Article Information

Authors: Michael Bacina, Louisa Xu, Tom Skevington
Service: Anti-money Laundering & Corruption, Blockchain, FinTech
Sector: Financial Services

Blockchain Bites: Paypal launching crypto services, Financial Stability Board reports, FinCEN fines for crypto mixers and Department of Justice: World Police

Michael Bacina, Tom Skevington, Louisa Xu, Jade McGlynn and Marc Kopelowitz of the Piper Alderman Blockchain Group bring you the latest legal, regulatory and project updates in Blockchain and Digital Law.

PayPal promotes payments with digital currency

PayPal announced in partnership Paxos Trust Company, that PayPal will be offering customers the ability to buy, hold and sell digital currency directly from their PayPal accounts in the coming weeks.

The launch is only to US customers and initially featuring only major digital currencies Bitcoin, Ether, Bitcoin Cash and Litecoin.

Dan Schulman, President and CEO of Paypal said:

> The shift to digital forms of currencies is inevitable, bringing with it clear advantages in terms of financial inclusion and access; efficiency, speed and resilience of the payment systems; and the ability for governments to disburse funds to citizens quickly.

Paypal was also the first company to receive a conditional Bitlicense from the the New York State Department of Financial Services (**DFS**) or virtual currencies. The Bitlicense is granted under a new framework to promote a well-regulated virtual currency marketplace for the benefit of New York Customers announced in June 2020.

The new offering is a signal of PayPal's plans to significantly increase digital currencies' utility by making it available as funding source for purchases at its 26 million merchants worldwide to its over 300 million customers. This launch confirms the rumours we reported on earlier in the year after speculation of a potential Bitcoin integration with PayPal.

Financial Stability Board focus on CBDCs and Libra

The Financial Stability Board (**FSB**) has published two papers related to digital currency in preparation for the G20 in late November. The first on global stablecoins, titled 'global stablecoins, titled 'global stablecoins, titled 'global stablecoins, titled 'global stablecoins, titled 'global stablecoins, titled 'Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements' outlines high-level recommendations for the regulation, supervision and oversight of global stablecoin (**GSC**) arrangements. The second explores cross-border payments and sets out a broad timetable to explore central bank digital currencies (**CBDC**) for cross-border purposes. Remarkably, two papers on GSC's manage to avoid mentioning Libra by name even once.

In the FSB's outline of the first report, it unfortunately adopts the FATF's penchant for the terminology "so called

stablecoins", and uses the following ambiguous definition:

> So called "stablecoins" are a specific category of crypto-assets which have the potential to enhance the efficiency of the provision of financial services, but may also generate risks to financial stability, particularly if they are adopted at a significant scale

Adding to the misfortune, the recommendations in the report appear to be little more than broad motherhood statements of laudable ends which few could disagree with, but the real challenges are how detailed regulation will assist in meeting this without stifling innovation and new business.

The second report focuses less on GSC's specifically and CBDC's generally, and focuses on the more general goal of enhancing cross-border payments as a whole. The roadmap in this report provides that, in terms of timing, the key international standards bodies will make revisions to cross-border payments standards by the end of 2021. By July 2022, national authorities have to consider the impact of those standards on local regulations. Given that Libra has repeatedly confirmed its intention to only launch once it is fully regulated and compliant, this appears unlikely to occur before the end of 2021, which is the apparent deadline for when:

> National authorities establish or, as necessary, adjust for any existing GSCs and stablecoin arrangements that have the potential of becoming a GSC.

FinCEN issues first fines for Bitcoin mixing

The US Financial Crimes Enforcement Network (**FinCEN**) has issued its first-ever financial penalty against a Bitcoin mixer. FinCEN, the US Treasury Department's bureau focused on money laundering and national security, found that Larry Dean Harmon, the creator, and operator of crypto-tumblers Helix and Coin Ninja, willfully violated the Bank Secrecy Act (BSA) registration, program, and reporting requirements. As a result, Harmon was hit with a US$60 million civil penalty, and is being prosecuted in the U.S. District Court for the District of Columbia.

A quick refresher on crypto-tumblers/mixers. In their purest form, tumblers/mizers are a service that mixes different digital asset inputs and outputs to obscure their origin and enhance user privacy. Because most digital assets are inherently pseudonymous, mixers arose out of a desire by some users to protect their privacy.

FinCEN links Harmon and the use of Helix and Coin Ninja with child exploitation website 'Welcome to Video', which was taken down in a Department of Justice investigation in late 2019 and which relied on blockchain tracking of payments to identify wrongdoers. According to FinCEN, Helix was used to conduct:

> at least 73 bitcoin transactions worth over $2,000 directly with Welcome to Video. Mr. Harmon failed to file a SAR on these transaction (sic).

While money laundering is of course illegal, there is no specific law (in Australia, or as far as we are aware, the US) which renders the mixing of digital assets as a services illegal. On the contrary, FinCEN's suggests that mixers, so long as they are appropriately licensed and comply with their AML/CTF obligations, could be legal, based on their comment that:

> An anonymizing services provider is a money transmitter under FinCEN regulations because it accepts and transmits convertible virtual currencies.

In comments on the charges, Assistant Attorney General Brian A. Benczkowski of the Justice Department's Criminal Division has causes a significant stir by saying:

> This indictment underscores that seeking to obscure virtual currency transactions in this way is a crime, and that the Department can and will ensure that such crime doesn't pay.

