Federal Bar Association

THE
FEDERAL LAWYER

The Magazine of the Federal Bar Association

On Bitcoin and Ponzi Schemes

By Tal J. Lifshitz

July/August 2021

Tal J. Lifshitz at Kozyak Tropin & Throckmorton

Bernie Madoff died in federal prison a few months ago with the dubious distinction of being the mastermind of the largest and most infamous Ponzi scheme of all time. Madoff stole tens of billions of dollars from thousands of investors over the course of 17 years. He received a 150-year prison sentence for his crimes and was ordered to forfeit $170 billion in assets. Madoff's

scheme collapsed in 2008, but the recovery and distribution of assets pursuant to the unwinding of the scheme, and the inevitable litigation accompanying that process, continue today.

Satoshi Nakamoto's legacy remains to be determined. Most know him as the man behind the curtain—the anonymous founder of Bitcoin, the cryptocurrency that has gone from a cypherpunk electronic cash experiment to a digital asset, which, at its all-time high, has already surpassed a $1 trillion market cap.

At least 35 publicly traded companies now hold bitcoin on their balance sheets. (Capital "B" Bitcoin refers to the Bitcoin network, which enables participants to send and receive the lowercase "b" bitcoin virtual currency that is sent through that network and can, for example, find itself on a company's balance sheet.) The recently confirmed SEC chair, Gary Gensler, has taught courses at MIT—"Blockchain and Money" (Fall 2018) and "FinTech: Shaping the Financial World" (Spring 2020)—exploring Bitcoin and other cryptocurrencies. And the Miami Heat's basketball arena, formerly known as AmericanAirlines Arena (or the "triple A"), will now be named for FTX, the cryptocurrency exchange that won the arena's naming rights earlier this year.[1]

At its 2021 all-time high, one bitcoin was worth over $63,000. A year ago, one bitcoin was worth approximately $20,000. A year before that, it was worth approximately $3,000. A year before that, Justice Breyer was analyzing the definition of "money" in an artful dissent in which he observed that "perhaps one day employees will be paid in [b]itcoin or some other type of cryptocurrency."[2]

Justice Breyer's prediction came true with astonishing speed. Earlier this year, Miami Mayor Francis Suarez suggested that the city pay municipal workers, accept tax payments, and invest city funds in bitcoin.[3] More recently, Mayor Scott Conger of Jackson, Tenn., announced that his city is likewise exploring paying employees in bitcoin, as well as mining bitcoin to add it to the city's balance sheet.4 And the NFL's most recent number one overall draft pick, Clemson quarterback Trevor Lawrence, announced that he's investing his approximately $22 million signing bonus in bitcoin and other ryptocurrencies (while at least two other NFL players have already been taking their salaries in bitcoin).

By any measure, Bitcoin has been an extraordinary, perhaps even evolutionary, success. Such success inevitably attracts new market participants. And there have been many. The global cryptocurrency market cap has already exceeded $2 trillion. There are nearly 5,000 digital coins or tokens tracked on CoinMarketCap, a popular price-tracking website for cryptoassets. Each coin offers unique features or utility and—if you are an investor or speculator—wildly varying opportunities for returns. By now, many people have, at a minimum, heard of Ether and Dogecoin, which themselves have accounted for approximately half a trillion dollars of the cryptocurrency market cap at their highs—notwithstanding that Dogecoin, which is based on an internet meme, was openly created as a joke to prove that people will buy anything.

The biggest problem with Bitcoin? It's complicated. In a March 2018 segment of his show Last Week Tonight, John Oliver described cryptocurrencies as "everything you don't understand about money, combined with everything you don't understand about computers."

Bitcoin's complexity inevitably invites confusion, fear, uncertainty, and doubt—what the cryptocurrency community aptly refers to as "FUD." FUD over how Bitcoin works, FUD over how cryptocurrencies work, FUD over how blockchain technology works, and general confusion and FUD over Ponzi schemes and how they work. All this FUD has inevitably led some to proclaim that Bitcoin itself, for example, is a Ponzi scheme.

Bitcoin may be difficult to understand. Its price may be subject to manipulation. Normal market forces may ultimately drive its price to zero. Some of its various promoters, acting independently, might be engaged in various forms of fraud. It might be a "bubble." Or one bitcoin could become worth millions and get adopted as a new global currency. Any of these scenarios could be true.

