2018

Cryptocurrency Fraud: A Look Into The Frontier of Fraud

Stafford C. Baum
Georgia Southern University

Cryptocurrency Fraud: A Look Into The Frontier of Fraud

An Honors Thesis submitted in partial fulfillment of the requirements for Honors in Accounting.

By
Stafford C. Baum

Under the mentorship of Dr. Britton McKay

ABSTRACT

This research project was conducted to look into what sort of frauds can be committed to steal unsuspecting investors' cryptocurrencies. The inspiration for this research came in the form of the fact that millions of dollars are lost to cryptocurrency fraud each day, and many of these frauds are successful due to the public's naivete towards the dangers of investing in cryptocurrencies. After researching many different cryptocurrency fraud cases, the frauds could be categorized into four major categories. These categories include Ponzi schemes, fake initial coin offering schemes, pump and dump schemes as well as cryptocurrency theft.

Thesis Mentor:_____

Dr. Britton McKay

Honors Director:_____

Dr. Steven Engel

December 2018
Accounting
University Honors Program
Georgia Southern University

Acknowledgements

I would like to sincerely thank Dr. Britton McKay for all her help and guidance while completing this project. I could not have completed this project without her mentorship and enthusiasm concerning my topic. I would have gone in a totally different direction with my research had I not been inspired by an anecdote concerning shady activities that could be conducted with cryptocurrencies in her A.I.S. class last spring semester.

The inspiration for this research project stemmed from the idea that not enough people are educated on the dangers of cryptocurrencies. Many crypto-investors lose large amounts of capital every day to fraud committed with cryptocurrencies and I have theorized that this is due in part to the public's naiveté towards all of the fraudulent activity that can be conducted with cryptocurrencies. I conducted research on the subject to test the hypothesis that a typical group of college students would not be able to correctly answer a majority of questions pertaining to cryptocurrencies and frauds that can be committed with them. The survey was administered in introductory business classes at two universities and included 125 students from 18 to 26+ years of age. The survey included many topics ranging from basic questions pertaining to how cryptocurrencies function, to basic financial frauds that could be committed with cryptocurrencies as well as questions designed to ascertain the students' level of understanding of unsafe crypto-trading procedures (fig. C). The results proved my hypothesis that college students could not successfully answer a majority of questions correctly pertaining to cryptocurrencies. The findings go to show that exactly 50% of the questions asked in the survey were answered correctly by a majority of participants, thus proving my hypothesis that the students could not answer a majority of the questions in the survey correctly. (fig. B). It is also interesting to note that that when asked about to what degree they believed that cryptocurrencies were safe investments utilizing a scale from 1-7, a majority of the participants fell within the 2-4 range. When asked about their familiarity concerning cryptocurrencies using the same scale, most participants fell within the 1-3 range. These findings prove that more people need to be educated about the potential dangers of investing in cryptocurrencies before they invest in them.

Ever since Bitcoin began the cryptocurrency craze when it was introduced in 2009, many investors have flocked to cryptocurrencies believing that they can be newest, hippest way to ‘get rich quick’. Many crypto-investors have experienced massive payouts from investing in cryptocurrencies as well as enjoyed the perks of having capital in a decentralized exchange. However, there is a dark side to this budding cryptocurrency market. As they have for centuries, fraudsters and con men have evolved with the times, finding new ways to defraud unassuming crypto-investors every day. This new generation of fraudsters has found ways to perpetrate Ponzi schemes, create fake initial coin offerings, pull exit schemes, coordinate pump and dump schemes as well as concoct many different schemes to steal investors’ cryptocurrencies out from under their noses. More and more people lose money to these frauds as the popularity of cryptocurrencies rises. A recent survey conducted by Bitcoin.com News found that crypto-investors lose $9.1 million a day on average to cryptocurrency fraud (Shobhit, 2018). This statistic just goes to show that the public needs to become more educated on the many ways one can lose money when investing in the proverbial ‘wild west’ of investments.

