiatives. Ultimately, the DEA seeks to reduce barriers to digital trade and build an environment where Australian businesses and consumers can yield the benefits of digital trade and a digitised economy.

Senator the Hon Simon Birmingham summarised the DEA as:

> [setting] new benchmarks including simplified arrangements for the exchange of electronic trade documents, and new rules that will prevent unnecessary data localisation requirements, including for the financial services sector, and forced technology transfers which can stifle trade and investment flows.

The Department of Agriculture, Water and Environment are also working on complimentary digital initiatives with Singapore regulators to progress paperless trading. As Australia's trading partners apply more rules and requirements to food exports relating to safety, provenance, and authenticity, blockchain developments in this area could significantly streamline manual paper based processes. This may also lead to a more flexible export regime so that exports can address new markets and respond to questionable bans or tariffs.

The Mt Gox Saga: Alexander Vinnik to serve 5 years in France

Alexander Vinnik, involved in the notorious BTC-e exchange in the EU, and the subject of a long running expedition battle between France, Russia, and the United states since his first arrest in Greece in December 2017, has finally been sentenced to serve five years in prison by a French court.

Vinnik, who prosecutors say operated the now-shuttered BTC-e exchange – once of the world's largest digital currency exchanges, was also fined USD$121,000 in relaiton to an alleged cryptocurrency fraud scheme. He is still yet to face authorities in Russia and the United States who are lining up to take their turn.

In Russia, his home country, Vinnik was charged in absentia with fraud over an alleged theft of just 9,500 euros. Meanwhile, the Department of Justice has been patiently waiting with with a list of 21 charges it announced in 2017. The DOJ alleges, similar to the French allegations, that BTC-e was a clearinghouse for funds sourced from "computer intrusions and hacking incidents, ransomware scams, identity theft schemes, corrupt public officials, and narcotics distribution rings." including the Mt Gox hack and other ransomware.

This sentencing is likely to be appealed and may represent a small door closing in the Mt Gox saga, which should further move closer to a resolution in a few days when news is expected as to when the 150,000 Bitcoin held by the trustees of the Mt Gox operating company will be released to former customers of the exchange. That process has been the subject of extensive delays to date.

Data breached? Ready Responses for Companies and Individuals

Hacks, data leaks and data breaches are fast becoming a fact of the digital age.

A recent leak of names and email from leading Australian digital currency exchange BTC markets demonstrates the importance of both internal data breach and incident response practices for companies. In this situation, the use of a third party email system resulted in emails being sent in batches of 1,000 with all 1,000 addressees included in each batch. The response from BTC Markets has been swift and forthright, showing the maturity of the digital currency exchange space.

This incident is a reminder to companies but also to users to secure their own data and protect themselves from scams or impersonations by bad actors.

Ultimately, individuals and businesses must be proactive about cyber security and take steps in advance of a breach occurring, with an action plan for when (not if) a data breaches occurs.

Suggestion & Surveillance: Talk of Chinese CBDC scares VIPs from Macau

Macau, a special administrative region of China with a gaming industry seven(!) times larger than that of Las Vegas, has been rattled by rumours of a CBDC being introduced. Eighty percent of Macau's gaming revenue traditionally is derived from just 5 percent of its VIP gamblers, and this fickle customer base plays a crucial role in the Macau gaming market.

Recent rumours that China's CBDC experiments will expand to Macau has seriously rattled junket operators – whose job it is to attract wealthy mainland Chinese gamblers to Macau.

What the situation comes down to is a common understanding that introducing the digital yuan would give a significantly increased surveillance capability to the Chinese government, via it's central bank, over the sources of cash flowing into and out of Macau.

As Junket service provider, Eric Leong, surmised:

> If the water is too clean, there'll be no fish. The big gamblers will go away if casinos need to be that transparent.

What adds salt to China's wound is Macau has already been hit hard by the pandemic. According to the latest figures from the Gaming bureau, Macau gaming revenue is down 80.5% in 2020 to $6.58 billion – a significantly larger drop for the "Vegas of China" than the downturn in Las Vegas itself, even before gamblers had to content with potentially increased surveillance.

Be that as it may, China is still consistently pushing ahead with the development and use of its digital yuan, with another pilot due to be trialled in the Suzhou district for the "Double 12" shopping event on Dec 12.