12-27-2019

Convenience Theory of Cryptocurrency Crime: A Content Analysis of U.S. Federal Court Decisions

Claire Nolasco Braaten
Texas A&M University-San Antonio, Claire.Nolasco@tamusa.edu

Michael S. Vaughn
Sam Houston State University

Convenience Theory of Cryptocurrency Crime: A Content Analysis of U.S. Federal Court Decisions

Claire Nolasco Braaten[a]* and Michael S. Vaughn[b]

[a]*Department of Criminology and Criminal Justice, Texas A&M-San Antonio, San Antonio, Texas, USA;* [b]*Department of Criminal Justice and Criminology, Sam Houston State University, Huntsville, Texas, USA*

*Claire Nolasco Braaten can be contacted at Texas A&M-San Antonio, One University Way, San Antonio, Texas 78224 at cnolasco@tamusa.edu

This work was supported by the Summer Faculty Fellowship Grant 2019 of the Texas A&M-San Antonio University.

Dr. Claire Nolasco Braaten, is an Associate Professor in the Criminology and Criminal Justice Department at Texas A&M-San Antonio. She has a Ph.D. in Criminal Justice, a J.D. in law, and and LL.M. in International Economic and Business Law. She is licensed to practice law in both California and the Philippines. Her research interests are in corporate financial crime, cybercrime, immigration rights and integration, empirical legal research, and judicial decision making in the criminal justice and legal processes.

Dr. Mike Vaughn is a Professor at the College of Criminal Justice at Sam Houston State University. He serves as Co-Director of the Institute for Legal Studies in Criminal Justice. Dr. Vaughn has served as Book Review Editor of the Journal of Criminal Justice Education (1993-1996), Editor of Police Forum (1997-2001), Editor of the Criminal Justice Review (2001-2005), and Editor of the International Criminal Justice Review (2001-2005).

.

Convenience Theory of Cryptocurrency Crime: A Content Analysis of U.S. Federal court Decisions

This article examines cryptocurrency cases decided in the U.S. District and Circuit Courts to determine the applicability of Gottschalk's convenience theory of white collar crime to cryptocurrency crime litigation and to empirically analyze whether the conditions under which cryptocurrency offenses occurred show support for the convenience theory. Analysis of U.S. federal district and circuit court case law involving cryptocurrency crimes and fraud indicate support for the convenience theory of white-collar crime. Defendants in various schemes were motivated by financial gain, either for the company or for personal use. Their roles and positions in the businesses allowed them access to resources that helped them perpetrate fraud through the following mechanisms: (1) operation of front companies; (2) relationship building by defendants; (3) over representing profits that investors would obtain from purchases of virtual currencies, representing that tokens were safe and reliable investments when they were risky, and overestimating abilities and capacities to provide services promised to investors in securities fraud; (4) breaching fiduciary duties to their clients and corporate stockholders by misappropriating profits for their own personal gain; and, (5) engaging in dark web transactions that guaranteed anonymity. Defendants also employed various neutralization techniques to justify their crimes.

Keywords: cryptocurrency; virtual currency; convenience theory; white collar crime; financial fraud; corporate crime

Introduction

Virtual currencies or cryptocurrencies are: (1) digital assets used as a medium of exchange (Young, Donley, and Kneller 2016); (2) stored electronically in "digital wallets" and transacted on the internet through a direct peer-to-peer system; and (3) called "cryptocurrencies" because they use "cryptographic protocols to secure transactions" recorded on publicly available decentralized ledgers called "blockchains" (*CFTC v. McDonnell* 2018a:218). The blockchain

allows the public to verify and acknowledge transfers of virtual currency from one user to another "without requiring any central intermediary" (Commodity Futures Trading Commission 2017). Advocates of distributed ledgers, the blockchain technology underlying virtual currencies, claim that these will "enhance economic efficiency, mitigate centralized systemic risk, defend against fraudulent activity and improve data quality and governance" (Giancarlo 2016, 2018). Virtual currencies, however, are not backed by any government, fiat currency, or commodity (Anello and Lee 2017) and at least one federal district court has ruled that bitcoin is not "money" although it operates as a medium of exchange because, unlike cash or currency, it "does not issue from or enjoy the protection of any sovereign" (*U.S v. Petix* 2016:*5).

The price of bitcoin and other virtual currencies remains volatile, rising and falling at extreme rates (Kharif 2017). On Feb. 6, 2018, coinmarketcap.com reported that there were more than 1,500 virtual currencies with bitcoin having the largest market capitalization of $121,264,863,386— one unit of bitcoin was valued at $7,196.92, while Strong Hands, the cheapest virtual currency was valued at $0.000001 (*CFTC v. McDonnell* 2018a). The "combined market capitalization" of all virtual currencies dropped from $795 billion on January 6, 2018 to $329 billion on Feb. 6, 2018 (*CFTC v. McDonnell* 2018a:219; Kharpal 2018). Due to their extreme variability in value, online exchanges such as Coinbase were created to allow the public to trade and invest in virtual currencies (*CFTC v. McDonnell* 2018a; Popper 2017).

The increase in online virtual currency transactions has resulted in a concomitant increase in fraudulent and criminal activity (Sanchez 2017). Silk Road, an online market for illicit activity and drugs, allowed transactions only in bitcoin. Since its closure following undercover operations by agents of the Federal Bureau of Investigation, other online black markets have sprouted, transacting solely in virtual currencies (Burks 2017). Virtual currency exchanges are

also susceptible to hacking and theft (Hern 2014). Hackers, for instance, have stolen approximately $532.6 million from the Tokyo-based cryptocurrency exchange Coincheck Inc., raising questions about security and regulatory protection (Wilson, Sano, and Zaharia 2018). These criminal activities have led to calls for increased governmental oversight and regulation of virtual currency (Braaten 2019).

Legal context of cryptocurrency regulation

Cryptocurrency as funds

Table 1 provides a summary of the statutes governing cryptocurrency litigation. Section 1960 makes it a crime to knowingly operate an "unlicensed money transmitting business" (*U.S. v. Budovsky* 2015:*6) and provides a penalty of a fine and not more than five years imprisonment (18 U.S.C. § 1960(a)). Section 5330, a provision of the Bank Secrecy Act, requires the registration of money transmitting businesses with the Secretary of Treasury while 31 C.F.R. § 1022.380(a)(1) requires its registration with the U.S. Department of the Treasury's Financial Crimes Enforcement Network ("FinCEN"). FinCEN also issued clarificatory guidelines, stating that virtual currency exchangers are considered money transmitters (the "2013 FinCEN Guidance") and that existing Bank Secrecy Act regulations apply to persons creating or transmitting virtual currencies (*U.S. v. Budovsky* 2015; *U.S v. Lott* 2014; U.S. Dep't of Treasury FinCEN 2013). The law and regulations require businesses to register as a money transmitter within 180 days from the date of its organization or incorporation. Cryptocurrencies such as bitcoin are subject to money transmitting and money laundering laws because they can be purchased in exchange for currency, act as a denominator of value, and are used in financial transactions (*Boumediene v. Bush* 2008; *Clark v. Rameker* 2014; *Nix v. Hedden* 1893; Oedel

1997; *SEC v. Shavers* 2013; *U.S v. Faiella* 2014; *Walters v. Metro. Educ. Enterprises, Inc.* 1997; *Yates v. U.S* 2015).

Cryptocurrencies as commodities

The Commodity Exchange Act ("CEA") defines "commodities" as including "all other goods and articles" and "all services, rights, and interests" in which contracts "for future delivery are presently or in the future dealt in" (Title 7 U.S.C. §1(a)(9)). A "commodity" is "an article of trade or commerce" (Garner 2014), "an economic good" (Merriam Webster 2019), "goods sold in the market with a quality and value uniform throughout the world" (Prentis 2015:626), a "store of value" that accommodates man's physical wants and needs (Litwack 2015:343), and a "type of monetary exchange" (*CFTC v. McDonnell* 2018a:225; Prentis 2015:628-629). In an administrative proceeding in 2015, the CFTC issued an order in which it found that virtual currencies can be classified as commodities (*In the Matter of: Coinflip, Inc.* 2015).

Table 1 summarizes the commodity anti-fraud provisions of Title 7 U.S.C. §9(1) of the CEA and 17 C.F.R. § 180.1. To prove a violation of the commodity fraud provisions of the CEA, the Commodity Futures Trading Commission ("CFTC") must show that: (1) defendants engaged in prohibited conduct (e.g., employed a fraudulent scheme; made a material misrepresentation, misleading statement or deceptive omission; or engaged in a business practice that operated as a fraud); (2) with scienter or intent; and (3) in connection with a contract of sale of a commodity in interstate commerce (*CFTC v. Commodity Inv. Grp., Inc.* 2006; *CFTC v. R.J. Fitzgerald & Co., Inc.* 2002). The CFTC has jurisdiction "if there is fraud or manipulation involving a virtual currency traded in interstate commerce" (*CFTC v. Hunter Wise Commodities* 2014:1348; *CFTC v. S. Tr. Metals*, 2018:1319).