Ponzi schemes are frauds in which perpetrators pay off old investors’ dividends with new investments from new investors. Most of the time, the perpetrator’s investment firm will not even own a single share of stock. New investors are wrangled in by falsified reports, unrealistically high return rates and the recommendations of older investors. Many are familiar with this fraud scheme due to the publicity that the Bernie Madoff case elicited. However, due to the general public’s naiveite concerning cryptocurrencies, most may not be familiar with Ponzi Schemes that can be committed with cryptocurrencies. Probably the most infamous ‘Crypto-Ponzi Scheme’ would be the scheme perpetrated by

Bitconnect. On the surface, Bitconnect seems like a perfectly legitimate cryptocurrency/exchange with a user-friendly website complete with a fun, animated video explaining its supposed perks. However, Bitconnect perpetrated a Ponzi scheme that relieved thousands of investors of their cash. Initial investors were promised returns of up to 120% in the early days of the cryptocurrency. Investors were told by Bitconnect that they would earn 'interest' on their BCC's if they stored and traded them on Bitconnect's native cryptocurrency exchange thus rendering 95% of BCC transactions to occur on said exchange (Buntinx, 2018). Another red flag was that any purchases of Bitconnect Coin (BCC) had to be paid in Bitcoin. This was most likely due to the fact that cash purchases are easier to trace as opposed to purchases using Bitcoin or any other cryptocurrency. Bitconnect supplied investors with earnings reports that would show how much they had gained in interest. The 'interest' was no doubt earned through the funds coming from new investors; the textbook definition of a Ponzi scheme (Jenkin, 2018). As of January 17th, 2018, many believe that Bitconnect's Ponzi scheme has come to a halt. The price of BCC had decreased drastically by 80% in a short amount of time falling from a lofty $400 per BCC to a mere $27 per BCC (Buntinx, 2018). This rapid decline is no doubt in response to many crypto-investors' realizations that they were most likely being scammed out of their money and had no chance of recovering their funds. Unfortunately, the perpetrators of the scheme covered their tracks very well. By operating anonymously and requiring that all BCC purchased be made be bought with Bitcoin, they made it nearly impossible for investigators to track them down. Some estimate that anywhere between 1 and 10 million dollars were stolen as a result of this fraud (cryptick, et al). Regardless of what the scope of the damage of this Crypto-Ponzi scheme actually

was, the fraud was prominent enough to make many potential crypto-investor wary of his or her next crypto-investment. Another notable 'Crypto-Ponzi Scheme' would be the one that a company by the name of Bitfinex perpetrated. Bitfinex started out as legitimate 'Crypto-company' that took in investors just as any public company would. The scam began when Bitfinex servers were hacked and thieves made off with $72,000,000 worth of customer investments. In an attempt to minimize the effects of the theft, Bitfinex executives encouraged investors to convert their shares into equity within the company thus creating value from nothing at all. Once most of the investors had converted their investments to shares, Bitfinex then encouraged them to sell their equity as shares to new investors. Once enough people had fallen for the fraud, they used the new investors' funds to pay off the hack victims' hold outs, in effect, creating an effective Ponzi scheme (Bitfinexed, 2017). The cryptocurrency Tether is yet another example of a Ponzi scheme committed with cryptocurrencies. Tether is a type of cryptocurrency that is purposefully set to an equal exchange rate. Theoretically, this allows Tether to act as a safe medium for investors who are constantly trading one cryptocurrency for another. Tether claims that for each Tether on the marketplace, there will be one U.S. dollar to back it up. Red flags manifest when you look into the numbers for yourself. On the open exchange at the time this research was conducted, Tether has approximately 2,830,109,970 Tethers in circulation (www.coinmarketcap.com). According to Tether's last audit at the time of this research, which occurred on May 23rd, 2017, auditors could only account for $44,771,061.81 in U.S. dollars which is not even close to the figure of Tether in circulation (Crypto Investor, 2017). Many crypto-investors believe that Tether is perpetrating a Ponzi scheme since the amount of cash that they are supposed to have to

back up their cryptocurrency is nowhere close to the amount of cryptocurrencies on the market as there should be. Along with the numbers not matching up, many crypto-investors are also wary of a few other red flags surrounding Tether's business practices such as the business ties with the aforementioned Bitfinex, the disintegration of relationships with many prominent banks, lawsuits against said banks, the tendency of Tether to withhold crucial information from investors as well as Ronn Torrosian's (head of public relations for Tether) past association with a company that had committed a Ponzi scheme in the past (*BitcoinExchangeGuide*,2017). Fraudsters are famous for their craftiness and ingenuity, so it is no surprise that they have adapted an age-old scheme to cryptocurrencies.

