12-14-2021

Old Frauds With a New Sauce: Digital Assets and Space Transition

Deborah Smith
Cleveland State University, d.l.smith11@csuohio.edu

Publisher's Statement

Dupuis, D., Smith, D. and Gleason, K. (2021), "Old frauds with a new sauce: digital assets and space transition", Journal of Financial Crime, Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/JFC-11-2021-0242

Old frauds with a new sauce: digital assets and space transition

Daniel Dupuis
Department of Finance, School of Business Administration, American University of Sharjah, Sharjah, United Arab Emirates

Deborah Smith
Department of Accounting, Monte Ahuja College of Business, Cleveland State University, Cleveland, Ohio, USA, and

Kimberly Gleason
Department of Finance, School of Business Administration, American University of Sharjah, Sharjah, United Arab Emirates

Abstract

Purpose – The purpose of this study is to describe the evolution of fraud schemes with historically conducted with fiat money in physical space to the crypto-assets in digital space as follows: ransomware, price manipulation, pump and dump schemes, misrepresentation, spoofing and Ponzi Schemes. To explain how fraud schemes have evolved alongside digital asset markets, this study applies the space transition theory.

Design/methodology/approach – The methodology used is a review of the media regarding six digital asset fraud schemes that have evolved from physical space to virtual space that are currently operational, as well as a review of the literature regarding the space transition theory.

Findings – This paper finds that the digital space and digital assets may facilitate pseudonymous criminal behavior in the present regulatory environment.

Research limitations/implications – The field is rapidly evolving, however this study finds that the conversion from physical to virtual space obfuscates the criminal activity, facilitating anonymity of the perpetrators, and creating new challenges for the legal and regulatory environment.

Practical implications – This paper finds that the digital space and digital assets may facilitate pseudonymous criminal behavior in the present regulatory environment. An understanding of the six crypto-asset fraud schemes described in the paper is useful for anti-financial crime professionals and regulators focusing on deterrence.

Social implications – The space transition theory offers an explanation for why digital space leads criminals to be better positioned to conduct financial crime in virtual space relative to physical space. This offers insights into behavior of digital asset fraudster behavior that could help limit the social damage caused by crypto-asset fraud.

Originality/value – To the authors' knowledge, this paper is the first to detail the evolution of fraud schemes with fiat money in physical space to their corresponding schemes with digital assets in physical space. This study is also the first to integrate the space transition theory into an analysis of digital asset fraud schemes.

Keywords Financial crime, Fraud, Cryptocurrency, Digital assets, Space transition theory

Paper type Research paper

1. Introduction

Like crows captivated by shiny objects, it is difficult for many individuals to look away when a new, innovative fraud scheme presents itself. With individuals quarantined at home and bored, surfing the web for stimulation and uncertain economic conditions setting

financial criminals on the prowl, fraud schemes have proliferated during the COVID-19 pandemic. Partly due to an increase in online time and the meteoric rise in social media attention, crypto-scams have taken flight. Brooks (2021) notes that between October 2020 and June 2021, Americans have lost $80m in cryptocurrency fraud schemes and the Federal Trade Commission (FTC) reports that they received over 7,000 complaints from consumers regarding crypto-investment scams.

A largely uninformed public and new technology, driven by social media influencers and high media visibility, creates an amenable environment for the evolution of new fraud schemes. In this paper, we integrate the fraud triangle theory with the space transition theory to describe the evolution of traditional fraud schemes committed in physical space to digital asset schemes that operate in digital space. We also address six currently operational crypto-based or crypto-enabled fraud schemes that are based on historic fraud schemes: ransomware, price manipulation, fraudulent disclosures, pump and dump schemes, Ponzi schemes and spoof sites and fake apps. We conclude with implications for regulators and anti-financial crime professionals.

2. Space transition theory the nature of digital assets

2.1 The nature of cryptocurrency and the space transition theory

By some estimates, cryptocurrency could replace up to one-fourth of national currency within a decade (Samejo *et al.*, 2018), and at the same time, Kethineni and Cao (2020) state the cryptomining attacks increased over one thousand percent in early 2018. Rob Wright, of Europol, estimates that billions of dollars of criminal money is laundered annually with cryptocurrency (Kethineni and Cao, 2020).

The problem is that the same features that make cryptocurrency appealing to the public at large make it useful for crime (Potgieter and Howell, 2021). Cryptocurrency provides a new opportunity to facilitate extant financial crime schemes, including Ponzi schemes, randsomeware (Kethineni and Cao, 2020), price manipulation and "pump and dump" projects (Cengiz, 2021). Low barriers to entry make it easy for criminals to elevate existing fraud schemes with digital assets (Kethineni and Cao, 2020). Further, digital coin transactions are instantaneous and irrevocable, and as the currency is portable, criminals can take advantage of international transferability (Kethineni and Cao, 2020).

While the borderless nature and nonreliance on central authorities facilitates commercial freedom, international anonymity creates opportunity for fraudsters. The blockchain ledger associated with cryptocurrency provides an audit trail, but digital coins are typically stored under encryption with private keys (Houben and Snyers, 2018). Because the ownership is in the form of a cryptographic key rather than personal identification, the participants are anonymous. Another reason that cryptocurrency is more anonymous than cash is the lack of an intermediary, such as a bank or financial institution, making it difficult, if not impossible, to require disclosures (Potgieter and Howell, 2021). Kethineni and Cao (2020) point out that cryptocurrencies enhance the opportunity for crime and extend crime in the virtual world to the real world, a concept that aligns with space-transition theory of crime (Jaishankar, 2008). Criminals are lured by the anonymity, security and the difficulty of tracing activity (Kethineni and Cao, 2020).

Cressey's (1953) fraud triangle theory can be integrated with a relatively new paradigm from the criminology discipline, the space transition theory (Jaishankar, 2008), to explain the transferability of fraud schemes from the physical space to the virtual space in which digital coins and their markets reside. The fraud triangle theory (Cressey, 1953) posits that three factors are required for fraud to occur:

(1) a nonshareable pressure or motivation;

(2) the ability to reconcile the cognitive dissonance arising from criminal activity with one's value system; and

(3) the opportunity to commit the fraud.

Integrating these two perspectives provides insights on the evolution of frauds in the physical space have transitioned to the digital space. Jaishankar (2008) developed the space transition theory to explain how the barriers to crimes once committed in physical space have less deterrence value in cyberspace. By using cryptocurrency rather than a government-sanctioned currency, criminals further shift crimes that are virtual or physical by adding anonymity and means of escape.

