Cryptocurrency and Crime: Old Crimes Committed in New Ways, or a New Order of Challenges for Law Enforcement?

By Stefan D. Cassella

Editorial for the *Journal of Financial Crime*

Issue 5, online publishing date: 21st September 2024

The recent conviction and sentencing of Samuel Bankman-Fried, the founder of the failed cryptocurrency exchange known as FTX, shines the proverbial spotlight on the way that cryptocurrency has become a central factor in criminal cases and the recovery of criminal proceeds. Bankman-Fried was sentenced to spend 25 years in federal prison and was ordered to forfeit the $11 billion (USD) in proceeds that he derived from his offense. But was his case just a run-of-the-mill securities fraud case dressed up in shiny new clothes, or was it a crime made easier to commit by what the *New York Times* called the "loosely regulated world of cryptocurrencies?"

In one sense, defrauding investors in a cryptocurrency business is no different from defrauding investors in a non-existent oil well or in an overvalued condo development. The crypto world is just the latest context in which fraudsters and grifters have learned to operate. But in another sense, the crypto world of ephemeral assets, marked by a complexity that few understand and a vocabulary that few have mastered, has created opportunities for criminals and challenges for law enforcement that simply did not exist in any prior age.

Just how pervasive has cryptocurrency become in the conduct of criminals? Curious about this, I surveyed the reported cases from the federal courts in the United States since 2019 – focusing only on those involving money laundering or asset forfeiture – and was astounded by the results. In the last five years, there have been nearly 50 cases – criminal prosecutions, non-conviction-based forfeitures, and others – in which cryptocurrency was the major player.[i] And they have come in all forms and contexts: Yes, there have been other investment frauds and money laundering operations, but cryptocurrency has also provided criminals with new ways of defrauding victims, of evading taxes, and of committing crimes without detection, while the currency itself has become a favored target of thieves.

Moreover, the cryptocurrency cases have prompted law enforcement to develop new tools of investigation that the courts have had to review, understand, and approve.

FTX was not the only cryptocurrency case involving an investment fraud scheme; it was just the biggest one. In *United States v. Sharma,* the defendants defrauded investors of hundreds of millions of dollars by artificially pumping up the price of digital tokens issued by their company, Centra Tech, in an "initial coin offering." In *United States v. Kwok,* the defendant allegedly induced investors to invest $262 million in something called Himalaya Coin through Himalaya Exchange, ostensibly to raise money for the support of Chinese dissidents, and used much of the money to buy a luxury yacht. And in *United States v. Scott,* the defendant was the money launderer for an international Ponzi scheme based in Bulgaria that sold fake cryptocurrency to victims in the U.S.

Most recently, in *United States v. Crater,* the defendant advised investors that he had invented a new form of cryptocurrency called My Big Coin that was similar to Bitcoin but was superior in that it was backed by gold. Investors purchased at least $6.3 million in the new currency before discovering that it was not backed by gold, and that it could not be redeemed.

Investment fraud, however, is far from the only way that criminals use cryptocurrency to commit crimes. For obvious reasons, criminals like to use cryptocurrency to launder the proceeds of other crimes. In *United States v. Iossifov,* for example, a criminal organization laundered the proceeds a scheme to sell non-existent goods first by converting the victims' money to Bitcoin in the United States, and then by transferring the bitcoin to Bulgaria where it was converted back to fiat currency.

In other cases, like *United States v. 89.9270303 Bitcoins, United States v. Guerrero, and United States v. Chastain,* criminals converted stolen money, drug proceeds, and the proceeds of trading on confidential information, respectively, into Bitcoin and Etherum in an attempt to hide the money.

Crypto money laundering has, of course, been greatly aided by cryptocurrency businesses created specifically for the purpose of facilitating criminal activity by others. In *United States v. Sterlingov* and *United States v. Harmon,* for example, defendants were indicted under the money laundering statutes for creating crypto tumbling businesses called Bitcoin Fog and Helix,

respectively, that they advertised as ways of concealing assets from law enforcement.

Other businesses, while not charged with money laundering *per se,* have been prosecuted for the failure to maintain adequate AML/KYC programs. Most famously, Binance pled guilty to allowing its exchange to be used by "mixing services" that laundered criminally derived cryptocurrency, by persons moving the proceeds of ransomware, and by persons moving the proceeds of "darknet market transactions." And it was ordered to forfeit $2.5 billion as part of its sentence.