But Bitcoin itself is not a "Ponzi" scheme. A Ponzi scheme is a particular species of fraud, and Bitcoin doesn't fit the definition.
Understanding how a Ponzi scheme works, and how Bitcoin and cryptocurrencies work, is important, not only for the sake of accuracy but also for the sake of consumer protection. Because there is plenty of fraud in the world of cryptocurrencies. A 2018 study that analyzed initial coin offerings (ICOs)—the unregulated cryptocurrency analog of an IPO—concluded that

over 80 percent were "scams."[5] Nothing suggests that those numbers have improved, which is a scary prospect in the aftermath of the 2021 cryptocurrency bull market. Fortunes are made in such markets, to be sure. Dogecoin, the "joke" coin, was at one point up approximately 11,680 percent so far this year (notwithstanding a slight dip after Elon Musk jokingly referred to it as a "hustle" while hosting Saturday Night Live). But such successes are inevitably accompanied by stories of life savings lost and lives ruined.

Perhaps some tragedy can be avoided. This article seeks to level the playing field a bit by clarifying some of the confusion around Bitcoin, ryptocurrencies, Ponzi schemes, and fraud; and by identifying red flags present in such scams—both "traditional" and those involving virtual currency. We will briefly review Ponzi schemes, how they started, and how they work. We will then analyze the genesis and evolution of cryptocurrencies, including some representative crypto-related fraud. We will conclude by examining the relevant regulatory and legal framework and whether it is sufficient to address the unsettling new world of crypto fraud.

What's a Ponzi Scheme?

The SEC defines a Ponzi scheme as "an investment fraud that pays existing investors with funds collected from new investors …. With little or no legitimate earnings, Ponzi schemes require a constant flow of new money to survive. When it becomes hard to recruit new investors, or when large numbers of existing investors cash out, these schemes tend to collapse."[6] This is why Ponzi schemes are commonly referred to as a "house of cards."

These schemes are named after Charles Ponzi, who defrauded thousands in the 1920s by falsely claiming he could sell international postal coupons—pieces of paper good for the price of one international airmail letter stamp in any country—at 100 percent profit.

Since individual postal administrations set the price of the coupons sold at their offices, a coupon bought in a country with low postage rates could be worth more than its purchase price in another country with higher rates. For example, if the United States sold a coupon for $.25 and Canada accepted the coupon in payment for a stamp worth $.50, a buyer of the U.S. coupon could double their money.

Ponzi realized he could exploit the price differential between Italian and American coupons to make a profit, since a coupon bought in Italy was then worth four times the price in the United States. Of course, actually converting the coupons into cash at any scale was utterly impracticable. But that didn't stop Ponzi, who convinced some of his friends that he could double their money in 90 days using the coupon scheme. While Ponzi never actually used the money to buy Italian coupons, he took in enough cash to pay some of the earlier investors, which helped him attract more investors, and on and on the cycle continued—until it collapsed when a savvy investor did the math and realized there weren't enough coupons in the world to support Ponzi's claims.[7]

There have been thousands of similar schemes. While no official statistics are available, a simple word search on Westlaw returns more than 9,000 separate opinions with the word "Ponzi."

Of course, there are now laws and regulations in place to prevent and uncover such misconduct. But none of those laws and regulations stopped Madoff. It took the 2008 financial crisis, which made it hard to recruit new investors, to bring down Madoff's scheme. And that same crisis ignited the cryptocurrency industry.

Enter Satoshi Nakamoto

"I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted party."[8]

On Oct. 31, 2008, Satoshi Nakamoto delivered the above message via email to a small mailing list of cryptographers. It contained a link to a nine-page white paper titled "Bitcoin: A Peer-to-Peer Electronic Cash System" that focused on the architecture of what is now called a "blockchain." On Jan. 3, 2009, Bitcoin's genesis block—the first block in its "chain"—was created. The timing of Bitcoin's debut was not a coincidence. Satoshi embedded a message in it, for anyone to see, referring to banks and bailouts: "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks."[9]

But what is a "peer-to-peer electronic cash system"? How does Bitcoin work? It's often described as digital money, which sounds simple enough. But Bitcoin is more accurately described as a worldwide platform that allows people to

communicate directly without a middleman (a trusted party like a bank) to validate their messages, and which is—above all else—focused on executing transfers of money. (If you are wondering what problem this solves, think wire transfers available 24/7 that settle rapidly with little to no fees or even a need for a bank account; at least, that's part of the idea.)