The idea behind Jaishankar's (2008) theory is that "people behave differently when they move from one space to another." Below, we summarize the main components of the space transition theory and integrate them with the fraud triangle factors:

- Persons with repressed criminal behavior (in the physical space) have a propensity to commit crime in cyberspace, which they would not otherwise *t* commit in physical space. While the nonshareable pressures that drive fraud in physical space still exist (desire to maintain status, position and reputational capital), individuals have a stronger behavioral propensity to operationalize fraud in the crypto-realm, including fraud with digital assets.
- Identity flexibility, dissociative anonymity and lack of deterrence in cyberspace provide the opportunity to commit cyber-crime and the ability to rationalize cybercrime, including digital asset fraud.
- The criminal behavior of offenders in cyberspace is likely to be imported to physical space which, and criminal behaviors in physical space may be exported to cyberspace as well; the fraud skills a fraudster has developed in the physical space can be transferred to the digital asset realm easily with the added perceived benefit of anonymity.
- The intermittent nature of offenders' ventures into the realm of cyberspace and the dynamic spatio-temporal nature of cyberspace offer the chance to quickly jump in and out between physical and cyberspaces, enhancing the ability to evade detection, which can make frauds with digital coins more lucrative than corresponding fraud schemes in the physical realm.
- Strangers are more likely to unite together in cyberspace to commit crime in the physical space. Associates of criminals in physical space are likely to unite to commit crime in cyberspace. Consequently, the opportunity exists for the establishment of networking to obtain the requisite technologies to facilitate digital assets schemes and to increase the scale and scope of digital asset frauds relative to fraud in the physical realm.
- Persons from closed societies are more likely to commit crimes in cyberspace than persons from open societies; this generates a greater opportunity through enhanced access to an expanded market for fraud and through which to disseminate information.
- The conflict of norms and values of physical space with the norms and values of cyberspace may lead to the ability to rationalize cyber-crimes (Jaishankar, 2008). Digital asset fraud schemes may be more lucrative than physical space fraud

schemes simply because fraudsters are more able to distance their physical persona from their crypto-persona.

The first two postulates of Jaishankar's (2008) theory are associated with anonymity. Virtual space provides anonymity to persons who might otherwise avoid crime due to personal status or position. Anonymity provides a flexible identity. The use of cryptocurrency improves the anonymity of the virtual space in which criminals operate.

Jaishankar's (2008) third postulate states that offenses from the physical are transferred to the cyberspace, and vice versa. Following that logic, cryptocurrency adds a new dimension to either the physical or the virtual world of criminal activity. Crimes with physical currency, whether associated with physical- or cyber-crime, can be transferred to cryptocurrency. Jaishankar's (2008) theory is designed to apply to the transition from one space to another, and cryptocurrency moves the means of compensation to a virtually unregulated, non-physical currency that can facilitate crime in either the physical or virtual space.

The fourth postulate states that cyberspace, compared to the physical space, improves the fraudster's odds of escape. Cryptocurrency increases the chance of evading authorities by adding elements of complexity. Law enforcement must keep pace with a variety of forms and processes for using cryptocurrency. There is a wide variety of digital currency, and the industry continues to grow. Some currencies are more regulated than others and the jurisdictions are disassociated, therefore complicating the determination of enforcement authority. Furthermore, cryptocurrency makes it easier for offenders to share compensation among persons in different countries.

Assarut *et al.* (2019) conduct a survey study and determine that cybercrime is facilitated by freedom and anonymity. They explain that the constant, easy access to social media has changed people's attitudes. Freedom and anonymity are also facilitated with cryptocurrencies. The use of cryptocurrency provides another layer of anonymity to a criminal transaction, weak regulatory authority reduces the likelihood of being caught, and the lack of country-level jurisdictional control of the currency provides freedom of access.

Felson and Clarke (1998) make the argument that the source of crime is rooted in opportunity. Cryptocurrency creates opportunity if fraudsters perceive a lower risk of identification or prosecution. Furthermore, the speed and easy access to cryptocurrency may increase the anticipated certainty and the amount of payoff from the crime. Collection is not subject to monetary institutions that operate during the business week and depending on the country where the criminal resides, there may be advantages based on the wide range of collection choices in multiple digital assets.

2.2 Challenges to regulation and enforcement

The space transition theory provides a framework through which the transition of fraudulent activity from the physical markets to the digital asset markets is highly lucrative in the criminal's perspective. The relatively undeveloped regulatory environment surrounding digital assets presents another opportunity factor for fraudsters relative to the physical space.

Because of the active evolution of digital asset markets, to be effective, regulators require an in-depth understanding of the rapidly developing underlying technologies. Thus, it is understandable that law enforcement has "not kept pace with the sophistication of emerging cybercrime (Kohnke *et al.*, 2021)." According to Potgieter and Howell (2021), regulatory agencies lack the inside knowledge of dynamic cryptocurrencies and are "ill-equipped to govern these institutions." Korver *et al.* (2019) advises prosecutors to be careful with online research because they may reveal their identity. Yet, law enforcement is working to improve

technology and training. The blockchain that cryptocurrency relies on can reveal transaction amounts, addresses, associated individuals. As criminals may use multiple web addresses, law enforcement uses software that clusters the addresses associated with the same owner (Korver *et al.*, 2019).

The international and regulatory boundaries of cryptocurrency create a jurisdictional challenge for authorities. For example, the IRS and the US Treasury Department in 2021 are seeking approval from Congress to expand authority related to cryptocurrency because of the international nature of the transactions (Sundaravelu, 2021). Former IRS director, Jorge Castro, says they did not think they had the authority to expand the reporting (Sundaravelu, 2021). Cryptocurrency is attractive to those seeking a decentralized monetary exchange and governance, but this means that authorities cannot aid victims of crime facilitated by cryptocurrency (Cengiz, 2021).

We next describe the evolution of six time-tested fraudulent schemes into the digital age.