Cryptocurrency has also made it easier for customers of criminal marketplaces to make purchases of illicit material clandestinely, or for the purveyors of such material to market their goods without being detected. The Silk Road cases which involved the purchase of various illicit product on the darknet are the most well-known, but in *United States v. Twenty-Four Cryptocurrency Accounts*, the Government brought a civil (non-conviction-based) forfeiture action against crypto wallets holding the funds used to pay for child pornography in South Korea; and in *United States v. Adegboruwa,* a drug dealer insisted that his customers pay for the drugs with cryptocurrency because that made the proceeds easier to launder afterwards.

Cryptocurrency has also provided criminals with new ways of committing fraud or embezzlement.

In *United States v. Approximately 32113.63 Tether (USDT) Cryptocurrency*, the victim of a fraud scheme was advised by a caller that his identity had been stolen and that he needed to purchase bitcoin and transfer it to a digital wallet (provided by the fraudster, of course) to protect it from theft. Similarly, in *United States v. Approximately 1.10387626 Bitcoin,* the victim was told that his bank account had been compromised and that he had to transfer the contents to a "secured digital wallet" to secure his funds. And in *United States v. Approximately 3879.16242937 bitcoin,* the defendant embezzled $154 million from his employer by directing the employer's bank to transfer the money to a crypto exchange where it was used to purchase bitcoin. In all three cases, the Government used civil forfeiture actions to recover the property and restore it to the victims.

Finally, cryptocurrency itself has become the object of theft. In *In the Matter of the Search of Multiple Email Accounts,* the defendants were arrested

and charged with the theft of $3.6 billion in bitcoins stolen from a Hong Kong-based exchange. In *United States v. 113 Virtual Currency Accounts,* operatives acting on behalf of North Korea gained access to the private keys of the customers of cryptocurrency exchanges in the United States, and stole hundreds of millions of dollars in virtual currencies. And *United States v. Approximately 69,370 Bitcoin,* involved the theft of $14 million in bitcoin by someone who hacked into the Silk Road. In the latter two cases, the Government again used civil forfeiture to recover the property.

All of this has naturally prompted law enforcement to up its game, creating new investigative tools and using all judicial means available to recover assets.

In *United States v. Approximately 1,360,000.748 Tether,* the FBI used blockchain analysis to trace $5.5 million in fraud proceeds through a series of "hops" from one cryptocurrency address to another until it came to rest in a particular account, and then convinced a court that the analysis was sufficiently reliable to support the issuance of a seizure warrant for the account where the funds landed. And in *United States v. Sterlingov,* the Government convinced a court that Chainalysis's Reactor program was a sufficiently reliable means of linking the defendant to an otherwise anonymous cryptocurrency address to be admissible as evidence against him in his criminal trial.

Finally, law enforcement in the United States has made robust use of the civil or non-conviction-based (NCB) asset forfeiture laws to bring actions to recover cryptocurrency when no criminal prosecution was possible --- generally because the perpetrator of the offense giving rise to the forfeiture was unknown, was a fugitive, or was a foreign national who committed the offense from China, North Korea, or some other country from which his extradition was unlikely. In such cases, NCB forfeiture is without doubt an essential law enforcement tool – and one that countries that have not yet enacted NCB forfeiture laws must hasten to implement.

The moral of the story is that cryptocurrency has become endemic in the criminal subculture. It has allowed old crimes to be committed in new ways, has fostered the commission of entirely new crimes, and has facilitated the laundering of criminal proceeds in a global marketplace that law enforcement finds difficult to penetrate. Indeed, the advent of cryptocurrency has spurred the creation of a new industry made up of businesses that exist solely to exacerbate

the difficulties faced by law enforcement, and to frustrate the efforts of victims to recover their property.

Nevertheless, the development of new means of analysis and the courts' acceptance of their reliability, coupled with the aggressive use of non-conviction-based forfeiture in appropriate cases, shows that Governments are able to respond to the new challenges in their myriad forms, to bring criminals to justice, and to recover property notwithstanding its being dressed in the guise of a shiny new object that can be devilishly hard to find.

Stefan D. Cassella is a former federal prosecutor in the U.S. Department of Justice who is now the CEO of Asset Forfeiture Law, LLC, a consulting firm in Baltimore, Maryland and Washington, DC.

---

[i] All of the cases referred to herein, and others dealing with cryptocurrency, are collected, with full citations and summaries provided, my website, www.AssetForfeitureLaw.us, in the post entitled, "Crypto Case Summaries."