Another typical fraud associated with cryptocurrencies would be the fake ICO scheme. In the world of cryptocurrencies, ICO's or Initial Coin Offerings are similar in many aspects to Initial Public Offerings for stocks. Typically, a cryptocurrency company will release a predetermined number of coins to the open market in the same way stocks are issued when a company goes public. Many ICO's are in fact legitimate cryptocurrencies that have potential to make the investor a profit like any other security. However, there is a substantial portion of ICO's that are deemed fraudulent since the executives of these companies attempt to coerce investors to invest in cryptocurrencies that do not actually exist in an attempt to relieve them of their money in a quick and efficient manner. These con artists capitalize on potential investors' FOMO, or 'fear of missing out' on the next big cryptocurrency payout (Zhu and Zhang, 2018). Researchers from a 'Big 4' accounting firm, Ernst & Young, estimate that more than 10% of the $3.7 billion invested in ICO's thus far have been stolen due to fake ICO schemes such as these

to date (Zhu and Zhang, 2018). Fake ICO perpetrators will attempt to entice potential investors to become ensnared in their scheme by fabricating exorbitantly high return rates, lying about the numbers of investors and how much they had invested as well as advertising novel features in an effort to make their non-existent cryptocurrency irresistible. A fake ICO scheme under the guise of a fake cryptocurrency by the name of Plexcoin did just this. Plexcoin's executives promised unbelievable returns of up to 1,354% in the first 30 days, which of course cannot be a number that any feasible security could guarantee (Levine, 2017). Plexcoin also brought in investors by suggesting that they were in the process of developing a credit card like instrument deemed 'Plexcard'. Supposedly, this fictitious card was designed to draw Plexcoin out of ATM's as well as "be used anywhere in the world and [would] be connected directly to [a] PlexWallet. It will give you the opportunity to spend your money in a totally confidential way" (Levine, 2017). In addition to the ridiculous statements concerning the fake cryptocurrency, Plexcoin's website and business plan were also worryingly vague. It turns out that the fake ICO scheme perpetrated by Plexcoin was the brainchild of a repeat fraudster, Dominic LaCroix. The S.E.C. was able to prosecute LaCroix since fake ICO's fall under securities fraud (Levine, 2017). Unfortunately, LaCroix was still able steal over $15 million before his arrest (Lee, 2017). Another interesting example of a fake ICO scheme would be the REcoin scheme. REcoin was a fictitious cryptocurrency created by a fraudster by the name of Maksim Zaslavskiy. Zaslavskiy pedaled his 'revolutionary', new cryptocurrency as being the first ever cryptocurrency to be backed by real estate. One article described REcoin as a great investment vehicle for investors wary of the world of cryptocurrency since, unlike any other cryptocurrency, the "proceeds from the initial sale

of tokens will be invested in the highly regulated real estate market in virtually all jurisdictions while reinforcing the holders' and investors' confidence in the REcoin "(Zaslavskiy, 2017). Zaslavskiy also perpetrated the same fraud with another fake cryptocurrency with the designation of DRC for Diamond Reserve Club. The theory behind DRC was similar to REcoin, but instead of proceeds being invested in real estate, proceeds were supposedly invested in diamonds (Morris, 2017). However, it seems as though Zaslavskiy never did invest any proceeds from REcoin into any real estate or any proceeds from DRC into diamonds. According to an investigation conducted by the SEC, it was discovered that neither REcoin or DRC had any operations (Morris, 2017). Zaslavskiy and LaCroix are just a few of many fraudsters that have attempted to perpetrate fake ICO schemes. The S.E.C. believes that this problem is so prevalent that this is such a prevalent issue for potential crypto-investors, that they have even made a mock, fake ICO website in order for them to consult when wondering whether or not invest in a cryptocurrency (Liao, 2018). The S.E.C.'s website can be reached at www.howeycoins.com and should be consulted by any and everyone who is on the fence about the legitimacy of a cryptocurrency (*HoweyCoins*, 2018).

The next scheme to be discussed is exit schemes. According to Investopedia, an exit scheme is "a fraudulent practice by unethical cryptocurrency promoters who vanish with investors' money during or after an ICO" (Shobhit, 2018). Sometimes, exit schemes may be able to start out as legitimate enterprises. However, due to adverse economic conditions, poor business planning or a combination of both, future perpetrators of exit schemes may attempt to vanish into thin air in an attempt to escape the consequences of overseeing a failing business, making off with all the investors' funds in the process. This