3. Old recipes [. . .] with an irresistible new sauce

Hope springs eternal in the minds of many investors. Financial market manipulations and frauds are not new; sometimes it is outright theft, other times false expectations focusing on a target's greed and ignorance; for example, the internet bubble was driven by unrealistic expectations regarding new technology and excessive optimism. Accordingly, many crypto-scams, once again, are old frauds dressed up with new technology. While the tactics remain similar to past antics, digital coins provide a new payment conduit for lawbreakers who feel protected by a perceived anonymity. Dupuis and Gleason (2020) argue that, although many of the cryptographic transactions can be traced, some avenues still exist to launder illicit funds; the main variable remains the criminal's level of sophistication and the innate reactive nature of regulation. Given the potential payoff of crypto-fraud, criminals are learning quickly.

3.1 Ransomware

In recent years, there has been an explosion of media attention related to crypto ransoms, to the extent that government representatives are debating the subject in the US Senate and the daily news is replete with stories on the subject. Ransomware is a type of malware designed to deny access, encrypt or publish data, either private or public. A demand for money quickly follows the attack – pay up or lose access to your network/hard drive/system forever as infected devices become inoperable. While this is a nuisance for private users (who wants all their private pictures spread all over the internet?), the impact for home computers is localized. On the other hand, corporate targets face major downtime and high operating losses, so many of them choose to pay, but the price is rising. Hospitals, retail food processors and distributors, utilities, any business is fair game including municipal and governmental entities. This scam is not new, but it has recently been reinvigorated by the introduction of digital coins. Prior to the cryptographic era, ransoms had to be paid in fiat or through secretive tax haven accounts – dangerous, prone to failure and somewhat easier to trace. Hacker groups now supply their services to organized syndicates with expert financial management, customer service and IT support for victims (yes, they will help you set up a Bitcoin wallet to pay the ransom!). Dobby (2021) explains that they plan their attacks for months and can be extremely polite: "Good afternoon, we've stolen your corporate data. Please kindly connect with one of our customer service agents to arrange payment." These fraudsters favor Bitcoin as compensation and, to a lesser extent, Monero. Bitcoin transactions are traceable, but it is possible to muddle the tracks, while Monero trades still remain concealed [1].

Recent examples in the US include Colonial Pipeline, a major oil provider that had to shut down operations for a week in May 2021, driving fuel pump prices above $3 per gallon. The initial hack apparently originated from the careless handling of a user id/password that opened a backdoor to the system's private network. The attack has been attributed to an Eastern European group called "DarkSide," and the ransom was set (and paid!) at 75 BTC, roughly US$4m at the time (Morrison, 2021). Interestingly, the US Department of Justice was able to recover 64 BTC, but declined to reveal the method used – most likely, the transaction was traced by using software like Chainanalysis or Anchain.ai's CISO (Compliance, Investigation, Security, Operations), and "reverse hacking" was used to access the target wallet as the illicit actors were probably negligent in the security of their financial endeavors [2]. This is one of the very few cases with a relatively "happy ending," and most of the attacks favor the criminal element. The retail hacking of home computers warrants much smaller amounts (typically a few thousand dollars) but what is lost in size is gained in volume and lack of defense. Most individuals do not have the expertise necessary to protect/retrieve their data and reaching out to a web-based "angel" can compound the problem as fake recovery services abound; once they gain access to the victim's computer, the game starts anew. Social networks are not immune to hacking; the Instagram accounts of small business owners and private users were attacked in May 2021 by "foreign actors" reputed to be based in Turkey – the investigation continues. It is estimated that home and corporate ransoms totaled over US$$18bn in 2020.

3.2 Price manipulation

Business entities have been attempting to manipulate stock prices since the existence of markets, including accounting schemes such as "big bath" earnings management, leaked rumors; examples are not difficult to find. Fortunately, in the USA, the Securities Exchange Commission (SEC) and other regulatory bodies are watching, but they have focused primarily on stock and derivatives markets; crypto exchanges are just beginning to feel the heat. For example, in 2018, Elon Musk (Tesla Chairman) tweeted that he could take Tesla private at $420 per share, triggering an immediate reaction in stock value. The SEC argued that there was no factual basis for this statement and acted, and Musk had to step down as Chairman, agree to have all communications reviewed by a legal team prior to disclosure, and both (Tesla and Musk) were fined US$20m each. In June 2021, the SEC took further action, claiming that Musk failed to comply with the 2018 settlement – as we are writing this paper, the case continues. This example serves as a backdrop to the present scene featuring digital coins; anything goes [. . .]. The same Elon Musk has repeatedly moved crypto markets with a single tweet while accumulating cryptocurrency positions, with no repercussions or reprimand by any regulatory body. Of course, there is a major difference between Tesla and Bitcoin/Dogecoin; Musk is not the Chairman for those digital coins. He has no responsibility to implement corporate strategy and therefore no authority or insider control – he is simply an influencer like many others, devoid of responsibility – with a strong following. Ante (2021) shows that Bitcoin and Dogecoin experienced abnormal returns of 18.99% and 17.31% following Musk's comments on Twitter – an action that would result in swift admonishment if it was stock-related. As various governing bodies are still struggling with the mere definition of a crypto-asset, the regulatory response is presently muted and the party continues. In Musk's own words: "I pump, but I don't dump!" Social media networks are rife with examples of coin marketing, rumors, false reports and blatant advertising disguised as newscasts. It is the Wild West out there, investor beware.

Price manipulations in the digital age are not limited to social media. In a move reminiscent of the ".com bubble" of 2000, the company "Long Island Ice Tea" changed its

name to "Long Blockchain" in 2017 while maintaining its main product line (beverages) and claiming that it would diversify into [...] blockchain technology. The stock price immediately tripled. In 2019, the FBI opened an investigation into potential insider trading allegations in relation to the name change and the SEC delisted the stock in 2021. Once again, if the problem was related to stock markets, supervisory protocols would act efficiently – but the same cannot be said of the crypto world. This lack of control over virtual coin operations opens the door to our next topic: the "Pump and Dump."