Or put another way, if the anonymizing service keeps the *public* identification of users secret, but still permits reporting to regulators, the service is more likely to be acceptable.

The significant penalty, and even more significant illegality of Harmon's conduct is more accurately characterised by how brazen/negligent his actions were. In FinCEN's words:

> the investigation demonstrated that Mr. Harmon deliberately disregarded his obligations under the BSA and implemented practices that allowed Helix to circumvent the BSA's requirements. This included a failure to collect and verify customer names, addresses, and other identifiers on over 1.2 million transactions. Harmon, operating through Helix, actively deleted even the minimal customer information he did collect. The investigation revealed that Mr. Harmon engaged in transactions with narcotics traffickers, counterfeiters and fraudsters, as well as other criminals.

Notwithstanding the now questionable legality of crypto mixing as a whole, this is the first-ever financial penalty against a major Bitcoin mixer.

Team DoJ: World Police

The U.S. Department of Justice has released a report from the Attorney General's Cyber Digital Task Force titled "Cryptocurrency Enforcement Framework", which provides some insight into how Team America interprets its jurisdiction regarding digital asset activities.

The report opens with a hopeful introduction noting:

> it bears emphasizing that distributed ledger technology, upon which all cryptocurrencies build, raises breathtaking possibilities for human flourishing.

But after noting the valuable research and numerous studies and US Federal agencies exploring blockchain use, the report asserts:

> this technology plays a role in many of the most significant criminal and national security threats our nation faces

As one would expect for a document titled "Enforcement Framework" the report focuses on the oft repeated claim that digital assets are some kind of criminal haven. The DOJ also claims:

> Criminals use cryptocurrency to facilitate crimes and to avoid detection in ways that would be more difficult with fiat currency or "real money." They can avoid large cash transactions and mitigate the risk of bank accounts being traced, or of banks notifying governments of suspicious activity

This of course completely ignores the practical reality that cash transactions are more difficult to trace by orders of magnitude than the vast majority of digital asset transactions (aside from privacy coins), with the vast majority of illegitimate market activity on digital assets occurring on entirely traceable blockchain protocols like Bitcoin and Ethereum. While privacy centric coins have been claimed to have infinite uses for criminals, time and time again criminals appear to show a preference for blockchains that enjoy deeper liquidity and more reliable networks.

Frustratingly, the various case studies included in the report setting out the Departments experience of cryptocurrencies in investigations, which includes the cases against 'Welcome to Video', 'Lazarus Group', among others, makes no mention of the significant contribution made by blockchain analysis companies like Chainalysis. The narrow focus on the "dark side" of cryptocurrency completely ignores the reality that cryptocurrency with immutable public ledgers is a terrible system for illegal value transfer and an excellent tool for regulators. Had the perpetrators of these various illegal schemes paid in cash or another means, the critical blockchain analysis which contributed to their resolution would never have been possible.

Crypto companies praised by NYDFS for rapid response to recent Twitter Hack

In July 2020, a 17-year old hacker and his mates invaded Twitter and took control of dozens of high-profile users' accounts, using them to tweet out a "double your bitcoin" scam which resulted in the theft of over USD$118,000 worth of Bitcoin. To the disbelief of many, the Twitter Hack did not involve any of the high-tech or sophisticated techniques often used in cyberattacks–no malware, no exploits, and no back-doors.

Beyond its immediate monetary impact, the "garden-variety" nature of the hack exposed inherent cybersecurity weaknesses in Twitter, a social platform valued at over $37 billion dollars and counting over 330 million active users. Sparking a need for serious review and investigation, the New York Department of Financial Services (**NYDFS**) resolved to issue a report dissecting the hack – evaluating its surrounding facts, the reasons it occurred, and what could be done to prevent future incidents.

A number of accounts the attackers targeted included companies regulated by the NYDFS. the companies which due to their robust programs around cybersecurity, fraud-prevention, and anti-money laundering (as required by DFS regulations) were found to respond the best to the widespread disruption.

In the review of the hack the NYDFS found that 15 of the 22 crypto firms blocked the Twitter hackers' crypto addresses within 40 minutes. Although the report noted that the inaction of 7 companies could be attributed to their different business models which does not allow for the direct handling of transfer services and custody, according to NYDFS:

> [The majority of crypto firms] responded quickly to block impacted addresses, demonstrating the maturity of New York's cryptocurrency marketplace and those authorised to engage within it. Their actions show that New York continues to set a high standard and attract only the most responsible actors.

To validate its claims the report detailed how a number cryptocurrency firms, separately but in unison, rapidly blocked bitcoin addresses the Hackers posted on Twitter:

- Coinbase blocked around 5,670 transfers, valued at roughly $1,294,000;
- Bitstamp blocked one transfer, valued at $250;
- Gemini blocked two transfers, valued at $1,80000, and;
- Square blocked 358 transfers, valued at approximately $51,000.

This was in stark contrast to other victim organisations like Apple and Uber and other high profile politicians, celebrities, and entrepreneurs, who failed to prevent unsophisticated hackers on account of there being no regulatory regime that reflects social media as critical infrastructure . Posing a large risk to society, the large and globally influential social media companies, not just limited to Twitter, essentially regulate themselves.