The CFTC is one of the federal administrative bodies exercising partial and concurrent

supervision over virtual currencies (*CFTC v. McDonnell* 2018a; Giancarlo 2018). The CFTC has anti-fraud and anti-manipulation authority over "any contract of sale of any commodity in interstate commerce" (*CFTC v. My Big Coin Pay, Inc.* 2018:495). The Securities and Exchange Commission ("SEC"), Internal Revenue Service ("IRS"), Department of Justice, Treasury Department, and state agencies have also exercised their concurrent regulatory authority over virtual currencies (Gorman 2018). The U.S. approach to oversight of virtual currency is "multifaceted" and "multi-regulatory" (Giancarlo 2018:10), consisting of the following: (1) criminal law prosecutions of Ponzi-like schemes by the Department of Justice, or state criminal agencies, or civil litigation based on allegations of fraud (*CFTC v. McDonnell* 2018a; *U.S v. Faiella* 2014; *U.S v. Lord* 2017); (2) regulation as commodities by the CFTC (Giancarlo 2018); (3) regulation as securities by the SEC (*SEC v. Plexcorps* 2017); (4) regulation for violation of U.S. anti-money laundering laws by the FinCEN (Hudak 2017); (5) regulation as property by the Internal Revenue Service ("IRS") (IRS Notice 2014-21; *U.S v. Coinbase, Inc.* 2017); (6) self-regulation by private exchanges (Nikkei Asian Review 2017); and (7) state regulations (Loconte 2017).

Insert Table 1 here

Cryptocurrencies as securities

Section 12(a)(1) of the Securities Act grants a private right of action against any person who offers or sells an unregistered security in violation of Section 5 (*Scheck Invs., L.P. v. Kensington Mgmt., Inc.* 2009, *SEC v. Unique Fin. Concepts, Inc.* 1999). Section 17(a) of the Securities Act, Section 10(b) of the Exchange Act, and Rule 10b-5 prohibit "fraudulent conduct or practices in connection with the offer or sale of securities" by means of interstate commerce

(*SEC v. Dain Rauscher, Inc.* 2001:855). The term "security" under the Securities Act and the *Howey* Test includes an "investment contract" which involves: "(1) an investment of money, (2) in a common enterprise, (3) with the expectation of profits solely from the efforts of others (*Gugick v. Melville Capital, LLC* 2014:*4; *S.E.C. v. Edwards*, 2004:395, quoting *United Hous. Found., Inc. v. Forman* 1975:852; *S.E.C. v. W.J. Howey Co.* 1946:299-299; *Tippens v. Round Island Plantation LLC* 2009:*9, quoting *SEC v. Unique Fin. Concepts, Inc.* 1999:1199). Transactions involving virtual currency are investment contracts or securities subject to federal securities laws, including the registration requirements and anti-fraud provisions of the SEC (*Balestra v. ATBCOIN LLC* 2019; *Hodges v. Harrison* 2019; *SEC v. Blockvest, LLC* 2018).

Convenience theory of white collar crime

White-collar crime typically involves offenders with special access to resources and opportunities due to their corporate roles, professional positions, power, influence, and trust by others (Felson and Boba 2017; Nolasco, Vaughn, and del Carmen 2013). Nolasco et al. (2013:387), for instance, explained that perpetrators of pyramid and Ponzi schemes were able to defraud investors through "deliberate misinformation and false promises" and that "defrauded investors also placed a significant amount of trust and reliance" on the offenders due to various "trust and affinity relationships based on socio-economic status, race or ethnicity, religion or special circumstances (i.e., disability or seniority)." Offenders in white collar crime abuse their organizational positions or professional status to gain information and access to victims (Felson and Boba 2017).

Marketing theory explains that convenience is the perceived savings in time and effort expended to accomplish a task, solve a problem, or exploit favorable circumstances (Farquhar and Rowley 2009). Convenience pertains to the time and effort exerted "before, during, and after

an activity" (Gottschalk 2017a:605) when accomplishing an illegal transaction process or processes (Collier and Kimes 2012). Convenience orientation refers to the individuals' and organizations' preference for convenient actions and strategies, including illegal actions, which save them time and effort when accomplishing goals (Farquhar and Rowley 2009; Gottschalk 2018c; Mai and Olsen 2016). Convenience orientation for illegal actions "increases when negative attitudes toward legal actions increase" (Gottschalk 2018a:1602). Motivated by greed or facing strain, white collar offenders perceive an illegal action as a viable and convenient solution to a difficult problem despite potential costs consisting of the likelihood of detection and future punishment. Financial crime saves them time and effort when solving a problem to obtain personal or organizational profit. Gottschalk (2017a:605) describes this as "[p]aying for convenience"—"reducing time and effort now entails a greater potential for future cost."

Convenience theory explains that convenience in three dimensions facilitate white-collar crime: (1) the economic dimension or financial desire attracts offenders to crime as a convenient way of satisfying desires for personal and organizational profits, including achieving the American dream (Trahan, Marquart, and Mullings 2005); (2) the organizational dimension or organizational opportunity enables offenders with key corporate roles to gain convenient access to corporate resources and personnel; and, (3) the behavioral dimension enables offenders to conveniently justify and rationalize their deviant behaviors (Gottschalk 2017, 2018a, 2018b, 2019; Kaptein and Van Helvoort 2019).

Gottschalk's (2017a) convenience theory posits the following: (1) financial crime can occur within an organization without being detected; (2) offenders are motivated by profits and success resulting from negative (threats) and positive (strengths) circumstances; offenders are motivated when faced with threats to protect company interests, to survive (Blickle et al. 2006),

or to pay off personal debts (Brightman 2009). Offenders are motivated from strengths when expanding into profitable foreign markets or satisfying their greed (Bucy et al. 2008; Goldstraw-White 2012; Hamilton and Mickethwait 2006); (3) the offender's profession and organizational role grants him or her access to resources (Benson and Simpson 2015; Pickett and Pickett 2002) and enables him or her to commit white-collar crime without substantial risk of detection and punishment (Aguilera and Vadera 2008; Haines 2014), especially when the prevailing organizational structure and culture is conducive to unethical or illegal behavior (Dion 2008; Pontell, Black, and Geis 2014; Puranam, Alexy, and Reitzig 2014); (4) the organizational environment enables the offender to commit financial crime "without being perceived as a deviant person or suspicious person" because of his or her social capital (Gottschalk 2017a:613); and (5) acceptance and neutralization of deviant behavior facilitates criminal behavior (Bystrova and Gottschalk 2015) by eliminating feelings of guilt when committing criminal acts (Sutherland 1940; Sykes and Matza 1957).

Dimensions of convenience theory

Economic dimension of crime. White-collar crime is a profit-driven crime, which results from "favorable circumstances" characterized by threats and strengths (Gottschalk, 2017a:606). Threats arise due to various types of strain (Langton and Piquero 2007), including sunk costs arising from capital expenses already invested in the enterprise, possibility of loss, bankruptcy, and unique market structures peculiar to the industry, such as monopolies (Chang, Lu, and Chen 2005; Piquero 2012). Potential competitors in monopolized industries, for example, are pressured to either join the monopoly or commit white-collar crime to protect their economic interests (Blickle et al. 2006). Strengths arise due to favorable circumstances, including : (1) the possibility of getting large contracts and foreign subsidiaries through bribing foreign government

officials; (2) the likelihood of being promoted, receiving increased compensation, and earning bonuses due to goal achievement; and (3) the possibility of enhancing corporate goodwill or individual reputation resulting from accumulation of profits (Gottschalk 2017b). Motivated by financial gain and greed, offenders resort to white-collar crime to ensure economic survival.

The economic dimension assumes a rational choice in which offenders weigh their economic interests against the probability of detection (Welsh et al. 2014) and desist from committing crime where punishment is more certain or severe (Pratt and Cullen 2005). An offender will commit white-collar crime if the illegal action is the most convenient and expedient option (Agnew 2014) that would allow him or her to achieve gains with the least amount of time and energy; offenders are more likely to commit white-collar crime because of his or her perception of the low possibility of punishment and detection by the authorities (Gottschalk 2017b).