3.3 Pump and dump

Kamps and Kleinberg (2018) trace pump schemes back to the South Sea Bubble from the early 1800s. They design a detection technique that relies on price anomaly over a defined window of time and merge the results with data on coins displaying a low market capitalization. The outcome is an identification system that positively flags potential ongoing schemes. Crypto "Pump and Dumps" lead to short-term bubbles, often drastically increasing prices within minutes, followed by a quick reversal (Li *et al.*, 2021). The digitization of assets has noticeably facilitated the task for schemers; increased speed, easy dissemination of fake news and a large audience are now the norm. Pumping asset prices through marketing and media presence dates back many centuries but a diligent stakeholder could always investigate the fundamental value of the asset. In that aspect, the pump and dump of virtual assets is somewhat more complicated to detect as the fair value of cryptocurrencies is difficult (or impossible, in the opinion of many) to assess and everyone believes they hit the jackpot when the coin price moves up. If this is a natural phenomenon due to a free-floating increase in demand (warranted or not) and a limited supply, it does not reside in the realm of frauds. Illicit actors are very astute at targeting the greed and gullibility of novice investors and empty promises of astounding returns are just that – promises. While we cannot expect all buyers to understand the efficient markets hypothesis (EMH), constant monthly returns of 10-15% *without* the associated risk are, simply put, impossible.

The digital "pump and dump" is a modernized version of the old "boiler room" fraud; first, buy the supply (as much as possible) of an illiquid, defunct (but listed) or stale asset. Second, pump the price through false news, media exposure, personality endorsement and pressurized sales tactics. In the old days, pumping required cold-calling target lists. It is much easier now with the extended reach of social networks – a few posts on chat rooms, a podcast from a known influencer and the marketing machine is activated; greed can do the rest. A common tactic is to highjack the comments section of crypto-related videos or discussions with feigned but convincing enthusiasm about a token or project:

> Good work, thank you, I love your broadcast. Can you please help me to decide about the $IDEA coin? They plan to make a public sale on (exchange name) after their amazingly successful private placement that was oversubscribed by $10M. Should I invest?

If the asset is a stock, a thorough fundamental analysis will quickly uncover the scam, but digital coins are peculiar as the intrinsic value tends to be subjective. Once the price of the coin increases, a psychological phenomenon is known as FOMO (fear of missing out) sets in and the path becomes parabolic – time for the "dump" part. The scam originators unload their position on unsuspecting victims at a substantial profit and the deed is done, leaving the more gullible targets holding a valueless asset. After the media onslaught ends, the price drops rapidly to a more sustainable (in-line with EMH expectations!) level, and late buyers can now experience regret.

The rapid growth of virtual assets has created a void that regulating bodies are slow to fill. For law enforcement to get involved, we need well-defined rules! In the absence of a legal framework, fraudsters are getting bolder: case-in-point, groups (yes, there are more than one) calling themselves "Crypto Calls." The premise is simple – they openly offer 6-h weekly pumps using various little-known coins [3]. They target followers on their Telegram channel and issue instructions as follows: first, wait for their signal. When it is sent, buy as many of the coin as possible, immediately. After five hours, when everyone "in the group" has made their purchase, the instigators will leverage the pump on social media thus inducing FOMO in the population at large. When the price is high, unload your coins and get rich at the expense of unsuspecting plebes! Simple, no? The following is a direct transcript of their promotional video:

> Welcome to Crypto Calls – a leading cryptocurrency pump group, where we skyrocket the value of coins for six hours at a time. To start, create an account on the CryptoPIA exchange and fund it with Bitcoin. For information on our weekly pumps including the name of the coin we are pumping, follow our Telegram channel. Once released, be sure to buy the coin as quickly as possible. When everyone in the group has purchased the coin, we will begin advertising it to other investors on social media: Twitter, Instagram, Youtube, Stocktwits and Telegram. Everyone is involved in marketing so we can achieve maximum profit. Throughout the six hours, you will see two or three major pumps powered by targeted marketing [. . .]. When it's time to sell our whole position about five hours into the pump, place your sell orders above market price. During the last hour, outside investors will fill the orders as they FOMO into the coin that we have increased in value by 1000 – 2000%. By the time the six hours is up, everyone in our group will have sold for profit [. . .].

Of course, the organizers are taking advantage of their followers. The promoters had already purchased the digital asset before releasing the call. Even if the advertising does not trigger a social media frenzy, the organizers profit when the members of the group start buying – and the last ones to the party are left holding the empty bag. Surprisingly, this scam is promoted openly, with impunity, over multiple channels. Other recent examples also include the "Dubai pump," where a false press release claimed that the Dubai authorities were officially endorsing the low-volume DubaiCoin, propelling the token from US$0.10 to US$1.50 (1,400%) in one week – all from a single "fake news" item. The government was quick to deny the allegations, and the price subsequently crashed 80% from its apex.

With the resurgence of digital pumps, the literature now focuses on detection. Nghiem *et al.* (2021) argue that they can predict the identity of a "pump and dump" target and estimate the highest trade price with a 6.1% margin of error. They use a neural network-based algorithm on market and social media signals to single out the coin under pressure and construct a model to evaluate the price peak. Nizzoli *et al.* (2020) investigate social media networks and find that 56% of Telegram messages originate from bots or suspended accounts and, vice-versa, 93% of Twitter bots messages revert to Telegram, promoting both "pump and dump" and Ponzi schemes. Hamrick *et al.* (2018) perform an analysis on a similar dataset (Telegram and Discord) and identify over 5,000 distinct pumps, enough to wonder if there are any real messages left on the platforms. If this research can be adapted into a commercially viable tool, there is hope of foiling pumping attempts. For now, detection software resides outside the reach of most traders, and investor education remains the main defense against most "pump and dump" schemes.

3.4 Misrepresentations and fraudulent disclosures

"Misrepresentation" refers to the falsification of declarations in financial statements, legal documents and promotional material. The fraud part becomes a question of intent (known

misrepresentation, a defining feature of fraud) – is management purposely altering the numbers/promises to obtain financial gain or simply neglecting to tell the whole story? Generally accepted accounting practices are well-defined and documented – multiple cases have been tried in court and resolved. Wells (2001) characterizes purposeful fraudulent omissions (from an accounting perspective) into five categories, namely, liability omissions, significant events, management fraud (even immaterial amounts), accounting changes and related party transactions. Gallo (2021) shows that the practice of false advertising reaches even peer-to-peer lending marketplaces; in 2021, the Securities Exchange Commission (SEC) and the Department of Justice (DOJ) charged LendingClub with wire fraud, false statements and covered conduct with the aim of increasing market share by facilitating the acceptance of sub-par borrowers. Remember the good old days of 2008 when manipulations were the exclusive domain of big banks?