This is what Satoshi meant by "peer-to-peer electronic cash." The Bitcoin platform is operated, managed, and maintained globally using open-source software available for anyone (including you) to see, download, and use. In this way, Bitcoin functions as a secure platform for electronic cash transactions by allowing those who run it to maintain and validate a public ledger. The ledger records every bitcoin transaction that has ever or will ever occur and allows anyone (including you) to retain a complete record of every transaction ever made on the network, to ensure that the ledger is immutable.

According to the SEC, "Bitcoin has been described as a decentralized, peer-to-peer virtual currency that is used like money—it can be exchanged for traditional currencies such as the U.S. dollar, or used to purchase goods or services, usually online. *Unlike traditional currencies, Bitcoin operates without central authority or banks and is not backed by any government."*[10]

That last sentence is critical. Bitcoin is "decentralized" because it operates without "central authority," instead distributing that authority to anyone who chooses to download the software and participate in maintenance of the platform. In other words, "[n]o one 'owns' the Bitcoin network, it is not a formal organization, and it has no board of directors or central governance structure."[11] So, at least as to Bitcoin, there is no individual "Charles Ponzi" to pay back early investors with new investor funds, there is no centralized recruitment of new investors, and there is no single figure whom investors (or the authorities) can chase if they seek to cash out or suspect fraud.

The revolutionary potential of this decentralized technology has largely driven the skyrocketing value of bitcoin as an asset. It was only a matter of time before fraudsters took advantage of this crypto hype.

Crypto Meets Ponzi

Bitcoiin—note the extra "i"—was actually promoted by Steven Seagal and billed itself as "the world's first self-sustaining cryptocurrency." Its promoters touted that the Bitcoiin tokens would be deliverable on a reputable blockchain called Ethereum, that invested funds would be used to develop a coin like bitcoin, and that the tokens would be tradeable on a proprietary digital asset trading platform. This was a sham. The promoters misappropriated millions of dollars of investor funds for their own personal benefit. Even Seagal was fined by the SEC for failing to disclose a fee he received in return for his promotion.

Bitconnect investors fared no better. They were promised returns of over 40 percent per month. Instead, Bitconnect collapsed when two state regulators issued cease and desist letters, and the crypto community started openly referring to it as a Ponzi scheme.

Representatives of OneCoin, which pitched itself as the next Bitcoin, were in the middle of a sales pitch to investors when law enforcement raided their meeting and arrested 18 company employees. Multiple national authorities have described OneCoin as a Ponzi scheme, which, according to some sources, stole up to $19.4 billion.

In the *Shavers* Ponzi scheme, the fraudsters advertised a bitcoin "investment opportunity" in an online Bitcoin forum. Investors were allegedly promised up to 7 percent interest per week and that their funds would be used for bitcoin arbitrage activities in order to generate the returns. Instead, in classic Ponzi fashion, invested bitcoin was used to pay existing investors and exchanged into U.S. dollars to pay the organizer's personal expenses.

The allure of the world of cryptocurrency to fraudsters has undoubtedly been strengthened by the lack of any crypto-specific regulations as well as the delayed application of existing regulations—such as federal and state securities laws—to the rapidly developing crypto space. In one particularly egregious example, a company called Crypto Calls held itself out as a leading "crypto pump group" that could skyrocket the value of a cryptocurrency using a classic "pump and dump" approach. Such tactics would never be permissible in the world of securities regulated by states and the SEC; but in the world of crypto, this company promoted its business openly.

So it was no surprise when, in 2013, the SEC issued an investor alert on "Ponzi Schemes Using Virtual Currencies." The SEC warned that, "[a]s with many frauds, Ponzi scheme organizers often use the latest innovation, technology, product or growth industry to entice investors and give their scheme the promise of high returns. Potential investors are often less skeptical of an investment opportunity when assessing something novel, new or 'cutting-edge.'"

Of course, in 2013, Bitcoin and other virtual currencies were—if nothing else—novel, new, and "cutting edge." The SEC was appropriately worried that "the rising use of virtual currencies in the global marketplace may entice fraudsters to lure investors into Ponzi and other schemes in which these currencies are used to facilitate fraudulent, or simply fabricated, investments or transactions."[12]

2014 brought another SEC investor alert titled "Bitcoin and Other Virtual Currency-Related Investments" to alert investors to the potential risks of investments involving bitcoin and other virtual currencies and explain that "the rise of Bitcoin and other virtual and digital currencies creates new concerns for investors." This time, the SEC singled out Bitcoin by name, warning that "[a] new product, technology, or innovation—such as Bitcoin—has the potential to give rise both to frauds and high-risk investment opportunities. Potential investors can be easily enticed with the promise of high returns in a new investment space and also may be less skeptical when assessing something novel, new and cutting-edge."[13]