Organizational dimension. The organizational dimension of convenience theory explains that white-collar criminals have the opportunity to commit illegal acts by virtue of their corporate positions and professional roles in society. Corporate officers (e.g., CEOs, CFOs, chairpersons, and executives) and business professionals (e.g., lawyers and accountants) abuse their positions and influence to access resources and commit white-collar crime for corporate or personal gain (Reed and Yeager 1996). Criminal opportunity is "the presence of a favorable combination of circumstances that renders a possible course of action relevant" (Aguilera and Vadera 2008:434). Opportunity arises when offenders perceive that they can engage in fraudulent or illegal behavior without surveillance, accountability, detection, or punishment (Benson and Simpson 2015; Fligstein and Roehrkasse 2016; Haines 2014). An organizational culture, for instance, where misconduct and unethical practices are pervasive encourages corporate employees to participate

in white-collar crime (Ashforth et al. 2008; Punch 2003). Opportunity also depends on the offender's social capital which enables his or her access to resources and fosters trust due to his or her position in a social or organizational hierarchy or network (Adler and Kwon 2002; Hansen 2009; Heath 2008).

Behavioral dimension. The behavioral dimension examines the causes and justifications of white-collar crime, including the situational context within which it occurs (Koppen, Poot, and Blokland 2010). White-collar criminal behavior occurs, for example, because: (1) it is convenient for the criminal to be deceitful to obtain personal gain at the expense of others (Pickett and Pickett 2002); (2) offenders apply techniques of neutralization that enable them to believe their actions are not unlawful, including denying responsibility, injury, and victim, condemning the condemners, appealing to higher loyalties, normality of action, entitlement, legal mistake, acceptability of their own mistakes, and existence of dilemmas where reasonable tradeoffs were made before committing the crime (Benson and Simpson 2015; Gottschalk 2017b; Siponen and Vance 2010; Sykes and Matza 1957); (3) narcissistic behavior (Arnulf and Gottschalk 2013; Ouimet 2009, 2010), including narcissistic organizational identification, enables the offender to perceive his or her identity as central to the identity of the organization (Galvin, Lange, and Ashforth 2015); and (4) small indiscretions over time which lead to incremental progression toward serious white-collar crime because of the presence of financial gains and benefits and the concomitant absence of supervision or control in an organizational culture permissive of unethical behavior (Welsh et al. 2014). This results in a slippery slope "defined as a gradual decline in which no one event makes one aware that he or she is acting unethically" (Arjoon 2008:78).

Gottschalk (2018a) found support for convenience theory in his analysis of data involving 405 white-collar prisoners in Norway from 2009 to 2015: (1) offenders were motivated by desire for corporate profits (17% of sample) or personal gain (83%) (economic dimension); (2) all offenders occupied trusted positions in their organizations (organizational dimension); and (3) offenders applied neutralization techniques to justify their crimes (behavioral dimension). Content analysis of media reports, court documents, and autobiographies showed that white-collar offenders employed the following neutralization techniques: (1) denied responsibility by rejecting accountability for the crime and denied leadership roles; (2) denied injury from the crime and refuted occurrence of harm; (3) dismissed the victims by denying that anyone suffered harm; (4) condemned the condemners by expressing skepticism of critics; (5) appealed to higher loyalties as a reason for their actions; (6) alleged normality of action by arguing that everyone does it; (7) claimed entitlement to action because of the situation; (8) argued legal mistake and considered infringement irrelevant because of error in the law; (9) felt entitled to make mistakes and argued that illegal action was within acceptable mistaken quotas; and (10) presented dilemma trade-offs by weighting various concerns that resulted in the illegality.

Objectives

Traditional methods of prosecution and enforcement against cryptocurrency crimes may no longer be appropriate because of the complexity of transactions involving cryptocurrency and the anonymity of the blockchain network through which these transactions occur. For criminologists, the rise in cryptocurrency crime presents a problem that must be examined and explained through appropriate theories. This article examines cryptocurrency cases decided in the U.S. District Courts and the U.S. Circuit Courts of Appeals. The article applies Gottschalk's convenience theory of white collar crime to cryptocurrency crime litigation to empirically

analyze whether the conditions under which cryptocurrency offenses occurred show support for the convenience theory. Through a systematic analyses of the mechanisms by which cryptocurrency crimes were perpetrated and examination of the common themes underlying each form of virtual currency scheme, the article explores the underlying conditions that allowed perpetration of various cryptocurrency offenses. The intent is to provide a better understanding of the underlying economic, organizational, and behavioral dimensions that allowed perpetration of cryptocurrency law violations.

Method

The WESTLAW computerized database contains electronic copies of published and unpublished court decisions. A keyword search was used to gather cases on bitcoin and cryptocurrency offenses decided by all U.S. federal courts until 20 February 2019. The advanced search parameters required that the term "bitcoin" appeared in the "main body" of the case (*N*=62). The authors then read each case individually and determined that not all cases were relevant to the article's focus, either because the case did not involve bitcoin or virtual currency, did not contain sufficient facts to enable full analysis, or contained a decision that either affirmed or repealed a lower court's decision, without discussing the facts. Also, some of the cases were repeated because of the appeal process through the federal courts. The deletion process yielded a total of 31 federal court cases. The authors conducted an inductive doctrinal analysis (Nolasco, Vaughn, and del Carmen 2010) to synthesize federal court decisions on bitcoin and virtual currency, creating a framework from which to organize the analysis (Nolasco and Vaughn 2010; Nolasco et al. 2015).

Content Analysis of Federal Court Cases

Mechanisms for perpetrating cryptocurrency crimes

Analysis of federal court cases indicate that offenders in cryptocurrency litigation perpetrated the following cryptocurrency schemes: (1) operating unlicensed money transmitting business and/or money laundering; (2) engaging in commodities fraud; (3) orchestrating securities fraud; (4) creating bitcoin scams, bitcoin exchange fraud, and other criminal activities related to bitcoin; and (5) owning, administering, or selling on the dark web.

Unlicensed money transmitting businesses

Table 2 summarizes the dimensions of convenience theory within federal court cases involving unlicensed money transmitting business dealing in cryptocurrency. In several cases, defendants operated an unlicensed money transmitting business dealing in the virtual currency bitcoin in violation of 18 U.S.C. § 1960 (*U.S. v. Faiella* 2014; *U.S v. Mansy* 2017; *U.S v. Petix* 2016; *U.S v. Stetkiw* 2019). Defendants involved in unlicensed money transmitting businesses were motivated by personal or corporate gains (economic dimension). Their positions in the organization provided them opportunities to perpetrate their unlicensed money transmitting scheme through: (1) creating front companies to conceal the true nature of their unlicensed money transmitting business (*U.S v. Murgio* 2016); (2) accessing resources that enabled them to defraud investors and government regulators, including company emails, accounts, websites, and other information technology infrastructure; and (3) implementing procedures in online digital currency exchanges that guaranteed anonymity among users (*U.S. v. Budovsky* 2015) (organizational dimension). Defendants justified or explained their behavior through various neutralization techniques: (1) alleging legality of action, arguing that state laws did not require virtual currency exchangers to obtain money service business licenses (*U.S v. Lord* 2019); and

(2) claiming no injury because he or she exchanged cash received from customers for the equivalent value in bitcoin (*U.S. v. Faiella* 2014) (behavioral dimension).

Insert Table 2 here

Opportunities: operation of front companies and anonymity among users

Several cases involved defendants who created front companies to conceal the illegal nature of their businesses. In *U.S. v. Murgio* (2016), defendant Murgio operated Coin.mx as an illegal bitcoin exchange and the Collectables Club as a sham front company to help its members sell and trade valuable memorabilia on the internet. At that time, conventional banks refused to process bitcoin transactions and closed defendants' bank accounts upon discovering that they transacted in bitcoin (*U.S. v. Gross* 2017:*5). Defendants thus misled banks by making it appear that the transactions were for the Collectables Club (and other, non-bitcoin businesses), instructing customers to lie to the banks. Similarly, in *U.S. v. Budovsky*, 2015, after the Costa Rican government regulator refused to grant a license to Liberty Reserve, it continued to operate in Costa Rica through Budovsky's shell company, transferring funds into more than two dozen shell-company accounts around the world to evade government seizures.

One case illustrates how anonymity in an online digital currency exchange facilitated its widespread use among criminal offenders. In 2006, defendants Budovsky and Kats incorporated Liberty Reserve in Costa Rica to provide online access to the virtual currency LR, "[an] instant, real-time currency for international commerce" (*U.S. v. Budovsky* 2015:*1). From 2006 to 2013, Liberty Reserve processed an estimated 55 million financial transactions and laundered more than $6 billion in criminal proceeds. Liberty Reserve was not registered with the United States

Treasury Department as a money transmitting business. It ensured anonymity by not requiring users to validate their identity, allowing them to hide their account numbers when transferring funds to make them untraceable and requiring them to use LR for all transactions. Criminal users of Liberty Reserve operated from countries worldwide, including China, Nigeria, and the United States and consisted of computer hackers for hire, drug-dealing websites, and traffickers of stolen credit card and personal identity information.