While regulatory bodies are well-equipped to handle misrepresentations related to traditional assets, the digital wave has created a completely new landscape for wrongful disclosures; ICOs (initial coin offerings), cryptocurrencies, cloud mining and NFTs (non-fungible tokens) are the new playground for illicit actors committing "oversights" (deliberate or not) and, in some cases, clear scams. Dupuis *et al.* (2021) argue that the present accounting/auditing standards need to adapt to the virtual era; they further highlight potential fraud risk factors tied to virtual assets and propose improvements for the education of future auditors. Many misrepresentations do not involve accounting principles but simply public statements that deviate from the truth, particularly when firms try to lure investors. Of course, most schemes described in this study include falsification in one form or another, but in some instances, the intent is real as opposed to a complete fraud; the devil is in the details [. . .] and their disclosure or promotion.

Even as the US legal and regulatory framework is developing, numerous governing bodies like the SEC, the DOJ, Commodities Futures Trading Commission, the Treasury Department, etc. are jousting for a piece of the pie and pursuing fraud cases – but the jurisdiction of each still remains unclear. In May 2021, the US Supreme Court ruled that the FTC did not have the authority to "obtain restitution" in the case of one of the cryptocurrency scam reports it received – and there were 7,000 other cases in the year 2020 [4]. Under existing laws, the demarcation between state and federal mandates is still ambivalent. The legal ramifications are beyond the scope of this study but, for illustration purposes, we highlight a few recent cases ranging from mild but worrisome (i.e. Tether) to failed attempts (DeFi Money Market) and outright cons (Bitcoiin2Gen, DeFi100, etc.).

Tether is advertised as a "stablecoin." By definition, each Tether coin is supposed to be backed by a US dollar in reserve. Tether Ltd. Is controlled by iFinex, the owner of Bitfinex, a crypto exchange. First issued in 2014, the coin was traded on Bitfinex as early as 2015 and mainstream adoption quickly ensued for valid reasons; the off-ramp between digital coins and fiat currency is cumbersome, costly and slow. If Tether really represents a US dollar, transactions in the crypto-space are greatly simplified. There has been rampant speculation that this stablecoin was used to manipulate Bitcoin prices (print "unbacked" Tether to buy BTC) as posited by Griffin and Shams (2020); their findings show that "purchases with Tether [. . .] result with sizable increases in Bitcoin prices [. . .] consistent with the supply-based hypothesis of unbacked digital money inflating cryptocurrency prices" thus contradicting Wang (2018), who disagrees and argues that "Tether grants did not Granger-cause Bitcoin returns."

The coin issuer, iFinex, is in full control of the supply and the only representation the firm makes is that Tether is pegged to, and fully backed by, USD on a ratio of 1 for 1. In a twist of events, iFinex's relationship with its auditor, Friedman LLP, was dissolved in

January 2018. The auditor's report for 2017 showed full compliance, but the same cannot be said of 2018 as the findings were never released. In 2019, the New York office of the Attorney General (OAG) filed a legal petition against Tether's issuers, not because of misrepresentation, but due to shady dealings concerning the cover-up of a US$850m loss (Keroles, 2021). The OAG concluded that, as of November 2018, Tether was not backed by fiat USD. The case was settled in 2021; Bitfinex and Tether, with no admission of guilt, agreed to pay US$18.5m in penalties and to discontinue any business activities with New York entities. Since then, Tether has updated its webpage as it now reads:

> Every Tether token is always 100% backed by our reserves, which include traditional currency and cash equivalents and, from time to time, may include other assets and receivables from loans made by Tether to third parties, which may include affiliated entities [. . .] [5].

The wording is now clearly different from the original. As the reserves include loans to affiliates, the notion of counterparty risk surfaces. In the event of a 2008-style meltdown, the domino effect from a potential default on loans could topple Tether with grave consequences for the crypto space. Recent reports have surfaced comparing a put option on the stablecoin to a credit-default swap; the bears are still on the hunt [6]. Strangely, the market seems to be oblivious to the danger as Tether presently has over US$62bn (August 2021) in circulation although competitors with a more stable profile like the Gemini Dollar and the USD Coin are gaining traction.

Coin projects sometimes straddle the line between failure and scam. Although the SEC makes liberal use of the "unregistered digital asset securities offering" all-encompassing accusation, the real fraud lies in the false claims made by the promoters. This is the case for a DeFi (decentralized finance) project called "DeFi Money Market" where Tokens were sold using smart contracts and promised a return of 6.25% based on collateralized car loans (Broderick, 2021). The volatility of digital assets caused the project's demise, but the promoters failed to inform the investors – hence the US$30m fraudulent misrepresentation. The perpetrators (corporation and individuals) were fined a total over US$13m for their actions.

Bitcoiin2Gen (B2G, notice the homoglyph? See Section 3.5) should belong to the category of fake ICOs because the coin never really existed, but prosecution was completed under the guise of multiple false statements – regardless of intent. B2G was promoted as a mineable coin, tradeable on the Ethereum blockchain through Start Options – the "largest Bitcoin exchange in euro volume and liquidity" and "consistently rated the best and most secure Bitcoin exchange by independent news media" (SEC, 2021); both statements are patently false. The case is still underway as of August 2021. If the demarcation between outright fraud and failure with good intentions is sometimes unclear, DeFi100 may fall on the wrong side of the line. On May 22, 2021, the project's website posted the following message:

> We scammed you guys and you can't do s*** about it. HA. All you moon bois have been scammed and you can't do s*** about it. (Broderick, 2021).

A little obvious, but we should thank the anonymous post for the clarification – the SEC's work would likely be facilitated by the comment. The owners of the project were quick to deny wrongdoing: "We never stole any funds," but decentralization implies little chance of the investors getting their money back. The promoters subsequently blamed the nefarious post on hackers and fake news, but the damage is done; the coin price is in freefall, from a height of US$3.30 to the present US$0.17. Incidentally, the project is still alive at the time of writing and no regulatory action has been reported.

To alleviate the likelihood of fraudulent misrepresentation, Krapels and Liebau (2021) proposes the "minimum disclosure requirements for cryptocurrency and utility token issuers," arguing that best practices should facilitate an efficient price discovery process.

They state that basic financial details must include, "token issuer information, initial and current cash positions, as well as token treasury information" while required non-financial data comprises contact info, open-source software and progress updates.