sort of scheme has become popular with cryptocurrency start ups seeing as anonymity is easy to maintain when all a business's operations are virtual. A crypto-company by the name of Giza perpetrated a scheme just like this. Investors believed Giza to be a legitimate company since it had announced a partnership with a Russian tech firm, Third Pin LLC. Giza contracted Third Pin to aid in the creation of a secure device that could store cryptocurrencies. Giza in turn raised over 2,100 Ethereum coins, an amount equal to roughly $2.4 million at the time. Investors began to worry when Third Pin announced that they had cut ties with Giza. Around February of 2018, all of the investors' funds were transferred out of the known Giza wallet, supposedly by the mysterious and anonymous C.E.O. of Giza, Marco Fike. No one has been able to track down Fike (if that is even his real name) since his LinkedIn profile contained falsified information such as the fact he attended Oxford University when Oxford has no record of his attendance (Kharpal, 2018). Giza has now become synonymous in the crypto-trading community with exit schemes. A similar exit scheme was perpetrated by the crypto-company, LoopX. LoopX told investors that it had developed a complex crypto-trading software that contained an algorithm that would earn investors weekly profits. Contrary to the payouts that they were expecting, investors were instead relieved of 276 Bitcoin and 2,446 Ethereum in January 2018. It appears as if LoopX decided to pull an exit scheme when they decided that they would not be able to convince investors that they were unable to come up with a software that could do everything that they promised. There are no traces of LoopX's website or the type-o riddled white paper anywhere on the internet seeing as the fraudsters wiped every trace of LoopX's existence from the internet (Mix, 2018). Even though some crypto-companies may pull an exit scheme to escape a business plan gone

wrong, there are many more fraudsters perpetrate the same scheme with no intention of ever delivering anything for their customers or investors. One of the biggest exit schemes that fits into this category would be the one pulled off by CabbageTech. Patrick McDonnell, C.E.O. of CabbageTech pulled his exit scheme by offering customers crypto-investment trading advice in exchange for payments of cryptocurrency. CabbageTech claimed that with their service, one could expect as high as a "300% return on an investment in less than a week" (Cheng, 2018). However, McDonnell never delivered the service to his customers, and attempted to simply exit the business with approximately $1.1 million worth of customers' Bitcoin. However, the Securities and Exchange Commission and Commodity Futures Trading Commission have filed charges against McDonnell and CabbageTech to thwart ever growing cryptocurrency fraud in America (Cheng, 2018). The CabbageTech fraud is not alone by any stretch of the imagination. Benebit was supposed to be a novel cryptocurrency company that would use benefits to incentivize customers to invest. Benebit also claimed that it would the rewards system would work like racking up frequent flyer miles from your airline. However, investors began to question Benebit's authenticity when they discovered that the photos of the team members were fake. Soon after the allegations were brought up, the scammers exited with estimated funds of $2.7 to $4 million before ever even bringing their novel cryptocurrency idea to the market (Kean, 2018). A cryptocurrency by the name of Opair has a very similar story. A mysterious developer who went by Wasserman offered a cryptocurrency that supposedly would act as a sort of "decentralized debit card system using its own token, XPO" (Kean, 2018). The cryptocurrency brought in an estimated $2.9 million before the fraudsters exited with all the funds after investors noticed that the

team's LinkedIn profiles were fake. To date, nobody knows the true identity of Wasserman, or where the money from Opair has gone to (Kean, 2018). Not all exit schemes have to be as elaborate as the previous examples do. Probably the most ridiculous exit scheme was perpetrated by the ironically named PonziCoin. PonziCoin raised over $250,000 before the perpetrator vanished with the funds. Apparently, the cryptocurrency openly marketed itself as a scam, however, gullible investors were still drawn to invest money into what they must have thought was a legitimate cryptocurrency (Kean, 2018). With the ever-increasing amount of exit schemes that are uncovered every day, prospective crypto-investors must remain careful to research the legitimacy of these cryptocurrencies and businesses now more than ever.

Pump and dump schemes have been around for ages and have proven to be fairly lucrative schemes for fraudsters to perpetrate. According to Investopedia, pump and dump schemes can be defined as a fraud "that attempts to boost the price of a stock through recommendations based on false, misleading or greatly exaggerated statements" (Investopedia, 2018). In other words, fraudsters will pump up the price by buying substantial amounts of the stock as well as propagating fake news through fake celebrity tweets or fake articles to entice others to help them inflate the price of the security, then dump it all in one single coordinated effort to make a profit. This may seem like a victimless crime, but one must consider the amount that investors who are purchasing the 'dumped' securities are purchasing them at an artificially inflated price under the false pretenses of the scammers. These new investors will no doubt lose significant amounts to the scam. Pump and dump schemes have been popular ever since the 1920's and remain relevant today almost 100 years later. Fraudsters have now taken to perpetrating these