In 2009, a Costa Rican government regulatory agency refused to grant a money transmitting business license to Liberty Reserve because it did not have basic anti-money laundering controls. Budovsky and his co-defendants then created a computer portal that allowed Costa Rican regulators to access and monitor fabricated information for suspicious activities. On November 18, 2011, FinCEN notified financial institutions about the risks associated with transacting with Liberty Reserve. Liberty Reserve then falsely informed Costa Rican officials that it sold its business and was no longer operating in Costa Rica, although it continued to operate through a shell company controlled by Budovsky. Shortly thereafter, the Costa Rican government seized—pursuant to a request by U.S. law enforcement—approximately $19.5 million in Costa Rican bank accounts held by Liberty Reserve. After this seizure, defendants moved Liberty Reserve funds into more than two dozen shell-company accounts around the world to evade further seizures. Budovsky and his co-defendants were charged with: (1) conspiracy to commit money laundering in violation of 18 U.S.C § 1956(h); (2) conspiracy to operate an unlicensed money transmission business in violation of 18 U.S.C. § 371; and (3) operation of an unlicensed money transmission business in violation of 18 U.S.C. § 1960. On June 23, 2015, Budovsky moved to dismiss the charges. The U.S. District Court for the Southern District of New York denied the motions.

Commodities fraud

Table 3 summarizes the dimensions of convenience theory within federal court cases involving cryptocurrencies considered as commodities fraud. Defendants in commodities fraud frequently solicit investors to purchase contracts of services involving cryptocurrency, which are considered commodities by the CFTC. These defendants are generally motivated by greed and profits derived from illegal operations (economic dimension); their positions within these companies provide them access to resources needed to defraud investors (organizational dimension); and they employ various neutralization techniques, including denial of responsibility and arguing their actions are legal (behavioral dimension). One case illustrates how defendants neutralize blame by shifting liability to others. In *CTFC v. McDonnell* (2018b:684), the defendant created multiple personas when dealing with clients to create the appearance that his company, CabbageTech, was operated by a specialized teams of experts. In reality, he assumed multiple employee personas when dealing with customers, including the fake identities of Jason Flack, Michelle Robertson, and Michelle Robinson.

The defendant's persona "Jason Flack" ignored client requests to withdraw their investments by neutralizing blame and shifting liability to his alter-ego Pat, explaining that: (1) Pat was "100%" the cause of the issues and not the company which "is really good;" (2) the company is "a legitimate outfit" and is "honestly doing everything possible to rectify the whole ordeal "in a pretty reasonable time frame with all that needed fixing;" (3) "I'm on your case and on your side;" and (4) "Pat did not reveal he was hacked [but] paid the ransom quietly behind my ex-Bosses back" (*CTFC v. McDonnell* 2018b:684). Defendant further neutralized blame by pointing out that,

> "[t]here is a wave of ransomware attacks globally if you google and [Pat's] lack of knowledge got [the company] site caught up in that web. Everyone from Major Corps. to Police Dept's. have

been infected with this malware [sic] top U.S. Gov't. agencies advise paying the ransom fee because it's anonymous encryption that cannot be reversed." (*CTFC v. McDonnell* 2018b:685)

Insert Table 3 here

Opportunities: fraudulent promises of exorbitant gains and creation of trust relationships with clients

Defendants in commodities fraud cases used their positions to falsely promise exorbitant gains to investors. Defendants in *CFTC v. My Big Coin Pay, Inc.* (2018:494) sold more than $6 million worth of cryptocurrency called My Big Coin ("MBC") by claiming that it was "backed by gold," could be used "anywhere MasterCard was accepted," and was "actively traded on several currency exchanges." The CFTC filed suit against defendants, alleging fraud in the sale of a commodity in violation of the Commodity Exchange Act ("CEA") (7 U.S.C. § 9[1]) and CFTC regulations (17 C.F.R. § 180.1[a]). The U.S. District Court for the Eastern District of Massachusetts denied defendants' motion to dismiss.

In another case, defendant Patrick McDonnell, owner and operator of CabbageTech Corp, sold membership services to provide expert cryptocurrency trading advice to 11 clients who transferred assets valued at $290,429.29 (*CTFC v. McDonnell* 2018a, 2018b). He falsely claimed that clients could potentially earn "300% profits on an investment in less than a week" (*CFTC v. McDonnell* 2018a:232). After receiving membership payments, McDonnell shut down his websites three months later without providing any of the promised trading advice, deleted social media accounts, ceased communicating with customers, and absconded with customers' funds (*CTFC v. McDonnell* 2018a). On January 18, 2018, the CTC brought enforcement action against defendant Pat McDonnell and CabbageTech, alleging that they operated "a deceptive and

fraudulent virtual currency scheme" in violation of the Commodity Exchange Act ("CEA") (*CTFC v. McDonnell* 2018b:653). McDonnell filed a motion to dismiss, arguing that CFTC lacked jurisdiction and standing. In denying the motion, the U.S. District Court for the Eastern District of New York held that the CFTC has broad anti-fraud authority over fraud related to virtual currencies transacted in interstate commerce.

In cases of commodity fraud, defendants made fraudulent statements to gain the trust of customers. In *CFTC v. My Big Coin Pay, Inc.* (2018), defendants gained the trust of clients by falsely assuring them that MBC was backed by gold and had real fluctuating value in an actively traded market. Similarly, in *CTFC v. McDonnell* (2018a, 2018b), Pat McDonnell was charming and personable, building personal relationships with clients to perpetuate fraud. Investors were misled by McDonnell's social media and internet presence, which included "misleading statements and omissions about his credentials," such as his "track record and prowess" as a professional Wall Street trader (*CTFC v. McDonnell* 2018b:661). He skillfully built personal relationships of trust and rapport with his customers, called them multiple times, and maintained constant communication through email, social media, and internet-based chats.

Securities fraud

Table 4 summarizes the economic, organizational, and behavior dimension of convenience theory as applied to cryptocurrency cases involving securities fraud. Defendants fraudulently sold securities or initial cryptocurrency coin offerings ("ICO") that were not registered with the SEC or were not exempt from registration under federal securities laws for the following reasons: (1) the prospect of significant financial gains pressured or incentivized defendants to commit fraud; (2) circumstances provided defendants with opportunities to commit fraud without detection; and (3) defendants justified their fraudulent acts through various

neutralization techniques.

Insert Table 4 here

Opportunities: false statements regarding nature and quality of virtual currency, expertise, and ability of promoters

The prospects of financial gain, investor desire to make huge profits, and defendants' organizational roles allowed defendants to commit fraud through the following strategies:

First, defendants overrepresented the amount of profits that investors would obtain from their purchase of virtual currencies (*Hodges v. Harrison* 2019). They falsely claimed that their digital tokens would outperform the market. In two related cases, Canadian based-defendants PlexCorps, Lacroix, and Paradis-Royer organized an ICO for an alleged 1 billion tokens of PlexCoin (*SEC v. PlexCorps* 2018a, 2018b). They fraudulently misrepresented that investors would earn 1,354% profit within 29 days. Defendants proceeded with the ICO even though the Quebec Financial Administrative Tribunal issued an *ex parte* order enjoining them from conducting the ICO. On December 1, 2017, SEC filed an action against defendants for securities fraud, claiming that they "unlawfully participated in a fraudulent fundraising scheme to obtain more than $15 million from tens of thousands of investors who purchased PlexCoins" (*SEC v. PlexCorps* 2018b:*1). Similarly, defendants in *Audet v. Fraser* (2017:*3) fraudulently represented that Paycoin had an estimated value of $80-$100 per coin with a price guarantee that it "would not fall below a $20 price floor."

Second, defendants represented that their cryptocurrencies were safe and reliable investments. Defendant Blockvest, for example, offered the digital coin BLV in exchange for other virtual currency such as bitcoin and Ether or fiat currency (*SEC v. Blockvest, LLC* 2018).

Blockvest falsely claimed that: (1) it was the "First Licensed and Regulated Tokenized Crypto Currency Exchange & Index Fund based in the US;" (2) the ICO was registered and approved by the SEC, the CFTC, and the National Futures Association; and (3) the Blockchain Exchange Commission ("BEC")—a fictitious regulatory agency with a fake government seal, logo, and mission statement—regulated their offering (*SEC v. Blockvest, LLC* 2018:*2). In another case, defendants in *In re Tezos Securities Litigation* (2018) also represented that the cryptocurrency Tezos was "a solution to the shortcomings of predominant digital currencies such as bitcoin and Ethereum."