3.5 Spoof sites and fake apps

This type of scheme relies on the blind trust that users display when dealing in the virtual space. The scam perpetrators design an application (Android, Google, iOS, etc.) or a webpage that precisely replicates the legitimate site and then create a fraudulent link by changing one or two characters in the original web address. They distribute this false gateway through trojanized malware, grayware, social media marketing, and search engines, often temporarily displacing the real link in the search hierarchy. In 2019, the official "Google Play Store App" was found to include 27 malicious apps that replaced the complete official Play Store with a fake one, inundating the unsuspecting users with full-screen advertising every time an app is loaded. While this was a merchandising scam, the same principle applies to crypto-related sites with a more nefarious intent to steal your virtual wallet identification and passwords, thus gaining access to your coins. For example, if you use a hot (online) wallet and buy a new phone, you will automatically go to the app store and download the latest version of the wallet. Unbeknownst to you, the loaded app is fraudulent but looks exactly the same as the original. You then enter your user identification and password, thus giving away complete control of your virtual assets to the illicit agent running the scheme. Beware of external .apk (Android) or .ipa (iOS) applications that are not screened by third parties. Fake apps have been created to replicate Binance, Gemini, Kraken, TDBank, Bittrex, etc. As with ransomware attacks, the scammers are becoming more sophisticated, with real customer support who will be glad to help you transfer funds into the account for an eventual crypto purchase – only the money will never get there. In January 2021, over twelve fake wallet apps were listed in the Google Play Store: the popular wallet Exodus was listed under three different possible choices – two were spoofs. Figure 1 shows two possible downloads; the real one on the left and a scam on the right. The provenance of the app (Exodus Movement Inc. versus Exotax) might raise a warning flag for knowledgeable users but most beginners will not take notice.

The same *modus operandi* applies to websites, but they may be easier to spot: the link address will differ slightly from the original; this is also known as a "homoglyph attack" or "typosquatting." A simple Google search will highlight dozens of webpages with exhaustive lists of fake sites [7]. Sometimes, the difference can simply consist in a one-letter swap in the address (the number "1" instead of the letter "l" – yes, they look exactly the same) or a change in font from the original logo. For example, "deriibit.com" is a fraud domain

Source: https://bitcointalk.org/index.php?topic = 5308754.0

Figure 1.
Apps for the exodus wallet: real on the left and fake on the right

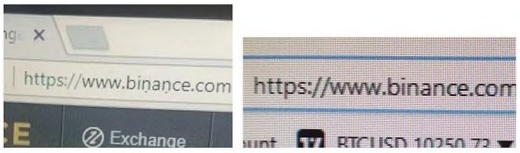
targeting the legitimate "deribit.com," "binonce.com" for "binance.com," etc. Figure 2 shows two different websites pretending to be Binance.com – can you tell the real from the scam?

Xia *et al.* (2020) identify 300 fake exchange apps and 1,595 scam domains. They contend that 60% are not identified as such, while 40.5% show up on at least one anti-virus engine [8]. In total, 323 fake applications targeted 38 exchanges, covering most, if not all of the major crypto platforms. The study shows that a large proportion of the fraudulent representations are controlled by a relatively small number of attackers and further discloses the Bitcoin blockchain addresses associated with the schemers, as well as their names, when available. The Poloniex exchange is the most "spoofed" with 35 fake apps and 45 fraudulent domains, while BitMax sits at the bottom of the list with only four scam applications. Though it is possible to track many of the impostor domains and apps, most novices will not be aware of the danger and investor education is the mainline of defense. Unfortunately, in line with the regulatory dialectic theory, new schemes are most likely under development as we write these lines.

3.6 Ponzi (pyramid) schemes

The origin of the term "Ponzi Scheme" dates back to 1919 and refers to Charles Ponzi, an Italian-American who swindled thousands of people out of approximately US$10m by promising a 50% return in 45 days. Although he caught the media's attention, he was not the first; Susan E. Howe (1879) and Warren Miller (1899), etc. preceded him, but the name stuck. Fast-forward to modern times, everyone has heard of Madoff; a US$64bn fraud with over 4,800 clients. The procedure is still the same: make a lofty promise about investment returns, use new clients' funds to pay profits to existing investors and skim off the top while the party lasts. By their nature, pyramid schemes cannot last; inflows must continuously accelerate to cover outflows, even when the reported amounts are fictitious, as some clients will sometimes insist on cashing out before the collapse. Why do people fall for these schemes? The answer generally lies in behavioral biases, but can simply be reduced to one word: greed – followed closely by pride and ignorance. The greed triggers the initial investment, ignorance fuels it, and pride prevents a timely exit or the dissemination of information. Even a superficial knowledge of the efficient market hypothesis (i.e. return is related to risk) could warn potential victims, but the swindle is still alive and well.

The digital age provides a new playground for fraudsters; the art of reheating an old scam with a new sauce. McGee and Conlon (2021) describe one of the most famous recent cases, OneCoin. A combination of Ponzi scheme, pump and dump and fake initial coin offering, OneCoin promoters claimed that it was a mined, decentralized and capped cryptocurrency, and it was touted as a "Bitcoin killer." Anyone searching a little further could have uncovered the fact that there was no blockchain and no active market for the coin



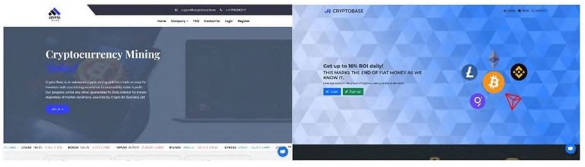
Source: https://www.reddit.com/r/CryptoCurrency/comments/7ykzar/be_careful_of_spoof_exchanges_would_you_have/

Figure 2.
Fake site versus the real one. Notice the dots below the "n"?

