Article Information

Authors: Alexa Bowditch, Luke Misthos, Michael Bacina
Service: Blockchain, FinTech
Sector: Financial Services, IT & Telecommunications

Blockchain Bites: Corporate governance remains online a little longer, Chainalysis Report Shows Ransomware as Fastest Growing Crypto-related Crime, Open the vault: 'Mr. White Hat' Returns Almost All Stolen Funds

Michael Bacina, Alexa Bowditch and Luke Misthos of the Piper Alderman Blockchain Group bring you the latest legal, regulatory and project updates in Blockchain and Digital Law.

Corporate governance remains online a little longer

With the realities of COVID-19 still impacting day to day corporate governance, the government has announced some welcome relief. The *Treasury Laws Amendment (2021 Measures No.1) Bill 2021* (**Bill**) received royal assent on 13 August 2021 giving relief to those who had been focused on having to meet paper processes again, after the recent COVID-19 relief from paper based company matters expired on 21 March 2021

After a brief lull following that expiration where we returned to business as usual the prior relief from paperbased paperwork is back until Easter next year with some added extras!

1. **Virtual corporate meetings** can continue to be held and meeting documents may be distributed electronically to participants.

2. **Electronic execution** can be used for company documents and where a common seal is used the fixing of the seal may be witnessed electronically. It should be noted that State by State variations, particularly in relation to deeds, will need to be considered.

3. **Continuous disclosure breaches will be assessed with a 'fault element'** meaning that entities can only be found to have breached their continuous disclosure obligations if they did so with a fault element of knowledge, recklessness or negligence. This recognises the difficulty obtaining information about the value of an entity's securities given the state of flux and uncertainty caused by COVID-19.

The previous relief (plus extras) have been extended until the sunset date of **1 April 2022.** ASIC may issue instruments to extend the relief for a further 12 months although we hope the measures will be made permanent given the desire with which companies want to operate electronically is only growing.

As is often argued, the use of verification mechanisms by third party such as hashes (which assimilate some of the features which make up blockchain technology) provide a level of objective verification of signatures that simply is not possible with wet ink signatures. Hopefully the extension of electronic extension is more than a sign of the times but a sign of future acceptance of electronic execution for company documents (and using Blockchain systems where possible).

Ransom-everywhere: Chainalysis Report Shows Ransomware as Fastest Growing Crypto-related Crime

Chainanalysis recently released a mid-year update on the still small, but growing threat of ransomware.

Ransomware continues to be a concerning cybersecurity issue. More than USD$210M has been taken from victims so far in 2021, which suggests full year numbers are likely to be at least the same as last year when payments to ransomware attackers rose 344% from 2019 to over USD$416M.

Despite the growth of ransomware attacks, many quite public, Chainanalysis data shows that in 2020, 82% of digital currency sent by identified ransomware addresses was delivered to just five digital currency services. That concentration is even more pronounced at the deposit address level. Just 199 deposit addresses received 80% of all funds sent by ransomware addresses in 2020, with an even smaller group of 25 addresses accounting for 46% of the total sums. This is of course further evidence of how small and trackable digital currency misuse is on public blockchains.

Chainalysis reports are fascinating in identifying other useful trends for transaction monitoring including that:

1. The average ransomware payment in Q1 2021 was USD$54,000, up from USD$12,000 in Q4 2019.

2. Larger ransoms are now being commanded from high-profile victims including Bombadier, Acer and Colonial Pipeline, to name a few.

3. More ransomware attacks appear to be carried out by cybercriminals in Russia and other Commonwealth of Independent States countries.

4. Ransomware payments can create sanctions risks for companies that help facilitate payments and this risk is up from 15% in 2020 to 32% in 2021.

Some have proposed mandatory ransomware notifications be required to help prevent ransomware, and it is clear that despite hackers seeking payment in digital currencies, the true danger or ransomware is the lack of security which permits a hacker to take control of computer systems to begin with. The evolution of government ransomware policies, updating and strengthening of cyber hygiene regulations and standards, improving information sharing and increasing investigative resources must be deployed together to help change the trajectory of ransomware trends in the future. We are sure that the publicly trackable nature of blockchain systems will be used to help identify those assisting in the payment of ransoms, and may lead to arrests in time.

Open the vault: 'Mr. White Hat' Returns Almost All Stolen Funds.

The cybercriminals behind one of the world's largest cryptocurrency heists have returned almost all of the hacked assets to Poly Network. Around AUD$823 million of digital assets were stolen from the DeFi platform recently after hackers exploited a vulnerability in the Poly Network system. The Poly Network is a little known blockchain system largely based in China and so the hack had little impact on digital currency markets globally.

The hackers exposed a weakness in the digital contracts Poly Network used to move digital assets, according to Chainalysis. A person claiming to have instigated the attack wrote they did it "for fun" and wanted to "expose the vulnerability" before others could exploit the weakness, according to a notation on an Ether transaction. The hacker went on to say returning the tokens was "always the plan" and that they were "not very interested in money."

The stolen assets includes hundreds of millions of dollars in Ethereum, Polygon and Binance Smart Coin. Before long however, small amounts of the assets began being returning to wallets under the control of the Poly Network platform. This could be due to the involvement of a blockchain security firm SlowMist, engaged within hours of the hack and a statement saying the hacker's email, IP address and device fingerprints had been identified.

Within 24-hours, the hackers contacted Poly Network via an encrypted message in a cryptocurrency transaction stating: "ready to return". Before long, almost half of the stolen assets, were returned and communication has continued between Poly Network and the person they are calling 'Mr. White Hat', a reference to a "White Hat Hacker" which is an ethical hacker who does not steal or break into systems maliciously, as distinct from a "Black Hat Hacker" who does the opposite.

It appears now that almost all of the assets have been return, save for the AUD$44.8 million that cryptocurrency firm Tether froze using built in freezing switches within Tether tokens once the attack occurred, and several hundred million dollars worth of assets still within a wallet which requires both the Poly Network operators and Mr White Hat to sign a transaction to release those assets.

Could it be that the hacker truly is a White Hat as suggested, seeking to highlight only the flaws in smart contract code to promote stronger cyber security? Some suggest the headache of laundering almost AUD$1B may have proven too much and the absence of a contemporaneous message proving the hack was ethical is suspicious. Others have speculated that the combined effort off a virtual army and SlowMist would eventually track him or her down.

Even if Poly Network decide not to pursue the mysterious figure involved in the heist, the public nature of blockchains may mean others, including law enforcement, may not take such a polite view. This is not the first time that a theft of digital assets has resulted in a return of assets or discussions between the victim and the hacker, with the DAO hack in 2016 remaining one of the most well known.