Sensing Bitcoin's growing momentum, the SEC began to tailor its fraud-related investment advice to the burgeoning cryptocurrency, advising investors that

> [i]f you are thinking about investing in a Bitcoin-related opportunity, here are some things you should consider. Investments involving Bitcoin may have a heightened risk of fraud. Innovations and new technologies are often used
> by fraudsters to perpetrate fraudulent investment schemes. Fraudsters may entice investors by touting a Bitcoin investment "opportunity" as a way to get into this cutting-edge space, promising or guaranteeing high investment returns. Investors may find these investment pitches hard to resist.

The SEC offered three specific warnings. First, that Bitcoin users may be targets for fraudulent or high-risk investment schemes because of their recent and unexpected increase in wealth (from the appreciation of their bitcoin). Fraudsters might, according to the SEC,

> take advantage of Bitcoin users' vested interest in the success of Bitcoin to lure these users into Bitcoin-related investment schemes. The fraudsters may be (or pretend to be) Bitcoin users themselves. Similarly, promoters may find Bitcoin users to be a receptive audience for legitimate but high-risk investment opportunities. Fraudsters and promoters may solicit investors through forums and online sites frequented by members of the Bitcoin community.

Second, the SEC warned that using bitcoin may limit recovery in the event of fraud or theft because the third-party wallet services, payment processors, and bitcoin exchanges that play important roles in the use of bitcoin may be unregulated or operating unlawfully, and because law enforcement officials could face particular challenges when investigating the illicit use of virtual currency. Such challenges include (i) money tracing, since traditional financial institutions (like banks) often are not involved with bitcoin transactions, making it more difficult to follow the flow of funds; (ii) the international scope of bitcoin transactions, which could potentially restrict how the SEC can use, receive, or even locate information as part of an investigation; (iii) the lack of any central Bitcoin authority, which leaves the SEC relying on other sources, such as bitcoin exchanges or users, for its investigatory focus; and (iv) the difficulty of seizing or freezing illicit proceeds held in bitcoin, even if located, since bitcoin wallets are encrypted and might not be held by a third-party custodian (unlike money held in a bank or brokerage account).

Finally, the SEC emphasized bitcoin's unique investment risks, each of which should be considered in connection with the evaluation of any bitcoin investment. First, while U.S.-based securities accounts and bank accounts are often insured by the Securities Investor Protection Corporation and Federal Deposit Insurance Corporation, respectively, bitcoin held in a digital wallet or exchange do not have similar protections. Second, bitcoin's exchange rate historically has been volatile and could drastically decline (it has dropped as much as 50 percent or more in a single day). Third, bitcoin are not legal tender (except in El Salvador as of June 2021), so federal, state, or foreign

governments may restrict their use and exchange. Fourth, bitcoin exchanges may stop operating temporarily or permanently due to fraud, technical glitches, hackers, or malware (and bitcoin also may be stolen by hackers). Finally, as a recent invention, Bitcoin does not have an established track record of credibility and trust (i.e., bitcoin and other virtual currencies are evolving daily).[14]

The government warnings have evolved as well. In 2019, another investor alert was released, this time jointly by the SEC's Office of Investor Education and Advocacy and the Commodity Futures Trading Commission's Office of Customer Education and Outreach (CFTC), warning investors to scrutinize investment opportunities through websites purporting to operate advisory and trading businesses related to digital assets. This alert, titled "Watch Out for Fraudulent Digital Asset and 'Crypto' Trading Websites," explained that "SEC and CFTC staff have recently observed investment scams where fraudsters tout digital asset or 'cryptocurrency' advisory and trading businesses. In some cases, the fraudsters claim to invest customers' funds in proprietary crypto trading systems or in 'mining' farms. The fraudsters promise high guaranteed returns (for example, 20-50%) with little or no risk."

In some cases, the alert explained, after the investors make an investment, typically using a digital asset such as bitcoin, they never hear from the fraudsters again, and the stolen funds have already quickly been moved overseas, out of the victim's practical reach. In other cases, the fraudsters con investors into paying purported taxes or other bogus fees to withdraw fake "profits": an advance fee fraud scam.[15]

There have been many alerts and warnings from the regulators over the last decade. But how much progress has been made in actually tracking and preventing such fraud, or more generally, in offering guidance and clarity to the crypto community over how and which regulations even apply? The answer is "not enough."