except the proprietary exchange Xcoinx – and you had to be a member (own the coin) to access it. It was promoted through webinars, roadshows and courses on cryptocurrencies – as part of a multi-level marketing strategy – and referrals were well-rewarded. The delivery method alone was enough to raise red flags, but in 2016 digital coins were the domain of dreams and fintech enthusiasts, mostly baffling to non-specialists. The main advocate of the scam disappeared in 2017 with US$4bn in investor money. Also straddling the fine line between fake ICO and pyramid scheme, BitConnect, released in 2016, was touted as a lending platform. Just convert your Bitcoins into BCC (BitConnect coins) on their proprietary platform and let the trading bot (another nice word for a black box) make miracles for you! Users were "promised" returns of 1% daily and the coin rose in value from US$0.17 to US $463.00 at its peak. The scheme was marketed through flamboyant influencers (i.e. Carlos Matos), multi-level marketing and word-of-mouth fueled by FOMO. In October 2017, regulators from Texas and North Carolina issued a cease and desist order that led to the closure of the lending platform and exchange. Other similar examples include PayCoin, PlusToken, GainBitcoin, etc. Despite the regulatory crackdown on some of the crypto-related pyramid schemes, the practice remains common as this article is written, even if warnings are readily available with a simple search. For example, webpages like https://www.cryptobase.best/ and https://www.cryptobase.team/ are both attacks on an Italian company called Cryptobase Ltd. These fraudulent websites apparently belong to the Milton Group and have no relationship with the Italian software firm – both scam sites are active, promising *daily* cloud mining returns of 16%. The scam website checker "fakewebsitebuster.com" reports multiple red flags: fake company age (domain name), copied text in the profile, exorbitant returns and referral fees, business relationships with non-existent firms (Crypto Bit Business Ltd does not exist), a US address with a UK phone number, spelling mistakes, etc [9]. Figure 3 shows two of the scheme's on-ramp webpages.

As with pumping frauds, researchers are now focusing on detection tools. Bartoletti *et al.* (2018) develop a data mining model based on probabilistic parameters and decision trees to recognize Bitcoin Ponzi schemes and thus identify 1,211 addresses that collectively received over US$10m. Unfortunately, identification does not equal protection – as proven by the fact that many pyramid schemes are still active. Perhaps the only line of defense, as with other frauds, is investor education. As the maxim goes: "If it looks too good to be true, then it's not real!"

While these six categories highlight the evolution of old schemes, there is an avalanche of new scams that derive their origin in the advent of cryptocurrencies and the digital era. They include fraudulent ICOs, rug pulls, cloud mining cons, exit scams, fake recovery services and developers, sim swaps, tampered hardware, impersonation, and social media giveaways, etc. While these are beyond the scope of this study, they will certainly occupy researchers in the near future.



Sources: https://www.cryptobase.team/ and https://www.cryptobase.best/

Figure 3.
Current cloud mining scam

4. Conclusions and directions for future research

Digital assets and related technologies have seized the consciousness of the investing public due to media attention, novelty, and the potential for speculation. Although these assets are relatively new to investors, the standard fraud schemes still generate significant economic rents, facilitating a process of innovation and evolution by criminals to incorporate digital assets. For regulators and law enforcement to properly respond to the threat posed in the digital asset sphere, they should comprehend how criminal activity differs in cyberspace, the nature of fraud schemes currently being carried out, and why investors fall prey to digital asset fraud schemes.

In this paper, we describe how cyberspace offers an expanded fraud opportunity set for fraudsters through the Space Transition Theory. We detail six old schemes operationalized historically in the physical space that have been recycled for applicability to digital assets: ransomware, price manipulation, improper disclosures, pump and dumps, Ponzi schemes, and spoof sites and fake apps. All have generated significant economic losses to investors thus far.

Regulators should enact a public awareness campaign regarding these fraud schemes so that potential victims recognize the fraud before investing. However, it may not be possible to overcome cognitive biases and a predilection for risk-taking behavior through education alone, so financial crime professionals and regulators will need to remain vigilant. Regulators should also exercise caution because negative externalities can occur when regulators attempt to regulate away undesirable rent-seeking activities. Over- or ill-conceived regulation may increase costs and ultimately reduce socially beneficial innovation related to digital asset markets or distort incentives, facilitating innovation in new fraud schemes.

This paper provides avenues for future research linking psychological theories to crypto-fraud schemes to better uncover the susceptibility of individuals to these fraud schemes. Research regarding the psychology of digital asset investors, the propensity to gamble using digital assets and fraud schemes that exploit gambling activity, and potential links between behavioral biases and digital fraud schemes could provide significant insights for anti-financial crime professionals. In addition, research regarding aspects of regulatory activity with the potential to reduce the reaction time of financial crime professionals to innovations in digital asset fraud. Further research can also address new schemes with digital coins, including fraudulent ICOs, rug pulls, exit scams, fake exchanges/developers/recovery, sim swaps, tampered cold wallets, and others, as they emerge.

Notes

1. See Dupuis and Gleason (2020) for the many ways crypto transactions can be traced and/or obfuscated.
2. See www.anchain.ai/ciso for software details.
3. See one of the advertising videos at www.youtube.com/watch?v=−3wUe2N2_OY
4. See Butler *et al.* (2021), available at www.jdsupra.com/legalnews/crypto-every-regulator-wants-a-piece-of-2031508/
5. Source: https://tether.to
6. See Roberts (2021) for details.
7. For example, see https://cryptochainuni.com/scam-list/
8. The complete scam dataset is available at: https://cryptoexchangescam.github.io/ScamDataset/
9. See https://fakewebsitebuster.com/cryptobase-team/ for details.

References

Ante, L. (2021), "How Elon Musk's Twitter activity moves cryptocurrency markets", Working paper, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3778844

Assarut, N., Bunaramrueang, P. and Kowpatanakit, P. (2019), "Clustering cyberspace population and the tendency to commit cyber crime: a quantitative application of space transition theory", *International Journal of Cyber Criminology*, Vol. 13 No. 1, pp. 84-100.

Bartoletti, M., Pes, B. and Serusi, S. (2018), "Data mining for detecting Bitcoin Ponzi schemes", 2018 Crypto Valley Conference on Blockchain Technology (CVCBT), pp. 75-84.

Broderick, R. (2021), "Inside the cryptocurrency scam vortex", *The Verge*, available at: www.theverge.com/22522380/cryptocurrency-scams-hacks-bitcoin

Brooks, K. (2021), "Cryptocurrency scams have soared 1,000% since October", CBS News, available at: www.cbsnews.com/news/bitcoin-cryptocurrency-investment-scams/

Butler, T., Carlson, C. and White, M. (2021), "Crypto: every regulator wants a piece of the action", Troutman Pepper, available at: www.jdsupra.com/legalnews/crypto-every-regulator-wants-a-piece-of-2031508/

Cengiz, F. (2021), "LSE European politics and policy (EUROPP) blog: What the EU's new MiCA regulation could mean for cryptocurrencies", *LSE European Politics and Policy (EUROPP) Blog: What the EU's New MiCA Regulation Could Mean for Cryptocurrencies*, available at: https://blogs.lse.ac.uk/europpblog/2021/07/05/what-the-eus-new-mica-regulation-could-mean-for-cryptocurrencies/

Cressey, D.R. (1953), *Other People's Money: A Study in the Social Psychology of Embezzlement*, The Free Press, Glencoe, IL.