In yet another case, *Balestra v. ATBCOIN LLC* (2019), defendants organized an ICO by offering their virtual currency ATB Coins ("ATB ICO"). According to defendants, the ATB Blockchain would be "the fastest blockchain-based cryptographic network in the Milky Way galaxy," capable of delivering "blazing fast, secure, and near-zero cost payments to anyone in the world" (*Balestra v. ATBCOIN LLC* 2019:*2). Over a three month period, the ICO raised over $20 million from thousands of investors. The ATB Blockchain did not have the technological feats that defendants advertised and the value of ATB Coins plummeted. Six months after the ICO, the value of ATB Coins decreased by more than 85% from its purchase price. Finally, in *Audet v. Fraser* (2017), defendants sold physical virtual currency mining equipments, hardware-hosted mining, cloud-hosted mining, investment contracts called Hashlets that "paid returns" on "virtual currency mining," their own virtual currency, Paycoin, and "investment contracts called HashStakers that held Paycoins and paid holders a fixed return" (*Audet v. Fraser* 2017:*2). These services were fraudulent because defendants did not own the computer hardware and computing power it marketed to its customers. They also falsely claimed that banks, investment firms, and merchants were "financially backing" and "widely adopting it" (*Audet v. Fraser* 2017:

*3).

Third, defendants overestimated their abilities and capacities to provide services promised to investors. In *Audet v. Fraser* (2017), for instance, defendants oversold their computing power by triple and quadruple amounts the number of digital products for which they had the actual ability to support. The sales also occurred before defendants finished setting up the datacenter where support services and infrastructure would be purportedly stored.

Bitcoin scams, bitcoin exchange fraud, and other criminal activities related to bitcoin

Table 5 summarizes the economic, organizational, and behavior dimension of convenience theory as applied to bitcoin scams, bitcoin exchange fraud, and other illegal activities related to the use of bitcoins (*U.S. v. Brown* 2017; *U.S. v. Gross* 2017). The economic motivation for defendant Shrem in *Winklevoss Capital Fund, LLC v. Shrem* (2019) was his desire for the Winklevaus brothers to invest in his company BitInstant to raise the public profile of bitcoin. Shrem offered to purchase bitcoin "at the best price" for the Winklevaus brothers' Winklevaus Capital Fund, LLC ("WCF"). Shrem, however, misappropriated 5,000 bitcoin worth $61,000 from the $750,000 investment of WCF.

Insert Table 5 here

In *Greene v. Mizuho Bank, Ltd.* (2016), defendant Mizuho, a Tokyo-based bank, was motivated by the desire to continue earning service fees from processing incoming Mt. Gox wire deposits. Mt. Gox, a bitcoin exchange based in Tokyo, Japan started experiencing internal problems because: (1) defendant Karpeles (President, CEO, and majority shareholder) was stealing bitcoins belonging to Mt. Gox users and (2) Mizuho was pressuring Karpeles to close

the Mt. Gox bank account at Mizuho due to concerns about a U.S. investigation into money laundering on the Mt. Gox account and potential legal liability or reputational harm to Mizuho. When Karpeles refused to close the account, Mizuho stopped processing international wire withdrawals for Mt. Gox, meaning that Mt. Gox users who wired fiat currency to Mizuho could not withdraw their money. Mizuho, however, did not publicly disclose that it had stopped all international wire transfers out of the Mt. Gox account; instead, defendants continued to accept deposits, which earned revenue from service fees. The plaintiffs were U.S. residents who had wired fiat money to Mizuho for trading in Mt. Gox. After Mt. Gox filed for bankruptcy in Japan on February 28, 2014, plaintiffs could not withdraw the U.S. currency that they wired to Mizuho. Plaintiffs filed a class action lawsuit against Mizuho Bank and Karpeles, asserting claims for tortious interference with contract, unjust enrichment, fraudulent concealment, and accounting. Plaintiffs sought to recover financial losses arising from collapse and bankruptcy of the exchange.

Opportunity: corporate roles allowing breach of fiduciary duty and fraudulent misrepresentation

In the above cases, defendants abused their corporate roles by breaching their fiduciary duty to their clients and corporate stockholders. Defendant Shrem breached his duty of loyalty to WCF by pocketing 5,000 bitcoins instead of turning the same over to his principal client (*Winklevoss Capital Fund, LLC v. Shrem* 2019). Mizuho Bank did not publicly disclose that it had stopped all international wire transfers out of the Mt. Gox account but continued accepting deposits and earning revenues; as a result, investors who continued to deposit money into Mizuho could not withdraw their funds (*Greene v. Mizuho Bank, Ltd.* 2016). Defendants in *Shin v. Time Squared Global, LLC* (2016) also deceived investors through a bitcoin mining scheme where they offered: (1) the opportunity to lease ASIC chips that allegedly would mine bitcoins

and give investors daily revenues from mining and (2) commissions for bringing other investors into the scheme. The scheme was fraudulent because the ASIC chips did not exist and investors who brought in other investors did not receive the promised commissions.

The case of *U.S. v. Gross* (2017) illustrates how defendants Murgio, Lebedev, and Gross abused their corporate positions to defraud corporate stockholders. Murgio and Lebedev operated Coin.mx as an illegal bitcoin exchange. They decided to take full control of a federal credit union to facilitate their bitcoin transactions. They paid $206,000 in bribes to Gross, Chairman of the Board of Directors ("Board") of Helping Other People Excel Federal Credit Union ("HOPE") to enable them to take over the Board of HOPE and to "evade potential scrutiny" from other financial institutions about the nature of their bitcoin business (*U.S. v. Gross* 2017:*1). After taking control of HOPE, defendants allowed KapCharge, a Canadian payment processing company, to process Coin.mx's automated clearing house ("ACH") transactions at HOPE (including its bitcoin transactions). Defendants allowed the processing of ACH transactions that were "unsafe" for the credit union because of lack of efforts to comply with various financial regulations (e.g., the Bank Secrecy Act and the Office of Foreign Asset Control) and the magnitude of these ACH transactions given the level of HOPE's capitalization, which was inconsistent with existing federal regulations (*U.S. v. Gross* 2017:*10). On March 17, 2017, defendant Gross was convicted of two counts: (1) participating in a conspiracy to bribe the Chairman of a federal credit union, obstructing an examination of the National Credit Union Administration ("NCUA"), and making false statements to the NCUA; and, (2) accepting bribes.

The dark web

In several cases, defendants used bitcoin to participate in the dark web or to facilitate their illegal activities, such as drug trafficking and the purchase and sale of illegal drugs. A

category of virtual currency litigation on the dark web involved vendors (*U.S v. Colldock* 2017; *U.S v. Donagal* 2014) or purchasers (*U.S. v. Michell* 2018; *U.S. v. Reuer* 2019) of illegal substances, such as Xanax powder, fentanyl, methamphetamine, and heroin. In these cases, defendants in cryptocurrency litigation involving the dark web were motivated by personal and/or corporate gains. Thousands of vendors, for example, used the dark web Silk Road to sell $183 million worth of illegal drugs, goods, and services. Ulbricht, the owner and operator of Silk Road who operated under the username Dread Pirate Roberts ("DPR"), earned millions of dollars in commissions profits (based on a portion of sellers' revenues) from transactions conducted on Silk Road (*U.S. v. Ulbricht* 2014, 2017). Vallerius, a Paris-based defendant, also acted as operator, administrator, moderator, and vendor of the dark web Dream Market under the username "OxyMonster" (*U.S v. Vallerius* 2018:*1). He received millions of dollars through the use of a bitcoin tip jar or electronic depository. Table 6 summarizes the economic, organizational, and behavior dimension of convenience theory as applied to cryptocurrency litigation involving the dark web.

Insert Table 6 here

Opportunities: anonymity of transactions and layers of security in the dark web

Defendants in cryptocurrency litigation availed themselves of characteristics of the dark web and exploited situational opportunities that allowed them to commit financial crime. The anonymity of transactions on the dark web gave defendants a sense of security that transactions would not be traceable to them by law enforcement authorities. The dark web's guaranty of anonymity is facilitated by: (1) the use of the Tor network that anonymizes internet traffic and makes it difficult to trace; (2) the use of virtual currencies, including bitcoin that enable

anonymous transactions not traceable to specific accounts and users; and (3) the ability to create multiple false accounts without means of identification.

Two related cases illustrate how the intrinsic nature of the dark web facilitates the perpetration of financial crime. Ulbricht, owner and operator of Silk Road under the alias of Dread Pirate Roberts ("DPR"), designed Silk Road as an online criminal marketplace (*U.S. v. Ulbricht* 2014, 2017). The Tor software of Silk Road enabled users to access the Internet anonymously by obscuring users' unique identifying Internet Protocol ("IP") addresses, which prevented surveillance or tracking by law enforcement authorities. All purchases conducted on Silk Road used bitcoins, an anonymous online currency (*U.S. v. Ulbricht* 2017). Between 2011 to 2013, Ulbricht through Silk Road enabled users located "anywhere in the world with an internet connection" to anonymously buy and sell illegal drugs and other illicit goods and services, including: (1) "heroin, cocaine, and lysergic acid diethylamide"; (2) malicious software designed for computer hacking, such as "password stealers, keyloggers, and remote access tools"; and (3) "murder-for-hire" schemes (*U.S. v. Ulbricht* 2014:549-550). In September 2013, after Ulbricht became a primary suspect in the DPR investigation, the government obtained five pen/trap orders under 18 U.S.C. §§ 3121-27 (the "Pen/Trap Act"). The pen/trap orders did not permit access to the content of Ulbricht's communications. Instead, the orders authorized law enforcement agents to "collect IP address data for Internet traffic to and from Ulbricht's home wireless router and other devices that regularly connected to Ulbricht's home router" (*U.S. v. Ulbricht* 2017:83). Ulbricht was arrested in a San Francisco public library on October 1, 2013. On the day of Ulbricht's arrest, the government obtained a warrant to seize Ulbricht's laptop and search it for information related to Silk Road and information that would identify Ulbricht as DPR.