So Where Are We With Crypto Regulations?

In the highest profile crypto-related lawsuit now pending, the SEC has sued one of the biggest players in the industry, Ripple, for the unregistered offer and sale of over $1.3 billion of its signature digital currency XRP. (XRP is currently ranked the fifth largest cryptocurrency on CoinMarketCap, with a

market cap of over $63 billion.) One of Ripple's defensive arguments is that it has been operating openly for eight years alongside other cryptocurrencies, like bitcoin, that have not been treated as securities. So Ripple asks, why is XRP being targeted, and why now? So far, that has proved to be a difficult question for the SEC to answer, and Ripple has scored some significant discovery victories regarding, for example, compelled production of internal SEC discussions about whether Ripple's XRP tokens are similar to cryptocurrencies like bitcoin, which have been deemed "commodities" outside the purview of the SEC.

The securities laws should provide guidance and clarity on, for example, whether a crypto coin or token like bitcoin or XRP meets the Supreme Court's Howey test for a security—thereby subjecting the crypto to a legal and regulatory regime that offers consumers substantial security and protection.16 Unfortunately, the guidance has been murky. In April 2019, the SEC released a "Framework for 'Investment Contract' Analysis of Digital Assets" to try to assist those considering an ICO in determining whether the federal securities laws would apply under Howey.17 But some commentators have said that the framework raises more questions than it answers.

Beyond the securities laws, historically there has been another check on fraudsters and Ponzi schemers. Federal law has long required banks—a necessary component of any "old school" Ponzi scheme—to be wary of such illegal conduct. Enacted in 1970, the Bank Secrecy Act (BSA), enlisted bank employees into the war against money laundering and other financial crimes. The BSA led to the adoption of "know your customer" (KYC) policies by financial institutions throughout the country. These policies require banks to know the customer's identity, the purpose of their accounts, and the types of transactions the customer is expected to have, in order to combat the illegal use of financial services.

Subsequent regulations have also required banks to report suspicious activity, including any potentially criminal conduct, to a centralized federal authority, the Treasury Department's Financial Crimes Enforcement Network. And after 9/11, the USA PATRIOT Act led to additional requirements for banks to identify and verify the identity of customers opening new accounts.

However, as the SEC noted in its 2014 alert, crypto-based frauds generally do not flow through banks, neutralizing the well-established oversight of the BSA

and the PATRIOT Act, and making it difficult (if not impossible) to trace and seize funds after a fraud is revealed.

Clarity, guidance, and investor protection are needed. Hopefully, some help is on the horizon. The Anti-Money Laundering Act (2020), for example, expands the scope of activities subject to BSA requirements to include institutions engaged in the transmission of virtual currencies—not just traditional banks. And in April, SEC Commissioner Hester M. Peirce, nicknamed "Crypto mom," released an updated version of a Token Safe Harbor Proposal that would give crypto startups a three-year grace period within which they could sell tokens through ICOs to fund development efforts, exempted from the registration provisions of the federal securities laws, as long as they comply with reporting requirements that could ensure the absence of fraud.

And most recently, the House of Representatives passed a bipartisan bill called the ''Eliminate Barriers to Innovation Act of 2021'' (H.R. 1602) that would create a digital assets working group between the SEC and the CFTC. If this act becomes law, within one year, the new working group will need to provide a report on the legal and regulatory frameworks related to digital assets, including the impact that the current lack of clarity regarding digital assets has had on primary and secondary markets, and provide recommendations on, among other things, how to reduce fraud and increase investor protections.

Closing Thoughts

E.O. Wilson, a sociobiologist from Harvard, has explained that the fundamental problem of humanity is that we have paleolithic emotions, medieval institutions, and accelerating God-like technology. Our evolutionary instincts and institutions, such as law and government, are stagnant compared to technologies like Bitcoin and blockchain, which advance every day and can become obsolescent in months rather than decades.

Our laws are struggling to keep up with our technologies and the scammers and fraudsters who exploit them. This is an exciting time in the world of cryptocurrencies and blockchain. It's also a dangerous time for those who are uninformed, don't do their research, and let the fear of missing out on something "novel, new, or cutting-edge" overwhelm rational and prudent investing diligence.