schemes with cryptocurrencies. Due to cryptocurrency's markets inherent qualities of volatility and unpredictability, crypto-investors' extreme fear of missing out on the next big cryptocurrency as well as the ability to remain completely anonymous using the internet, pump and dump perpetrators have found it relatively easy to make a quick profit off budding cryptocurrencies. Usually these scams are started by only one or a handful of people. These 'investment groups' (as many pump and dump groups like to refer to themselves) coordinate their efforts through anonymous messaging apps such as Discord and Telegram and recruit new members through means of shameless social media advertising and member recruitment. Recruitment is vital to the success of these pump and dump schemes since the biggest contributing factor to how much the price of the cryptocurrency can be inflated is based solely on how many coins are bought up by how many investors. Members are enticed to recruit new members with the incentive of being promoted to higher ranks within the group based on how many new members that they have invited. The advantages of being of a higher rank means that you will get anywhere 0.5 to a 3.5 second earlier notification when to dump your coins to get a higher return on an investment since you will be selling before a majority of the group does. This means that the higher rank you are within the group, the better opportunity you will have to make the highest possible profit. However, this logic backfires for most of the members, in effect, scamming the scammers. Only the top of the group sees any real profit while the ones who lost are left to rationalize their loss based on the assumption that they simply sold too late (Martineau, 2018). As these scams have become more and more popular over the past couple years, the government has decided to step in to try to regulate them. The Commodity Futures Trading Commission has announced that they

will focus on “detecting and deterring fraudulent activities, such as pump and dump schemes, while not stifling early innovation in the crypto space” (CFTC, 2017). The CFTC and SEC can prosecute pump and dump schemes under the Securities Act of 1933 (SEC, 2017). However, due to the anonymity of the message groups, it is hard to discern who is involved in these schemes. This is the reason for the CFTC offering rewards of $100,000 or up to 30% of the sanctions recuperated by the fraudsters for whistleblowers who expose the heads of these pump and dump schemes (Crypto Insider, 2018).

In addition to the aforementioned schemes that can be committed with cryptocurrencies, there are a few schemes that I have categorized simply as ‘cryptocurrency theft’. Due to the inherent nature of cryptocurrencies being a virtual currency, hackers have attempted to relieve unsuspecting investors of their cryptocurrencies for years. I have chosen to categorize the following frauds as cryptocurrency theft since they all involve some sort of perpetrator stealing cryptocurrencies from an unsuspecting holder. Most financially literate individuals will be familiar with the infamous ‘Nigerian Prince’ or 419 fraud (labeled 419 due to the section of Nigerian law that makes it illegal). This scheme is a type of advance fee scheme that involves a scam artist, stereotypically from Nigeria, that entices someone to wire him or her a small sum of money in order to clear a large sum in which the scammer claims can be split between both the con-man and the conned. However, all these stories are fictitious, and the investor usually never sees any of their investment ever again. These scammers are now perpetrating these same 419 scams, but now with cryptocurrencies. In addition to scamming citizens abroad such as us in America, these Nigerian scammers have also taken to scamming their own countrymen. The goal is to

convince unsuspecting Nigerians to wire over naira; the local, Nigerian currency, for phony cryptocurrencies such as ‘billion coin’ (McDonnell, 2018). In addition to these crypto-Nigerian schemes, hackers have also become prevalent threats to the security of investors’ cryptocurrencies. These hackers will use many different tactics to steal cryptocurrencies. Despite the many safeguards that blockchain technology can offer to help protect investors from hackers, they still manage to steal cryptocurrencies every day. One man in a suburb of Los Angeles lost his life savings to crypto-hackers. Chris Dejrit lost over $22,000 to hackers posing as technicians for the exchange that he was using. The requested that Dejrit give them his personal logins so that they could fix some bugs in his profile. The next time Dejrit logged in, he noticed that his entire stash of Bitcoin was gone without a trace (CBS Los Angeles, 2017). Another type of cryptocurrency theft that has become more and more popular over the past couple years are ransomware schemes. These schemes have caught the entire crypto-world off guard. Fraudsters perpetrate these schemes by utilizing ransomware to take over people’s computers and vow only to unlock them once a payment of untraceable cryptocurrency has been made to the fraudster’s e-wallet. In 2015, it was estimated that CryptoWall, a specific type of ransomware virus, made off with over $18 million worth of cryptocurrencies (THE DATA TEAM, 2017). Ransomware, another prominent ransomware virus, also swept across Europe in May of 2017 causing considerable damage to all those affected. The impact was so great that many European legislators attempted to make cryptocurrencies illegal so that scams such as Ransomware would not be allowed to persist (Coleman, 2017). However, the most egregious cryptocurrency thefts that the world of cryptocurrency has ever seen would have to be the hacks of Mt. Gox and Bitfinex. Mt.