Dobby, C. (2021), "Good afternoon, we've stolen your corporate data", Please kindly connect with one of our customer service agents to arrange payment. The Star, available at: www.thestar.com/business/2021/06/17/good-afternoon-weve-stolen-your-corporate-data-please-kindly-connect-with-one-of-our-customer-service-agents-to-arrange-payment.html

Dupuis, D. and Gleason, K. (2020), "Money laundering with cryptocurrency: open doors and the regulatory dialectic", *Journal of Financial Crime*, Vol. 28 No. 1, pp. 60-74.

Dupuis, D., Gleason, K. and Kannan, Y.H. (2021), "Bitcoin and beyond: crypto-asset considerations for the auditing classroom", Working Paper, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3900742

Felson, M. and Clarke, R.V. (1998), "Opportunity makes the thief", *Police Research Series, Paper*, Vol. 98 Nos 1/36, p. 10.

Gallo, S. (2021), "Fintech platforms: lax or careful borrowers' screening?", *Financial Innovation*, Vol. 7 No. 1.

Griffin, J.M. and Shams, A. (2020), "Is bitcoin really untethered?", *The Journal of Finance*, Vol. 75 No. 4, pp. 57-87.

Hamrick, J.T., Rouhi, F., Mukherjee, A., Feder, A., Gandal, N., Moore, T. and Vasek, M. (2018), "The economics of cryptocurrency pump and dump schemes", *SSRN Electronic Journal*.

Houben, R. and Snyers, A. (2018), "Cryptocurrencies and blockchain: legal context and implications for financial crime, money laundering and tax evasion", available at: https://op.europa.eu/en/publication-detail/-/publication/631f847c-b4aa-11e8-99ee-01aa75ed71a1/language-en/format-PDF/source-76403102

Jaishankar, K. (2008), "Space transition theory of cyber crimes", in Schmallager, F. and Pittaro, M. (Eds), *Crimes of the Internet*, Prentice Hall, Upper Saddle River, NJ, pp. 283-301.

Kamps, J. and Kleinberg, B. (2018), "To the moon: defining and detecting cryptocurrency pump-and-dumps", *Crime Science*, Vol. 7 No. 1, pp. 1-18.

Keroles, C. (2021), "Bitfinex, tether found to misrepresent USDT backing and obscure user fund losses", *Bitcoin Magazine*, available at: https://bitcoinmagazine.com/business/bitfinex-tether-found-to-misrepresent-usdt-backing-and-obscure-user-fund-losses

Kethineni, S. and Cao, Y. (2020), "The rise in popularity of cryptocurrency and associated criminal activity", *International Criminal Justice Review*, Vol. 30 No. 3, pp. 325-344.

Kohnke, A., Laidlaw, G. and Wilson, C. (2021), "Challenges in bridging the law enforcement capability gap", *International Conference on Cyber Warfare and Security*, 521–XII.

Korver, M.R., Counsel, D. and Poteat, E. (2019), "Attribution in cryptocurrency cases", *DOJ Journal of Federal Law and Practice, February*, pp. 233-262.

Krapels, N. and Liebau, D. (2021), "An exploratory essay on minimum disclosure requirements for cryptocurrency and utility token issuers", *Cryptoeconomic Systems*, Vol. 1 No. 2, pp. 1-23.

Li, T., Shin, D. and Wang, B. (2021), "Cryptocurrency pump-and-dump schemes", available at: SSRN 3267041.

McGee, R. and Conlon, T. (2021), "ICO fraud and regulation. Batten-Corbet-Lucey handbooks in alternative investments", Forthcoming, available at: https://ssrn.com/abstract=3770659 or http://dx.doi.org/10.2139/ssrn.3770659

Morrison, S. (2021), "How a major oil pipeline got held for ransom", available at: www.vox.com/recode/22428774/ransomeware-pipeline-colonial-darkside-gas-prices

Nghiem, H., Murić, G., Morstatter, F. and Ferrara, E. (2021), "Detecting cryptocurrency pump-and-dump frauds using market and social signals", *Expert Systems with Applications*, Vol. 182.

Nizzoli, L., Tardelli, S., Avvenuti, M., Cresci, S., Tesconi, M. and Ferrara, E. (2020), "Charting the landscape of online cryptocurrency manipulation", Working paper, available at: www.researchgate.net/publication/338883850_Charting_the_Landscape_of_Online_Cryptocurrency_Manipulation

Potgieter, P.H. and Howell, B.E. (2021), "Regulating cryptocurrencies: mapping economic objectives and technological feasibilities", doi: 10.2139/ssrn.3927658, Available at SSRN 3927658

Roberts, M. (2021), "Crypto equivalent of credit default exchange?", *Journal Beat*, available at: https://journal-beat.com/crypto-equivalent-of-credit-default-exchange/

Samejo, A., Bhatti, M.Y. and Mailto, A. (2018), "A review of cryptocurrency analysis, regulation and security measures to risks and threats", *International Journal of Computer Science and Emerging Technologies*, Vol. 2 No. 2, pp. 42-56.

Securities and Exchange Commission (2021), "SEC charges three individuals in digital asset frauds", available at: www.sec.gov/news/press-release/2021-22

Sundaravelu, A. (2021), "Why the US is pushing for higher cryptocurrency tax reporting standards", *International Tax Review*, July, available at https://search-ebscohost-com.proxy.ulib.csuohio.edu/login.aspx?direct=true&db=bth&AN=151229917&site=eds-live&scope=site

Wang, C.W. (2018), "The impact of tether grants on bitcoin", *Economics Letters*, Vol. 171, pp. 19-22.

Wells, J.T. (2001), "... and nothing but the truth, uncovering fraudulent disclosures", *Journal of Accountancy*, Vol. 192 No. 1, p. 47.

Xia, P., Wang, H., Zhang, B., Ji, R., Gao, B., Wu, L., Luo, X. and Xu, G. (2020), "Characterizing cryptocurrency exchange scams", *Computers and Security*, Vol. 98, p. 101993.

Corresponding author
Kimberly Gleason can be contacted at: kgleason@aus.edu