



CRYPTOCURRENCY AND CRIMINAL DEFENSE

RISING TO THE CHALLENGE OF MODERN-DAY CLIENTS AND MODERN-DAY PROBLEMS

BY IAN N. FRIEDMAN & MARA M. HIRZ

Talk of cryptocurrency and the blockchain is rather commonplace today. Between “hot” investment tips from relatives; think pieces about the environmental impact of Bitcoin mining farms; and the high-end art community’s sudden interest in non-fungible tokens (NFTs), opinions abound. As trends in cryptocurrency and other blockchain technologies continue to evolve, so too must the modern attorney evolve. At times, cryptocurrency topics may feel confusing or difficult to navigate — but do not be dissuaded. This article will provide a synopsis of recent trends in cryptocurrency and blockchain development, discuss cryptocurrency crimes and the Government’s response, and provide practical tips for criminal defense lawyers when handling cryptocurrency cases.

Cryptocurrency Digital Landscape

While the history of digital currencies dates to the 1980’s, Satoshi Nakamoto’s 2008 creation of Bitcoin is often marked as the invention of modern-day cryptocurrencies. The development of Bitcoin spurred a new generation of digital currencies and brought cryptocurrencies into the mainstream. Now, by some estimates, there are over 6,000 cryptocurrencies in existence. Each of these cryptocurrencies has a unique purpose or function, however the core concepts remain the same: they are all online peer-to-peer systems which allow payments or assets to be sent directly from one party to another.

Cryptocurrencies, in and of themselves, have clearly changed the modern financial landscape. The technology underlying cryptocurrencies has even led to the creation of other new digital currencies and assets. One such evolution is Stablecoins, which peg their value to an external reference, such as a fiat currency (like the United States Dollar), commodity, or other derivative

asset. As the name suggests, this connection to an external reference offers price stability in a way that traditional cryptocurrencies do not. Cryptocurrencies can be extremely volatile, as their values can fluctuate wildly. For some investors, this volatility may be desirable as it can lead to high risk, high reward profits. However, not every person using cryptocurrency is doing so for investment purposes. Accordingly, Stablecoins offer the security, privacy, and transferability of traditional cryptocurrencies while also providing the stable valuation of fiat currencies.

Another digital asset born of cryptocurrency technology is the Non-Fungible Token (NFT) — a digital asset that correlates to real-world objects such as art, music, or an in-game item for a video game. Unlike cryptocurrencies, NFTs tend to be one of a kind. The first NFT ever created, which occurred in 2014, was “Quantum,” a digital animation made by artist Kevin McCoy. In June of 2021, Sotheby’s auctioned Quantum for \$1.4 million. At the same auction, a different NFT, which is part of a series titled “CryptoPunk,” sold for \$11.8 million.

Cryptocurrency Crimes and the Government’s Approaches

With the rise in the popularity of cryptocurrency comes the need for Government regulation. However, rather than defining and classifying cryptocurrency as its own entity, and then creating a body of regulation specifically suited for it, the Government has opted to regulate cryptocurrency within the confines of existing statutes. This has led to confusion about the classification of cryptocurrency as well as the agencies which have authority to regulate it.

For example, the Commodity Futures Trading Commission (CFTC) classifies cryptocurrencies as “commodities.” Meanwhile, in 2014, the Internal Revenue Service (IRS) issued a

Notice declaring that, for federal tax purposes, virtual currency (including cryptocurrency) is treated as “property.” The United States Securities and Exchange Commission (SEC), however, has classified some cryptocurrencies as “currencies,” while classifying others as “securities.” These inconsistencies make it difficult to lawfully navigate purchasing, selling, or trading cryptocurrencies, and often require the advice of crypto-experienced counsel to ensure compliance.

The Department of Justice (DOJ) is now expanding the resources spent investigating and prosecuting cryptocurrency crimes. In October of 2020, the DOJ released its Cryptocurrency Enforcement Framework (the Framework), which it developed as part of the Attorney General’s Cyber-Digital Task Force. The Framework “provides a comprehensive overview of the emerging threats and enforcement challenges associated with the increasing prevalence and use of cryptocurrency.” The Framework suggests that cryptocurrency crimes tend to fall into one of three categories: using cryptocurrency to make illegal purchases (such as buying illegal narcotics or funding terrorism); using cryptocurrency to commit money laundering and tax fraud; or using cryptocurrency to commit crimes directly involving the cryptocurrency marketplace (such as cryptocurrency theft or using the promise of cryptocurrency to defraud investors). The Framework demonstrates that the DOJ is taking cryptocurrency crimes seriously and will be increasing resources to the investigations and prosecutions of these crimes.

In October of 2021, the National Cryptocurrency Enforcement Team (NCET) was announced. According to the Department of Justice, the purpose of NCET is to “tackle complex investigations and prosecutions of criminal misuses of cryptocurrency, particularly

crimes committed by virtual currency exchanges, mixing and tumbling services, and money laundering infrastructure actors.” NCET utilizes experts from many different DOJ divisions and provides another tool for law enforcement to investigate and prosecute unlawful conduct related cryptocurrency.