Gox and Bitfinex are both what the cryptocurrency community refers to as exchanges. A cryptocurrency exchange acts as a market place where cryptocurrencies can be stored and traded. These exchanges hold massive amounts of the world's cryptocurrencies and are trusted by their customers to provide a safe trading environment. Mt. Gox was not hacked once, but twice. The first hack occurred in 2011 when the hacker gained access to the exchange by using an auditor's credentials that were supposed to be kept confidential. The first hack made off with 2,609 Bitcoins, a miniscule amount compared to what was lost during the second hack. The second hack, which occurred in 2014, relieved Mt. Gox of 750,000 Bitcoins which is the equivalent to around $350 million, an amount equal to over 70% of Bitcoins in circulation at the time. With the second hack, all of Mt. Gox's customers had lost all faith in the company, and it filed for bankruptcy shortly afterwards (Khatwani, 2017). Along with the Mt. Gox hack, hackers were also able to do comparable damage to the Bitfinex exchange. Hackers were able to exploit a weakness in Bitfinex's authentication controls and steal 120,000 Bitcoins from investors making it the second biggest cryptocurrency theft since Mt. Gox (Khatwani, 2017). Along with Mt. Gox and Bitfinex, other popular exchanges such as Bitfloor, Poloniex and Bitstamp, rendering the aforementioned examples to not be isolated incidents (Khatwani, 2017). It is important to note that all the hacks were made possible due to negligence or oversight by those in charge of the exchanges and not simply investor error such as some other examples mentioned earlier.

Works Cited

(55), cryptick, et al. “BitConnect Scam: How Many People Are Involved? Post 4 - Steemit.” - *Steemit*, steemit.com/bitconnect/@cryptick/bitconnect-scam-how-many-people-are-involved-post-4.

“Bitfinex & Tether Fraud Mismanagement – What Is USDT All About?” *BitcoinExchangeGuide*, 14 Dec. 2017, bitcoinexchangeguide.com/bitfinex-tether-fraud-mismanagement/.

Bitfinexed. “Bitfinex Never 'Repaid' Their Tokens, Bitfinex Started a Ponzi Scheme.” *Medium*, Augmenting Humanity, 28 Oct. 2017, medium.com/@bitfinexed/bitfinex-never-repaid-their-tokens-bitfinex-started-a-ponzi-scheme-86a9291add29.

Buntinx, JP. “The BitConnect Ponzi Scheme Has Finally Collapsed as Exit Scam Becomes Evident.” *NewsBTC*, 26 Mar. 2018, www.newsbtc.com/2018/01/17/bitconnect-ponzi-scheme-finally-collapsed-exit-scam-becomes-evident/.

CBS Los Angeles, director. *Local Man Loses $22,000 In Cryptocurrency Scam. YouTube*, YouTube, 2017, www.youtube.com/watch?reload=9.

Cheng, Evelyn. “Staten Island-Based 'CabbageTech' Charged with Bitcoin-Related Fraud after Promising 300% Returns in a Week.” *CNBC*, CNBC, 19 Jan. 2018, www.cnbc.com/2018/01/19/us-regulator-charges-cabbagetech-with-bitcoin-related-fraud.html.

Coleman, Frederick. “The Dark Side of Bitcoin: Illegal Activities, Fraud, and Bitcoin.” *Blockonomics Blog*, Blockonomics Blog, 16 June 2017, blog.blockonomics.co/the-dark-side-of-bitcoin-illegal-activities-fraud-and-bitcoin-360e83408a32.

Crypto Insider. “CFTC Offers $100,000+ Bounty for Crypto Pump and Dump Whistleblowers.” *Crypto Insider*, 19 Feb. 2018, cryptoinsider.21mil.com/cftc-offers-bounty-on-crypto-pump-dump-whistleblowers/.

Crypto Investor, director. *Is Tether Committing Fraud? YouTube*, YouTube, 10 Sept. 2017, www.youtube.com/watch?v=6Qo61zxrVOU.

Investopedia. “Pump And Dump.” *Investopedia*, Investopedia, 27 June 2018, www.investopedia.com/terms/p/pumpanddump.asp.

Jenkinson, Gareth. “Bitconnect Ponzi Scheme - No Sympathy From Crypto Community.” *Cointelegraph*, Cointelegraph, 3 July 2018, cointelegraph.com/news/bitconnect-ponzi-scheme-no-sympathy-from-crypto-community.

