Article Information

Authors: Jordan Markezic, Michael Bacina
Service: Blockchain, FinTech
Sector: Financial Services, IT & Telecommunications

Blockchain Bites: FBI Forms Crack Team to Target Crypto Crime, First DAO-n: $4bn sought to buy Denver Broncos: Critical bug in Coinbase reported and fixed

Michael Bacina and Jordan Markezic of the Piper Alderman Blockchain Group bring you the latest legal, regulatory and project updates in Blockchain and Digital Law.

FBI Forms Crack Team to Target Crypto Crime

The United States Federal Bureau of Investigation (**FBI**) has announced that it is launching a new team dedicated to blockchain analysis, virtual asset seizure and investigating cryptocurrency related crime.

The announcement follows the largest ever financial seizure by the FBI – USD$3.6 billion from a 2016 exchange hack. Deputy Attorney General Lisa Monaco said the Virtual Asset Exploitation Unit (VAEU) will be able to:

> combine cryptocurrency experts into one nerve center… [and to provide] blockchain analysis, virtual asset seizure, and training to the rest of the FBI.

The VAEU will work in conjunction with the U.S. Department of Justice's (**DOJ**) own targeted crypto-crime team, the National Cryptocurrency Enforcement Team.

The NCET has broad powers to:

> identify, investigate, support and pursue the department's cases involving the criminal use of digital assets, with a particular focus on virtual currency exchanges, mixing and tumbling services, infrastructure providers, and other entities that are enabling the misuse of cryptocurrency and related technologies to commit or facilitate criminal activity.

It is also likely that the VAEU will have a similar remit and powers.

The establishment of the VAEU and NCET will also have ramifications on privacy enforcement and responses to notifiable data breaches. Deputy Attorney General Monaco made it clear that ransomware will also be within the remit of the VAEU and NCET, which will be a step forward for enforcement agencies trying to 'bust [the] business model' for launching these attacks.'

The move towards crypto-crime disruption as opposed to outright prevention is interesting, as measures such as providing decryption keys or seizing servers used for cybercrime attacks could potentially limit the ability for law enforcement agencies to level criminal charges against offenders.

While it's unlikely that we'll be seeing a 1983 GMC Vandura van with a red-stripe on news reports taking down crypto-criminals, it's a positive step in increasing accountability within the market and establishes a precedent for a similar arrangements in Australia.

First DAO-n: $4bn sought to buy the Denver Broncos

Earlier this month, Denver Broncos CEO Joe Ellis announced that the franchise was in the early stages of being put up for sale. Sports media outlets such as ESPN have valued the franchise at approximately USD$4 billion.

In response, Investors and fans have setup a decentralised autonomous organisation – or a DAO – called "BuyTheBroncos" to try and raise enough funds to buy the Broncos and make them a community owned team (via a DAO). The BuyTheBroncos' website says:

> If we are successful in purchasing the Broncos, the fans would govern the team through a DAO, which would take the legal form of a cooperative. Your membership in the cooperative makes you an owner of the Broncos and, thus, able to participate in the governance. The DAO is regulated by smart contracts which ensure every single member is subject to the same rules.

We have previously reported on Colorado's adoption of crypto, and Colorado Governor Jared Polis has signalled his personal enthusiasm and interest in the project saying:

> I would be excited to be part of it myself… The challenge will be it'll take a lot of money… but you know what, if your imagination is big enough, then it can happen. And anything I can do to make it happen, I'd be happy to.

While it may be a stretch to raise USD$4 billion, it follows in the path of similar community minded DAOs such as the ConstitutionDAO which sought to buy a copy of the US Constitution. Expect to see more of this democratic form of leadership enabled by a DAO.

Critical bug in Coinbase reported and fixed

A security engineer under the user name 'Tree of Alpha' has been paid USD$250,000 as a 'bug bounty' for locating a frighteningly simple bug in the Coinbase website that, in effect, allowed users of the platform to sell cryptocurrency which they did not own.

The engineer discovered that, due to a simple flaw in the website code of a new trading feature launched by Coinbase, users could submit a trade in one cryptocurrency, but cause the trade to occur in another cryptocurrency which they did not own. This loophole was created in the absence of a validation check from a brokerage API endpoint which permitted the instructions to be submitted. This meant, for example, a sell order for 50 Dogecoins held by a customer could have been spoofed into becoming a 50 Bitcoin sell order.

The engineer initially reported the bug to the Coinbase bounty program and resorted to Twitter to raise the alarm, calling the vulnerability as:

> potentially market-nuking.

Coinbase shut the new product down in 30 minutes and responded within six hours that the vulnerability was remedied. Coinbase say the bug had not been misused previously. After responding to the vulnerability, Coinbase published an explanation as to the nature of the bug:

> A user has an account with 100 SHIB, and a second account with 0 BTC. The user submits a market order to the BTC-USD order book to sell 100 BTC, but manually edits their API request to specify their SHIB account as the source of funds. Here, the validation service would check to determine whether the source account had a sufficient balance to complete the trade, but not whether the source account matched the proposed asset for submitting the trade. As a result, a market order to sell 100 BTC on the BTC-USD order book would be entered on the Coinbase Exchange.

This highlights the distinction between 'white hat' and 'black hat' hackers. Traditionally, the public are taught when hearing about 'hackers' – to picture a criminal behind a laptop in a dark room: the so-called 'black hat' hacker who breaks into computer networks with malicious intent and are driven by self-serving, often economic, motivations.

On the other hand, however, exists another form of hacker – the ‘white hat’ hacker. These hackers seek to exploit computer systems to identify security flaws so that they can be fixed.

Of course, when talking about absolutes like ‘black’ and ‘white,’ it would be difficult to overlook the middle ground – the ‘grey hat’ hacker. These are hackers that act somewhere in the middle of ‘black’ and ‘white’ hacking. Oftentimes, they will exploit vulnerabilities without the permission of the platform owner in order to gain publicity and attract a fee.

Most bug bounties are, however, publicly offered so as to attract white hat hackers to test and challenge code, with a known reward if they succeed, and are popular in many blockchain and DeFi projects.