Another characteristic of dark web operations is the ability to reach global markets at a rapid pace (Holt, Burruss, and Bossler 2018). Since the dark web is accessible online by anyone with a reliable computer and an internet connection, its potential reach is only limited by the confines of the internet. The dark web is also capable of operating initially without detection by law enforcement authorities or government regulators. This lack of regulation and visibility at the outset enables it to operate under the radar of government authorities—at least until it reaches a critical mass in terms of transactions and currency before government regulators become aware of its operations.

Conclusion

Analysis of federal case law reveal patterns and methods of perpetrating illegal cryptocurrency activities, including operating unlicensed money transmitting and money service businesses, commodity fraud, securities fraud, bitcoin scams, including bitcoin exchange fraud and corporate takeover of a credit union to perpetuate illegal bitcoin transactions. Other cryptocurrency crime was administered on the dark web, which involved selling and purchasing illegal goods and services. Analysis of U.S. federal district and circuit court case law involving cryptocurrency crimes and fraud indicate support for the convenience theory of white-collar crime. Defendants in various schemes were motivated by financial gain, either for the company or for personal use. Their roles and positions in the businesses allowed them access to resources that helped them perpetrate fraud against clients, investors, and stockholders, including availing of the following opportunities and favorable circumstances: (1) operation of front companies in cases involving unlicensed money transmitting and money service businesses dealing with bitcoins and other virtual currencies; (2) relationship building by defendants and neutralization of blame in cases of commodity fraud; (3) over representing profits that investors would obtain

from purchases of virtual currencies, representing that tokens were safe and reliable investments when they were risky, and overestimating abilities and capacities to provide services promised to investors in securities fraud; (4) breaching fiduciary duties to their clients and corporate stockholders in bitcoin scams by misappropriating profits and service fees to which they were not entitled or using the company for their own personal profits instead of for the stockholders' and investors' benefits; and (5) engaging in dark web transactions by administrators, vendors, and purchasers that were guaranteed anonymity and through an online venue that had far reaching and rapid global access and was not actively regulated by law enforcement or government authorities. Defendants employed various neutralization techniques to justify their crimes, which included allegations of legal mistake and the legality of their actions. Defendants also denied injury or harm, denied responsibility, condemned the condemners, appealed to higher loyalties, and presented dilemma trade-offs by weighing various concerns that resulted in the illegal act, including normality of action.

This article contributes to existing literature in the nascent field of cryptocurrency crime by providing a comprehensive analysis based on federal case law of how various types of cryptocurrency crimes are perpetrated. The article also develops common themes underlying each type of cryptocurrency crime activities, and the reasoning and modus operandi of federal court defendants. The article also uses convenience theory to more fully understand cryptocurrency crimes and fraudulent schemes. Reliance on case law serves as a proxy for interviewing persons involved in cryptocurrency crimes. Future research should empirically examine cryptocurrency crimes to determine the factors that predict either engaging in cryptocurrency crime or victimization in cryptocurrency crime.

References

Adler, Paul S., and Seok-Woo Kwon. 2002. “Social Capital: Prospects for a New Concept.” *The Academy of Management Review* 27:17-40. http://www.jstor.org/stable/4134367.

Agnew, Robert 2014. “Social Concern and Crime: Moving Beyond the Assumption of Simple Self-Interest.” *Criminology* 52:1-32.

Aguilera, Ruth, and Abhijeet K. Vadera. 2008. “The Dark Side of Authority: Antecedents, Mechanisms, and Outcomes of Organizational Corruption.” *Journal of Business Ethics* 77:431-49.

Anello, Robert, and Christina Lee. 2017. “New-Wave Legal Challenges for Bitcoin and Other Cryptocurrencies.” *Law Journal Newsletters.* Retrieved July 8, 2019. (http://www.lawjournalnewsletters.com/2017/11/01/new-wave-legal-challenges-for-bitcoin-and-other-cryptocurrencies/?slreturn=20190326114236).

Arjoon, Surendra. 2008. “Slippery When Wet: The Real Risk in Business.” *Journal of Markets & Morality* 11:77-91.

Ashforth, Blake, Dennis A. Gioia, Sandra L. Robinson, and Linda K. Treviño. 2008. “Re-reviewing Organizational Corruption.” *Academy of Management Review* 33:670-84.

Arnulf, Jan K. and Petter Gottschalk. 2013. “Heroic Leaders as White-Collar Criminals: An Empirical Study.” *Journal of Investigative Psychology & Offender Profiling* 10:96-113.

Benson, Michael, and Sally S. Simpson. 2015. *Understanding White-Collar Crime-An Opportunity Perspective.* New York: Routledge.

Blickle, Gerhard, Alexander Schlegel, Pantaleon Fassbender, and Uwe Klein. 2006. “Some Personality Correlates of Business White-Collar Crime.” *Applied Psychology: An International Review* 55:220-33.

Braaten, Claire 2019. “Chasing the Cryptocurrency Trail Down the Silk Road: Implications for

Prosecution." *Criminal Law Bulletin* 55:685-95.

Brightman, Hank. 2009. *Today's White-Collar Crime: Legal, Investigative, And Theoretical Perspectives.* New York: Routledge, Taylor & Francis Group.

Bucy, Pamela, Elizabeth Formby, Marc Raspanti, and Kathryn Rooney. 2008. "Why Do They Do It? The Motives, Mores, and Character of White-Collar Criminals." *St. John's Law Review* 82:401-571.

Burks, Christopher. 2017. "Bitcoin: Breaking Bad or Breaking Barriers?" *North Carolina Journal of Law & Technology, 18*:244-82.

Chang, Juin-Jen, Huei-Chung Lu, and Ming-Shen Chen. 2005. "Organized Crime or Individual Crime? Endogenous Size of a Criminal Organization and the Optimal Law Enforcement." *Economic Inquiry* 43:661-75.

Collier, Joel, and Sheryl Kimes. 2012. "Only If It Is Convenient: Understanding How Convenience Influences Self-Service Technology Evaluation." *Journal of Service Research* 16:39-51.

Commodity Futures Trading Commission. 2017. *A CFTC primer on virtual currencies*, 1-20. Retrieved June 28, 2019. (https://www.cftc.gov/sites/default/files/idc/groups/public/documents/file/labcftc_primercurrencies100417.pdf).

Dion, Michel. 2008. "Ethical Leadership and Crime Prevention in the Organizational Setting." *Journal of Financial Crime* 15:308-19.

Farquhar, Jillian and Jennifer Rowley. 2009. "Convenience: A Services Perspective." *Marketing Theory* 9:425-38.

Felson, Marcus and Rachel Boba. 2017. *Crime and Everyday Life.* Thousand Oaks, CA: Sage Publications.

Fligstein, Neil, and Alexander Roehrkasse. 2016. "The Causes of Fraud in the Financial Crisis of 2007 to 2009: Evidence from the Mortgage-Backed Securities Industry." *American Sociological Review* 81:617-43.

Galvin, Benjamin, Donald Lange, and Blake E. Ashforth. 2015. "Narcissistic Organizational Identification: Seeing Oneself as Central to the Organization's Identity." *Academy of Management Review* 40:163-81.

Garner, Bryan. 2014. *Black's Law Dictionary*. 10th ed. Eagan, MN: Thomson West.

Giancarlo, J.Christopher. 2016. "Keynote Address of Commissioner J. Christopher Giancarlo Before The Markit Group, 2016 Annual Customer Conference New York." Retrieved July 10, 2019. (http://www.cftc.gov/PressRoom/SpeechesTestimony/opagiancarlo-15)

Giancarlo, J.Christopher. 2018. "Written Testimony of Chairman J. Christopher Giancarlo Before the Senate Banking Committee." Retrieved June 16, 2019 (https://www.banking.senate.gov/imo/media/doc/Giancarlo%20Testimony%202-6-18b.pdf)

Goldstraw-White, Janice. 2012. *White-Collar Crime: Accounts of Offending Behaviour*. London: Palgrave Macmillan.

Gorman, Thomas. 2018. "Blockchain, Virtual Currencies, and the Regulators." Retrieved July 18, 2019 (https://www.secactions.com/blockchain-virtual-currencies-and-the-regulators/).