While new efforts to address cryptocurrency offenses are being announced, it must be noted that the DOJ has been actively prosecuting cryptocurrency criminals for several years. Presently, these cases are most often viewed as: wire fraud and securities fraud violations; money laundering and unlicensed money transmitting violations; and ransomware and extortion violations. Fraud cases are the most prevalent and tend to be predicated on false guarantees of investment returns and/or Ponzi schemes. As an example, the reportedly largest cryptocurrency scheme in recent times, which at its core was nothing more than a Ponzi scheme, involved a fraudulent cryptocurrency called BitConnect. On November 12, 2021, U.S. District Judge Todd W. Robison granted a request from the DOJ and the U.S. Attorney’s Office for the Southern District of California to liquidate approximately \$56 million in fraud proceeds seized from the “number one promoter” of BitConnect. To date, this is the largest single recovery of a cryptocurrency fraud by the United States government. More should be expected with the increase of crypto use, regulation, and enforcement.

Advice for Criminal Defense Attorneys

In many ways, cryptocurrency crimes are no different than their traditional fiat currency counterparts. At its core, cryptocurrency fraud is fraud, cryptocurrency money laundering is money laundering, and cryptocurrency tax evasion is tax evasion. Like any other financial case, a defense attorney must identify the scheme and follow the money. However, since cryptocurrency is a relatively new technology, often the defense attorney must also take on the role of translator. While cryptocurrency is growing in popularity, it is incumbent on the defense attorney to distill and demonstrate the simplicity of the overall alleged crime. Counsel must dispel early on the notion that the use of cryptocurrency is reserved for nefarious purposes only. To the contrary, it must be stressed that the global financial system is rapidly evolving toward a digital structure and that those at the forefront must not be automatically considered suspect. There seems to be a persistent belief, by several governmental agencies, including the some at the highest levels of law enforcement,



BUILD YOUR CASE WITH FORENSIC ACCOUNTING EXPERTS

APPLE GROWTH PARTNERS
Healthy Growth.

SERVICES INCLUDE:

- Domestic Relations Litigation
- Shareholder Disputes
- Fairness & Solvency Opinions
- Collaborative Divorce
- Expert Witness Testimony
- Forensic Accounting Services for Fraud Cases

LEARN MORE: [APPLEGROWTH.COM/LITIGATION- SUPPORT](https://applegrowth.com/litigation-support)

that cryptocurrency is still primarily used for illegal purposes. Because of this, it is important to recognize that many people, including judges and jurors, presume negative context surrounding the use of cryptocurrency. This presumption is immediately damaging to a targeted individual or entity and must be refuted by the criminal defense team.

To that end, an expert may be necessary to explain what cryptocurrency is, how it is used for legitimate purposes, how cryptocurrency transactions are made, how these transactions can be traced, and how cryptocurrency affects the case in general. A qualified expert can clarify these issues and reduce confusion and bias about cryptocurrency. Because cryptocurrency is still in its infancy, selecting the right cryptocurrency expert can be challenging. Unlike other commonly used experts, potential cryptocurrency experts may not yet have the credentials, certifications, or clearly defined practice areas seen in other contexts. Many who are properly credentialed, do not have a track record of being declared a court expert nor have they testified to a substantial degree. Certain cases may require an expert familiar with cryptocurrency investment strategies and fiduciary duties, while others may require a software coder or an expert familiar with emerging technologies and novel cryptocurrencies. Accordingly, a criminal defense attorney must be diligent in selecting a cryptocurrency expert with the right qualifications and familiarity with the specific technical issues. Counsel must be weary of engaging a traditional certified public accountant or forensic accountant to analyze the purported crypto-scheme or determine loss amount. This is due to the fact that traditional accounting experts will not be sufficiently aware of the ever-shifting crypto landscape, which includes differing views of value and loss.

Additionally, many criminal cryptocurrency cases have parallel civil proceedings. Therefore, the criminal defense team must be prepared to work with civil counsel to share discovery resources, discuss defense theories, and craft global resolutions which are in the client’s best interest.

Today, the need for capable and informed defense attorneys, who understand cryptocurrency, is critical. Cryptocurrency technology cannot be considered a passing fad and will only continue to evolve and grow. Moreover, the DOJ, and other law enforcement agencies, have made it clear that investigating and prosecuting cryptocurrency-related crimes will be a priority in the coming years.



Ian N. Friedman is the founding partner of Friedman & Nemecek, L.L.C. He is a former CMBA president, which he has been a member of since 2002. Ian is also a former president of the American Board of Criminal Lawyers, and the Ohio Association of Criminal Defense Lawyers. As a professor teaching Cybercrime at the Cleveland-Marshall College of Law, Ian maintains a diverse and ever evolving technology practice. He can be reached at (216) 928-7700 or inf@fanlegal.com or via Twitter @IanNFriedman.



Mara M. Hirz is an attorney at Friedman & Nemecek. She holds a joint J.D./M.B.A. from the Cleveland-Marshall College of Law. She has been a member of the CMBA since she was barred in 2021. Prior to entering the world of criminal defense law, Mara practiced as a mechanical engineer with focus on microelectronics and semiconductors. Proudly embracing her tech-nerd side, Mara is an extremely effective advocate for individuals and entities faced with any investigation or prosecution involving technology. She can be reached at (216) 820-4653 or mmh@fanlegal.com.