Kean, Brian. “Don't Believe the Hype. Five Largest ICO ‘Exit Scams’: Expert Take.” *Cointelegraph*, Cointelegraph, 3 July 2018, cointelegraph.com/news/dont-believe-the-hype-the-five-largest-ico-exit-scams-expert-take.

Kharpal, Arjun. “Mysterious Cryptocurrency Scammers Ran off with More than $2 Million after Ditching Their Investors.” *CNBC*, CNBC, 12 Mar. 2018, www.cnbc.com/2018/03/09/cryptocurrency-scammers-of-giza-make-off-with-2-million-after-ico.html.

Khatwani, Sudhir. “Top 5 Biggest Bitcoin Hacks Ever.” *CoinSutra - Bitcoin Community*, 21 Nov. 2017, coinsutra.com/biggest-bitcoin-hacks/.

Lee, Timothy B. “Feds Shut down Allegedly Fraudulent Cryptocurrency Offering.” *Ars Technica*, Ars Technica, 4 Dec. 2017, arstechnica.com/tech-policy/2017/12/feds-shut-down-allegedly-fraudulent-cryptocurrency-offering/.

Levine, Matt. “SEC Halts a Silly Initial Coin Offering.” *Bloomberg.com*, Bloomberg, 5 Dec. 2017, www.bloomberg.com/view/articles/2017-12-05/sec-halts-a-silly-initial-coin-offering.

Liao, Shannon. “The SEC Created Its Own Scammy ICO to Teach Investors a Lesson.” *The Verge*, The Verge, 16 May 2018, www.theverge.com/tldr/2018/5/16/17361750/sec-cryptocurrency-ico-investors.

Martineau, Paris. “Inside the Group Chats Where People Pump and Dump Cryptocurrency.” *The Outline*, The Outline, 23 Jan. 2018, theoutline.com/post/3074/inside-the-group-chats-where-people-pump-and-dump-cryptocurrency?zd=5.

McDonnell, Tim. “How Nigerians Beat Bitcoin Scams.” *Bloomberg.com*, Bloomberg, 22 Jan. 2018, www.bloomberg.com/news/articles/2018-01-22/how-nigerians-beat-bitcoin-scams.

Mix. “Cryptocurrency Startup LoopX Pulls Exit Scam after Raising $4.5M in ICO.” *The Next Web*, 12 Feb. 2018, thenextweb.com/hardfork/2018/02/12/cryptocurrency-loopx-scam-ico/.

Morris, David Z. “The SEC Filed Fraud Charges Against 2 Bitcoin-Inspired ICOs.” *Fortune*, Fortune, 2017, fortune.com/2017/10/01/sec-ico-fraud-charges/.

“PRE-ICO SALE IS LIVE.” *HoweyCoins*, 2018, www.howeycoins.com/index.html.

“REcoin: The First Ever Cryptocurrency Backed by Real Estate, Confirms Token Pre-Sale and ICO Launch Dates.” *PR Newswire: News Distribution, Targeting and Monitoring*, PRNewswire, www.prnewswire.com/news-releases/recoin-the-first-ever-cryptocurrency-backed-by-real-estate-confirms-token-pre-sale-and-ico-launch-dates-300487074.html.

Seth, Shobhit. “What's a Cryptocurrency Exit Scam? How Do You Spot One?” *Investopedia*, Investopedia, 23 Mar. 2018, www.investopedia.com/tech/whats-cryptocurrency-exit-scam-how-spot-one.

Seth, Shobhit. “$9 Million Lost Each Day In Cryptocurrency Scams.” Investopedia, Investopedia, 13 Mar. 2018, www.investopedia.com/news/beware-9m-are-lost-each-day-crypto-scams/.

“Tether (USDT) Price, Charts, Market Cap, and Other Metrics.” *CoinMarketCap*, 2018, coinmarketcap.com/currencies/tether/.

THE DATA TEAM. “Ransomware Attacks Were on the Rise, Even before the Latest Episode.” *The Economist*, The Economist Newspaper, 15 May 2017, www.economist.com/graphic-detail/2017/05/15/ransomware-attacks-were-on-the-rise-even-before-the-latest-episode.

"The Laws That Govern the Securities Industry." *SEC.gov*, 1 Oct. 2013, www.sec.gov/answers/about-lawsshtml.html.

U.S. Commodity Futures Trading Commission. *Customer Advisory: Beware Virtual Currency Pump-and Dump Schemes* . www.cftc.gov/sites/default/files/idc/groups/public/@customerprotection/documents/file/customeradvisory_pumpdump0218.pdf.

