

Cryptocurrency Crimes Are in A Class of Their Own

DAVID WHITE
ALIXPARTNERS LLP

► **As insolvent exchanges and IPOs continue to grow, finding the right technical partner with computer and accounting forensic skills to resolve the issues raised by digital currencies is more important than ever.**

Criminals are always at the ready to exploit the fast-moving pace of technological advancement. Cryptocurrencies are no exception. As these new financial transaction payment methods rapidly gain acceptance worldwide, so too have they become a prime target for hackers and fraudsters. One driver is the rapid deployment of new and often ill-tested technologies in the race to go to market. Another reason is that stealing credit cards and personal information to support identity theft is becoming harder and harder. Advances in chip and pin technology, better security protocols and better fraud detection by banks have all made credit card fraud and identity theft lucrative. Criminals have now begun to look for payouts in other places, especially those that yield direct cash payments. Two key targets are cryptocurrency exchanges – where the actual cryptocurrency coins are stolen and then liquidated for cash, and Ponzi fraud schemes built into many initial coin offerings (ICOs) – where the operators of the ICO siphon off investor funds for their own enrichment.

Both these types of methods have been yielding losses in the millions of dollars. Ten of the most high-profile ICO scams have swindled a staggering \$687.4 million from unsuspecting investors. A recent study prepared by ICO advisory firm Statis Group revealed that more than 80 percent of ICOs conducted in 2017 by number were identified as scams. According to the study, total funding of coins and tokens in 2017 amounted to \$11.9 billion, and over \$1.5 billion of this funding went to scams. The vast majority went to three

large Ponzi scams: Pincoin (\$660 million), AriseBank (\$600 million) and Savedroid (\$50 million), which together equal \$1.31 billion.

Cryptocurrency hacking is equally as lucrative. In September, hackers reportedly stole \$59 million worth of cryptocurrencies from Japanese exchange Zaif, while in Korea there have been at least seven hacks reported in the past 12 months totaling over \$100 million U.S. dollars in losses and leading to the bankruptcy of the largest exchange in that country. Globally, \$731 million worth of cryptocurrencies were reported stolen from crypto exchanges in the first half of 2018, a figure that is nearly three times the 2017 annual total. And the cyberfirm Carbon Black reports that roughly \$1.1 billion worth of digital currency was stolen across all sources in the first half of this year, with exchanges accounting for 27 percent of these hacks. Even countries that have banned cryptocurrency exchanges and ICOs outright have still seen large losses. This summer in China, three local men were arrested in Hunan, Changchun and Beijing for running an 87-million-dollar domestic cryptocurrency hacking scheme.

The Cyberheist at Mt. Gox

The Mt. Gox exchange hack in 2014 was one of the earliest, and still the largest, of the cyberheists. While it is still unclear if this was an inside or outside job, the result was the loss of over 750,000 Bitcoins (BTC) from the company coffers, which brought the exchange into bankruptcy. The proceedings, which are now consolidated in Japan, are still ongoing and very few creditor claims have been paid out to date. The case, however, calls out many of the unique legal issues relating to asset recovery in the world of digital currencies. For example, one of the primary questions in discussion has been whether successful claimants can expect a proprietary remedy in tokens, or merely an

unsecured creditor claim for the cash value of the tokens at the time of insolvency. That is, does a token holder have a creditor claim or a property claim in the estate? This question, which is common to any insolvency proceeding involving cryptocurrency tokens, is important as it can have serious financial repercussions for the claimants. The answer, as Mt. Gox demonstrated, turns on the legal classification of the tokens, which differs widely around the globe, as well as on the structure of the relationship between the user and the platform and how the courts choose to characterize that relationship.

U.S. securities law does not include cryptocurrency tokens in the definition of “money,” but rather treats them as intangibles, a classification that severely restricts their utility as a mainstream payment medium and as an asset that can easily be made the subject of a security interest. Intangibles are also treated as the least negotiable of all UCC forms of property. In Japan, however, the Mt. Gox court held that, under the local Civil Code, tokens are not capable of personal ownership at all. This meant that those with recoverable claims would not be able to recover their tokens back. Instead, they would only be able to recover the pre-filing cash value of those tokens. At the time of the bankruptcy filing in 2014, the Bitcoins had a total value of about \$438 million U.S. dollars. Since then the value of Bitcoin has increased considerably, putting the present-day value at several billion U.S. dollars. This creates a large residual in the estate that could lead to a potential windfall recovery for the owner of Mt. Gox, the very person who was likely instrumental in its failure and who is still facing criminal charges. It is not surprising that this less-than-equitable outcome was highly controversial given that bankruptcy proceedings are brought in equity. Accordingly, after years of litigation, the claimants moved for conversion of the proceedings to a civil rehabilitation action to revive the company,

hoping this would allow them to recover a pro rata share of the full estate value. That wish was finally granted by the court this past summer, and now the claimants are expected to recover at full present value. It has taken nearly four years of legal gymnastics to work through these novel issues, however, and the new claims process is still being worked out.