Gottschalk, Petter. 2017a. "Convenience in White-Collar Crime: Introducing a Core Concept." *Deviant Behavior* 38:605-19.

Gottschalk, Petter. 2017b. *Understanding White Collar Crime: A Convenience Perspective*. Boca Raton, FL: CRC Press.

Gottschalk, Petter. 2018a. "Approaches to the Empirical Study of Convenience Theory for White-Collar Crime." *Deviant Behavior* 39:1600-14.

Gottschalk, Petter. 2018b. "Empirical Study of Convenience Theory: A Student Elicitation On White-Collar Crime." *Deviant Behavior* 39:747-57.

Gottschalk, Petter. 2018c. "Convenience Orientation and White-Collar Criminogenity: An Empirical Study." *Deviant Behavior* 39 1419-26.

Gottschalk, Petter. 2019. "Empirical Evidence of Convenience Theory: Reports of Investigations by Fraud Examiners." *Deviant Behavior* 40:110-21

Hamilton, Stewart and Alicia Micklethwait. 2006. *Greed and Corporate Failure: The Lessons From Recent Disasters.* Basingstoke, UK: Palgrave Macmillan.

Haines, Fiona. 2014. "Corporate Fraud as Misplaced Confidence? Exploring Ambiguity in the Accuracy of Accounts and the Materiality of Money." *Theoretical Criminology* 18:20-37.

Hansen, Laura. 2009. "Corporate Financial Crime: Social Diagnosis and Treatment." *Journal of Financial Crime* 16:28-40.

Heath, Joseph. 2008. "Business Ethics and Moral Motivation: A Criminological Perspective." *Journal of Business Ethics* 83:595-614.

Hern, Alex. 2014. "A History of Bitcoin Hacks." *The Guardian.* Retrieved June 20, 2019. (https://www.theguardian.com/technology/2014/mar/18/history-of-bitcoin-hacks-alternative-currency).

Holt, Thomas, George Burruss, and Adam Bossler. 2018. "Assessing the Macro-Level Correlates of Malware Infections Using a Routine Activities Framework." *International Journal of*

Offender Therapy & Comparative Criminology 62:1720-41.

Hudak, Steve. 2017. "FinCEN Fines BTC-e Virtual Currency Exchange $110 Million for Facilitating Ransomware, Dark Net Drug Sales." *Financial Crimes Enforcement Network.* Retrieved July 13, 2019. (https://www.fincen.gov/news/news-releases/fincen-fines-btc-e-virtual-currency-exchange-110-million-facilitating-ransomware).

Internal Revenue Service. 2014. *Notice 2014–21*. Retrieved July 20, 2019 (https://www.irs.gov/pub/irs-drop/n-14-21.pdf).

Kaptein, Muel and Martien Van Helvoort. 2019. "A Model of Neutralization Techniques." *Deviant Behavior* 40:1260-85.

Kharif, Olga. 2017. "All You Need to Know About Bitcoin's Rise, from $0.01 to $15,000." *Bloomberg Businessweek.* Retrieved June 29, 2019. (https://www.bloomberg.com/news/articles/2017-12-01/understanding-bitcoin-s-rise-0-01-to-11-000-quicktake-q-a)

Kharpal, Arjun. 2018. "Over $60 Billion Wiped Off Value of Cryptocurrencies as Bitcoin Drops Below $8,000 Again." Retrieved June 30, 2019. (https://www.cnbc.com/2018/02/05/bitcoin-price-drops-below-8000-over-60-billion-wiped-off-cryptocurrencies.html).

Langton, Lynn and Nicole Piquero. 2007. "Can General Strain Theory Explain White-Collar Crime? A Preliminary Investigation of the Relationship Between Strain and Select White-Collar Offenses." *Journal of Criminal Justice* 35:1-15.

Litwack, Seth. 2015. "Bitcoin: Currency or Fool's Gold? A Comparative Analysis of the Legal Classification of Bitcoin." *Temple International & Comparative Law Journal* 29:309-48.

Loconte, Richard. 2017. "DFS Grants Virtual Currency License to Coinbase, Inc." Retrieved

August 1, 2019. (https://www.dfs.ny.gov/about/press/pr1701172.htm).

Mai, Huynh Thi Xuan and Svein Ottar Olsen. 2016. "Consumer Participation in Self-Production: The Role of Control Mechanisms, Convenience Orientation, and Moral Obligation. *Journal of Marketing Theory & Practice* 24:209-23.

Merriam Webster. 2019. "Commodity." Retrieved August 1, 2019. (https://www.merriam-webster.com/dictionary/commodity).

Nikkei Asian Review. 2017. "Japan Tries Light Touch in Bringing Cryptocurrencies Out of Regulatory Limbo." Retrieved August 5, 2019. (https://asia.nikkei.com/Business/Banking-Finance/Japan-tries-light-touch-in-bringing-cryptocurrencies-out-of-regulatory-limbo).

Nolasco, Claire, Rolando V. del Carmen, Kevin Steinmetz, Michael S. Vaughn, and Aneta Spaic. 2015. "Building Legal Competency: Foundations for a More Effective Criminology and Criminal Justice Discipline." *Journal of Criminal Justice Education* 26:233-52.

Nolasco, Claire and Michael S. Vaughn. 2010. "Judicial Scrutiny of Gender-Based Employment Practices in Criminal Justice Agencies." *Journal of Criminal Justice* 39:106-19.

Nolasco, Claire, Michael S. Vaughn, and Rolando V. del Carmen. 2010. "Toward a New Methodology for Legal Research in Criminal Justice." *Journal of Criminal Justice Education* 21:1-23.

Nolasco, Claire, Michael S. Vaughn, and Rolando V. del Carmen. 2013. "Revisiting the Choice Model of Ponzi Schemes: Review of Case Law." *Crime, Law, & Social Change* 60:375-400.

Oedel, David. 1997. "Why Regulate Cybermoney?" *American University Law Review* 46:1075-1103.

Ouimet, Gerard. 2009. “Psychology of White-Collar Criminal: In Search of Personality.” *Psychologie Du Travail Et Des Organisations* 15:297-320.

Pickett, K.H. Spencer and Jennifer Pickett. 2002. *Financial Crime Investigation, and Control.* New York: John Wiley & Sons.

Piquero, Nicole. 2012. “The Only Thing We Have To Fear Is Fear Itself: Investigating The Relationship Between Fear Of Falling And White Collar Crime.” *Crime & Delinquency,* 58:362-79.

Pontell, Henry, William Black, and Gilbert Geis. 2014. “Too Big To Fail, Too Powerful To Jail? On the Absence of Criminal Prosecutions After the 2008 Financial Meltdown.” *Crime, Law, & Social Change* 61:1-13.

Popper, Nathaniel. 2017. “Coinbase: The Heart of the Bitcoin Frenzy.” *New York Times.* Retrieved June 30, 2019. (https://www.nytimes.com/2017/12/06/technology/coinbase-bitcoin.html).

Pratt, Travis and Francis Cullen. 2005. “Assessing Macro-Level Predictors and Theories of Crime: A Meta-analysis.” *Crime & Justice* 32:373-450.

Prentis, Mitchell. 2015. “Digital Metal: Regulating Bitcoin as a Commodity.” *Case Western Reserve Law Review* 66:609-38.

Punch, Maurice. 2003. “Rotten Orchards: Pestilence, Police Misconduct, and System Failure.” *Policing & Society* 13:171-96.

Puranam, Phanish, Oliver Alexy, and Markus Reitzig. 2014. “What’s ‘New’ About New Forms of Organizing?” *Academy of Management Review* 39:162-80.

Reed, Gary and Peter Yeager. 1996. “Organizational Offending and Neoclassical Criminology: Challenging the Reach of a General Theory of Crime.” *Criminology* 34:357-82.

Sanchez, Edgar. 2017. “Crypto-Currencies: The 21st Century’s Money Laundering and Tax Havens.” *University of Florida Journal of Law & Public Policy* 28:169-91.

Siponen, Mikko, and Anthony Vance. 2010. “Neutralization: New Insights Into the Problem of Employee Information Security Policy Violations.” *MIS Quarterly* 34:487-502.

Sutherland, Edwin. 1939. “White-collar Criminality.” *American Sociological Review* 5:1-12.

Sykes, Gresham, and David Matza. 1957. “Techniques of Neutralization: A Theory of Delinquency.” *American Sociological Review* 22:664-70.

Trahan, Adam, James Marquart, and Janet Mullings. 2005. “Fraud and the American Dream: Toward an Understanding of Fraud Victimization.” *Deviant Behavior* 26:601-20.

U.S. Dep’t of Treasury, FinCEN. 2013. “FIN-2013-G001, Guidance: Application of FINCEN’s Regulations to Persons Administering, Exchanging, or Using Virtual Currencies.” Retrieved August 16, 2019. (http://fincen.gov/statutes_regs/guidance/pdf/FIN–2013–G001.pdf).