Zhu, Julie, and Shu Zhang. "China to Use Cornerstones to Help Alibaba, Xiaomi List in Mainland:..." *Reuters*, Thomson Reuters, 25 May 2018, www.reuters.com/article/us-china-cdr/china-to-use-cornerstones-to-help-alibaba-xiaomi-list-in-mainland-sources-idUSKCN1IQ10R.

Appendix

Fig. A

Questions	% Correct	% Wrong
1	49%	51%
2	18%	82%
3	43%	57%
4	19%	81%
5	50%	50%
6	78%	22%
7	55%	45%
8	44%	56%
Bitcoin	94%	6%
Dogecoin	74%	26%
Ethereum	20%	80%
Vadarcoin	84%	16%
Poppycoin	83%	17%
Ripple	26%	74%
Dash	14%	86%
Ponzicoin	19%	81%
NYSNC	90%	10%
Bernina	97%	3%
Janone	97%	3%
Quartzcoin	78%	22%
Saluki	97%	3%
NEM	13%	87%
***# of Participants:	125	

***Hi-lighted percentages in the '% Correct' column go to prove my hypothesis because they signify that the majority of the students answered the question incorrectly.

Fig B

Total % of Questions Where the Majority Answered Correctly:		
50.00%		

***Since the students answered less than a majority (for the purposes of this research; 50.01%) of the answers correctly, the hypothesis has been proven correct.

Fig C.

Cryptocurrency Fraud Perceptions

1. On a scale of 1-7, do you consider investing in cryptocurrencies to be a risky (1) or safe (7) venture, relative to other investments such as the stocks or bonds?

2. On a scale of 1-7, how familiar would you consider yourself on the subject such as cryptocurrencies such as Bitcoin? 7 being very familiar, 1 being not familiar at all.

Explanation: You are being administered this survey as a means of gauging a specific population's grasp on financial frauds, specifically those than can be committed using cryptocurrencies. Please respond as truthfully as possible to the following questions concerning cryptocurrency fraud.

3. A Ponzi scheme is a fraud in which…
   A. ***New investor's funds are used to pay off old investor's funds giving the illusion of a legitimate business.
   B. A thief steals investments by first laundering the money through a bank or other reputable financial institution.
   C. A fraudster sets up a fake online business which will take orders, but never deliver on any of the products.
   D. A fraudster sets up off shore accounts in which money from illegal sources can be wired to safely.
4. The term I.C.O. stands for…
   A. International Currency Organization
   B. International Currency Omission
   C. ***Initial Coin Offering
   D. Intermodal Communication Organization
5. An Exit Scheme occurs when…
   A. A fraudster leaves the country after committing a fraud.

B. A fraudster deletes all internet presence after committing a fraud.
C. ***A fraudster takes all funds invested into a venture, wires them to different accounts and ceases all business activities.
D. A fraudster wipes all hard drives in a business of all financial data, then exits the business with all current funds leaving behind no trace.

6. 'Pump and Dump' schemes occur when…
   A. Funds are dumped into a secure account in which a fraudster can make off with the entire account in one fell swoop.
   B. Funds are pumped into a shell company which in turn can be dumped into an account of the fraudsters choosing which will allow the fraudster to easily steal the funds.
   C. A group of fraudsters share private keys for crypto-wallets in order to build up enough of a single cryptocurrency to fraudulently invest in a fledgling business, then steal the funds later on down the line.
   D. ***A group of fraudsters band together to buy large quantities of a cryptocurrency or stock at one time, then sell it at the inflated price at a specified time in order to make a profit.
7. True of False. You can store your Bitcoins offline in a hard drive.
   A. ***True
   B. False
8. True or False. It is impossible for a hacker to steal your Bitcoins even if they have your access to your computer because you need a wallet id number to access cryptocurrencies.
   A. True
   B. ***False
9. True or False. Cryptocurrencies are backed up to a certain extent by the U.S. Federal Reserve.
   A. True
   B. ***False
10. True or False, the S.E.C. cannot prosecute any supposed crimes committed with cryptocurrencies because they do not qualify as a regulated currency.
    A. True
    B. ***False
11. Please indicate which of the following are Crytocurrencies.
    Bitcoin***
    Dogecoin
    Ethereum***
    Vadarcoin
    Poppycoin
    Ripple***
    Dash***
    Ponzicoin***
    NYSNC

Bernina
Janone
Quartzcoin
Saluki
NEM***
-Correct answers are marked with ***.