Grasping the Intangible

In addition to novel legal issues around asset classification, there are also a whole host of new technical and logistical issues that arise when an exchange, ICO or wallet holder goes into insolvency. These primarily stem from the digital nature of cryptocurrencies, which raises complex problems that simply are not seen with tangible or secured assets and fiat currencies. One area where this is most evident is bringing assets under the control of the receiver or trustee. This task can always be a challenge. Our firm has served as claims agent in the liquidation of assets for the Bernie Madoff Trust since his Ponzi scheme collapsed nearly 10 years ago, and bringing all of Madoff’s assets under control has been no small task. However, it pales in comparison to gaining control of digital assets that are not only encrypted but may also be scattered around the globe with no associated financial institutions attached to them. One of the first U.S. cases to bring these issues forward is the Cryptsy exchange liquidation. Cryptsy, a U.S.-based cryptocurrency trading



David White is a director at AlixPartners, where he advises clients on information governance, information security and electronic discovery. Reach him at dwhite@alixpartners.com.



platform, claimed to be hacked in January of 2016 for 13,000 BTC and 300,000 LTC. Since then the founder of the exchange, Paul Vernon, left his residency in Miami, Florida, and is now allegedly hiding out somewhere near Liaoning, China. The exchange was placed into receivership after its customers filed a class action law suit for recovery of their losses. After a default judgment was issued against him for failing to appear, the defendant confessed through a blog posting that the exchange had been insolvent after \$5 million disappeared in June 2014 and that he concealed this fact from customers and regulators. He also admitted having operated a fraudulent scheme for nearly 18 months while withdrawals were made from profits in its business operating account rather than being funded from safeguarded assets. Unfortunately, this scenario is becoming all too common across the hundreds of failed exchanges and fraudulent ICOs.

During its heyday, Cryptsy had a small IT team who ran a full stack of servers needed to manage a vast array of digital wallets. The deposits were comprised of billions of coins from over 1,000 different cryptocurrencies, each running on its own blockchain software that the receiver had to take control over and manage. This involved not only engaging a team of IT experts, but also computer forensic experts with blockchain experience to both operate and investigate the hardware and software. Each wallet contained hundreds of thousands of transactions that had to be uncovered, analyzed and assessed for claims settlements. For each account, the entire blockchain history must be analyzed in order to validate its balance. To this end, both the creditors' and the debtors' anonymous public encryption keys first had to be discerned from forensic evidence and records. But these encryption keys only allow for analysis of

the blockchain. In order to take control of the assets of the debtors, the receiver also had to uncover and take control of the debtors' own private encryption keys as well. Some token holders store these keys on their computers or mobile devices. In such a case, they may be able to be forensically recovered in the absence of cooperation if you have physical access to the devices and they themselves aren't further encrypted or locked. However, many token holders wisely opt to store their digital credentials offline and in secure areas such as in cold USB wallets. In extreme cases, token holders with significant holdings are reportedly storing their private keys on offline computers locked underground in decommissioned Swiss military bunkers to avoid hacking. In the absence of cooperation, it may be impossible to gain control of keys and their associated assets if they are stored in such unknown or inaccessible places. In the Cryptsy case, some wallets were also corrupt or damaged, and some maliciously destroyed by the debtor. Recovery of this data, where possible, required an even deeper level of digital forensic expertise. Further, the debtor sought to obfuscate or dissipate assets by destroying computer servers, destroying a database of books and records and their backups, starting a new exchange in China so he could transfer cryptocurrencies to it, and by converting tokens to jewelry and real estate. Unlike traditional funds tracing, tying these tangible assets back to token sales required careful and detailed analysis of digital transactions spread across the many crypto wallets and their associated blockchains. This could only be completed once all the data was safely secured and recompiled.

Further Challenges

Other hurdles still abound. Beyond recovery and control, assets may also need to be liquidated before claims can be paid out. Despite what headlines say about

the fungibility and demand of popular coins like Bitcoin and Ethereum, not all tokens are created equal. There are a great many alternative cryptocurrencies that have low to medium liquidity and very little demand, making liquidation difficult. Also, as the Mt. Gox trustee found out, liquidating large amounts of coin can have significant negative impacts on their market values and require strategic timing. Blockchains, the ledgers that record cryptocurrency transactions, are by design also immutable. This means that once you have agreed on a transaction and recorded it, it can never be changed. Doing so corrupts and invalidates the entire ledger. You can subsequently record another transaction about that asset to change its state, but you can never alter or remove the original transaction. This is great for preserving the provenance of assets. For any asset, you can tell where it is, where it's been and what has happened throughout its life. It also means that unwinding fraudulent conveyances and other reviewable cryptocurrency transactions is technically impossible. Recording a subsequent transaction may be the only viable option, which means that receivers and trustees are being forced to find or produce creative new ways of unwinding needed transactions within the law. This is often akin to fitting a square peg in a round hole with today's jurisprudence, however.

Cryptocurrencies and other blockchain technologies will undoubtedly continue to disrupt financial payment systems, and criminals will continue to find more and more lucrative ways to exploit these technologies and those who use them. This means that the number of insolvent exchanges and ICOs is only going to grow. In the face of this, it is imperative that our profession continues to evolve both legally and technically at an equal pace. It also means finding the right technical partners with the computer forensic skills and forensic accounting skills needed to resolve the many unique issues raised by digital currencies. ■