Van Koppen, M. Vere, Christianne Poot, and Arjan Blokland. 2010. “Comparing Criminal Careers of Organized Crime Offenders and General Offenders.” *European Journal of Criminology* 7:356-74.

Welsh, David, Lisa Oronez, Deirdre Snyder, and Michael Christian. 2014. The Slippery Slope: How Small Ethical Transgressions Pave the Way for Larger Future Transgressions.” *Journal of Applied Psychology* 100:114-27.

Wilson, Thomas, Hideyuki Sano, and Marius Zaharia. 2018. “The Coincheck Hack and the Issue with Crypto Assets on Centralized Exchanges.” *Thomson Reuters.* Retrieved August 5, 2019. (https://www.reuters.com/article/us-japan-cryptocurrency-q-a/the-coincheck-hack-and-the-issue-with-crypto-assets-on-centralized-exchanges-idUSKBN1FI0K4).

Young, Mark, Maureen Donley, and Theodore Kneller. 2016. "Bitcoins and Blockchain: The CFTC Takes Notice of Virtual Currencies." Retrieved July 16, 2019. (https://www.skadden.com/insights/publications/2016/01/bitcoins-and-the-blockchain-the-cftc-takes-notice).

Cases Cited

Audet v. Fraser, 2017 WL 4542386 (D. Conn. 2017).

Balestra v. ATBCOIN LLC, 380 F.Supp.3d 340 (S.D. N.Y. 2019).

Boumediene v. Bush, 553 U.S. 723 (2008).

Clark v. Rameker, 134 S. Ct. 2242 (2014).

Commodity Futures Trading Comm'n v. Commodity Inv. Grp., Inc., 2006 WL 353466 (S.D. N.Y. 2006).

Commodity Futures Trading Comm'n v. Hunter Wise Commodities, LLC, 21 F.Supp.3d 1317 (S.D. Fla. 2014).

Commodity Futures Trading Commission v. McDonnell, 287 F.Supp.3d 213 (E.D. N.Y. 2018a), *adhered to on denial of reconsideration*, 321 F.Supp.3d 366 (E.D. N.Y. 2018).

Commodity Futures Trading Commission v. McDonnell, 332 F.Supp.3d 641 (E.D. N.Y. 2018b).

Commodity Futures Trading Commission v. My Big Coin Pay, Inc., 334 F.Supp.3d 492 (D. Mass. 2018).

Commodity Futures Trading Comm'n v. R.J. Fitzgerald & Co., Inc., 310 F.3d 1321 (11th Cir. 2002), *rehearing and rehearing en banc denied*, 103 Fed.Appx. 668 (11th Cir.), *cert. denied, R.J. Reynolds & Co., Inc., v. Commodity Futures Trading Comm'n*, 543 U.S. 1034 (2004).

Commodity Futures Trading Comm'n v. S. Tr. Metals, Inc., 894 F.3d 1313 (11th Cir. 2018), *cert.*

denied, Southern Trust Medals Inc. v. Commodity Futures Trading Comm'n., 139 S.Ct 1464 (2019), *on remand, Commodity Futures Trading Comm'n. v. Southern Trust Medals, Inc.*, ___ F.Supp.3d ___, 2019 WL 2295488 (S.D. Fla. 2019),

Greene v. Mizuho Bank, Ltd., 206 F.Supp.3d 1362 (N.D. Ill. 2016).

Gugick v. Melville Capital, LLC, 2014 WL 349526 (S.D. N.Y. 2014).

Hodges v. Harrison, 372 F.Supp.3d 1342 (S.D. Fla. 2019).

In re Tezos Securities Litigation, 2018 WL 4293341 (N.D. Cal. 2018).

In the Matter of: Coinflip, Inc., CFTC Docket No. 15-29 (2015).

Nix v. Hedden, 149 U.S. 304 (1893).

Scheck Invs., L.P. v. Kensington Mgmt., Inc., 2009 WL 10668565 (S.D. Fla. 2009).*Securities and Exchange Commission v. Blockvest, LLC*, 2018 WL 4955837 (S.D. Cal. 2018).

Securities and Exchange Commission v. Dain Rauscher, Inc., 254 F.3d 852 (9th Cir. 2001).

Securities and Exchange Commission v. Edwards, 540 U.S. 389 (2004).*Securities and Exchange Commission v. Plexcorps*, 2017 WL 5988934 (E.D. N.Y. 2017).

Securities and Exchange Commission v. PlexCorps, 2018 WL 3038500 (E.D. N.Y. 2018a).

Securities and Exchange Commission v. PlexCorps, 2018 WL 4299983 (E.D. N.Y. 2018b).

Securities and Exchange Commission v. Shavers, 2013 WL 4028182 (E.D. Tex. 2013), *adhered to on reconsideration*, 2014 WL 12622292 (E.D. Tex. 2014).

Securities and Exchange Commission v. Unique Fin. Concepts, Inc., 119 F.Supp.2d 1332 (S.D. Fla. 1998), *aff'd.*, 196 F. 3d 1195 (11th Cir. 1999).

Securities and Exchange Commission v. W.J. Howey Co., 328 U.S. 293 (1946).

Shin v. Time Squared Global, LLC, 2016 WL 8856653 (C.D. Cal. 2016).

Tippens v. Round Island Plantation LLC, 2009 WL 2365347 (S.D. Fla. 2009).*United Hous.*

Found., Inc. v. Forman, 421 U.S. 837 (1975).

U.S. v. Brown, 68 F.Supp.3d 783 (M.D. Tenn. 2014), *aff'd.*, 857 F.3d 334 (6th Cir. 2017).

U.S. v. Budovsky, 2015 WL 5602853 (S.D. N.Y. 2015).

U.S. v. Coinbase, Inc.,, 2017 WL 3035164 (N.D. Cal. 2017).

U.S. v. Colldock, 2017 WL 9615895 (D. Ariz. 2017), *report and recommendation adopted*, 2018 WL 3069477 (D. Ariz. 2018).

U.S. v. Donagal, 2014 WL 4418192 (N.D. Cal.), *aff'd.*, 2014 WL 6601843 N.D. Ca. 2014).

U.S. v. Faiella, 39 F.Supp.3d 544 (S.D. N.Y. 2014).

U.S. v. Gross, 2017 WL 4685111 (S.D. N.Y. 2017), *aff'd.*, *U.S. v. Lebedev*, 932 F.3d 40 (2nd Cir. 2019).

U.S. v. Leonard, 529 F.3d 83 (2nd Cir. 2008), *appeal after new sentencing hearing, aff'd.*, *U.S. v. Newsom*, 399 Fed.Appx. 625 (2nd Cir. 2010), *cert. denied*, *Dickau v. U.S.*, 562 U.S. 1263 (2011).

U.S. v. Lord, 2017 WL 1424806 (W.D. La. 2017), *aff'd*., 915 F.3d 1009 (5th Cir. 2019).

U.S. v. Lott, 750 F.3d 214 (2nd Cir.), *cert. denied*, 135 U.S. 253 (2014).

U.S. v. Mansy, 2017 WL 9672554 (D. Me. 2017).

U.S. v. Michell, 2018 WL 2688803 (D. Ariz. 2018).

U.S. v. Murgio, 209 F. Supp. 3d 698 (S.D. N.Y. 2016).

U.S. v. Petix, 2016 WL 7017919 (W. D. N.Y. 2016).

U.S. v. Reuer, 2019 WL 1012187 (D. S.D. 2019).

U.S. v. Stetkiw, 2019 WL 422200 (E.D. Mich. 2019).

U.S. v. Ulbricht, 31 F.Supp.3d 540 (S.D. N.Y.2014).

U.S. v. Ulbricht, 858 F.3d 71 (5th Cir. 2017), *cert. denied*, 138 S.Ct. 2708 (2108).

U.S. v. Vallerius, 2018 WL 2325729 (S.D. Fla. 2018), *report and recommendation adopted*, 2018 WL 2324059 (S.D. Fla. 2018).

Villeneuve v. Advanced Bus. Concepts Corp., 698 F.2d 1121 (11th Cir. 1990).

Walters v. Metro. Educ. Enterprises, Inc., 519 U.S. 202 (1997).

Winklevoss Capital Fund, LLC v. Shrem, 351 F.Supp.3d 710 (S.D. N.Y. 2019).

Yates v. U.S., 135 S. Ct. 1074 (2015).

Laws Cited

17 C.F.R. §180.1

31 C.F.R. § 1022.380(b)(3)

7 U.S.C. § 1(a)(9)

7 U.S.C. § 9(1)

18 U.S.C. § 337

18 U.S.C. § 1956(h)

18 U.S.C. § 1960(a), (b)(2)

18 U.S.C. §§ 3121-27