The red flags of fraud haven't changed. "Guaranteed" high investment returns don't exist. Unsolicited sales pitches from people you don't know are suspicious. If the investment sounds too good to be true, it probably is. Investments providing higher returns typically involve more risk. Fraudsters like to try to create a false sense of urgency to get in on the investment, so take your time researching an investment opportunity before handing over your money.

While Bitcoin doesn't satisfy the definition of a "Ponzi" scheme, there are undoubtedly many cryptocurrencies that do. Time will tell. Be careful. Do your research. And if you find yourself a victim, contact an attorney.

DISCLAIMER

The views expressed in this article are not those of the author's employer, clients, or any other organization. The opinions expressed do not constitute legal advice or risk management advice. The views discussed are for educational purposes only.

Tal J. Lifshitz is a partner in Kozyak Tropin & Throckmorton's complex litigation department. An experienced litigator and former federal judicial law clerk, he has represented a wide range of sophisticated corporate and individual clients, including investors in high-stakes business disputes, investment and securities frauds, and Ponzi scheme litigation. Lifshitz speaks and writes regularly on trial practice, class actions, and the intersection of law and technology, including FinTech, blockchain, and digital currency. He is active on social media and can be followed on LinkedIn and Twitter for litigation skills and tips, thoughts on law and technology, and more.

Endnotes

1 Andrew Ross Sorkin et al., *Miami Wants to Be the Hub for Bitcoin*, N.Y. Times (Mar. 23, 2021), https://www.nytimes.com/2021/03/23/business/dealbook/miami-suarez-crypto.html.

2 *See Wisconsin Cent. Ltd. v. United States*, 138 S. Ct. 2067, 2076 (2018) (Breyer, J., dissenting) (citing F. Martin, Money:

The Unauthorized Biography—From Coinage to Cryptocurrencies 275–278 (1st Vintage Books ed. 2015)).

3 Sorkin, *supra* note 1.

4 Mayor Scott Conger (@MayorConger), Twitter (Apr. 20, 2021, 10:13 PM), https://twitter.com/MayorConger/status/1384691758936825857.

5 Shobhit Seth, *80% of ICOs Are Scams: Report,* Investopedia (Apr. 2, 2018), https://www.investopedia.com/news/80-icos-are-scamsreport/.

6 Sec. Exch. Comm'n, Ponzi Schemes, https://www.investor.gov/introduction-investing/investing-basics/glossary/ponzi-schemes (last visited May 10, 2021).

7 As Chief Justice Taft explained, when analyzing Ponzi's scheme at the Supreme Court, Ponzi "was always insolvent, and became daily more so, the more his business succeeded. He made no investments of any kind, so that all the money he had at any time was solely the result of loans by his dupes." *Cunningham v. Brown*, 265 U.S. 1, 8 (1924).

8 Satoshi Nakamoto, Bitcoin P2P E-cash Paper, https://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html (last visited June 4, 2021).

9 Justin S. Wales and Richard J. Ovelmen, *Bitcoin Is Speech: Notes Toward Developing the Conceptual Contours of Its Protection Under the First Amendment*, 74 U. Miami L. Rev. 204, 206–07 (2019).

10 Sec. Exch. Comm'n, Investor Alert: Bitcoin and Other Virtual Currency-Related Investments (May 7, 2014), https://www.sec.gov/oiea/investor-alerts-bulletins/investoralertsia_bitcoin.html.

11 Wales and Ovelmen, *supra* note 9, at 210–12.

12 Sec. Exch. Comm'n, Investor Alert: Ponzi Schemes Using Virtual Currencies (July 1, 2013), https://www.sec.gov/investor/alerts/ia_virtualcurrencies.html.

13 FINRA had also recently issued an Investor Alert cautioning investors about the risks of buying and using digital currency such as bitcoin, and the North American Securities Administrators Association (NASAA) included digital currency on its list of the top 10 threats to investors for 2013.

14 Virtual Currency-Related Investments, *supra* note 10. 15 Sec. Exch. Comm'n, Investor Alert: Watch Out for Fraudulent Digital Asset and "Crypto" Trading Websites (Apr. 24, 2019), https://www.sec.gov/oiea/investor-alerts-andbulletins/ia_fraudulentdigitalasset.

16 *SEC v. W.J. Howey Co.*, 328 U.S. 293 (1946).

17 Sec. Exch. Comm'n, Framework for "Investment Contract" Analysis of Digital Assets n.1 (Apr. 3, 2019), https://www.sec.gov/corpfin/framework-investment-contractanalysis-digital-assets#_edn1.July