

# Cryptocurrency: Rich or Glitched?

## The Path to Protecting Investor Interests



By: Lora Bishop

Lora Bishop  
Rigorous Writing Paper – Final

***Cryptocurrency and cryptic criminals: How does the government step in to protect consumer interests in an industry utterly opposed to regulation?***

*Lora C. Bishop*

## **I. Introduction**

When most people think of cryptocurrencies, virtual tokens, and online trading, they may think of places like Bitcoin, Coinbase or Crypto.com. These online exchange platforms allow investors to trade real assets for virtual tokens in hopes of turning a profit. Most of the influencers who encourage use of these platforms describe it as an investment opportunity that yields outrageous returns and little regulation. While this may seem like an investor's dream, the lack of regulation has let scammers, thieves and fraudsters run rampant on any number of the exchange platforms. This prevailing problem can have dire consequences for many people. Losing any amount of money that you have worked long and hard for is devastating, and the lack of opportunity to obtain relief might send victims into a spiral they never climb out of. This paper will explore what virtual trading exactly entails, its legal landscape as of today, arguments for the inclusion of cryptocurrency in current legislation and regulation, and proposals for legislation in an effort to curtail the theft of assets that has been a prevailing problem in the arena since its inception in 2009.

## **II. Cryptocurrency and the virtual world: What is it? Where did it come from?**

Bitcoin, Kraken, Crypto.com and other platforms used for the trading of “cryptocurrencies” allow investors to trade virtual currency over the internet through a virtual

“address.”<sup>1</sup> Trade in this arena of investment is controlled by computer software and code instead of the traditional way of issuing currency through banks and other financial institutions. The virtual address used by investors of bitcoin is a “unique string of characters akin to a bank account number,” and each person controls their address with a password or “private key.”<sup>2</sup> Cryptocurrencies are traded on online platforms called “exchanges,” which, “allow customers to exchange virtual currencies for conventional money . . . .”<sup>3</sup> While Bitcoin is the most heavily used, there are more than 1,000 types of “virtual coins or tokens” circulating the market today.<sup>4</sup> Bitcoin and other virtual coins and currency like it are “computer codes created and maintained on a blockchain.”<sup>5</sup> Virtual tokens are held on a blockchain that merely consists of a string of numbers on an “electronic ledger.”<sup>6</sup> Bitcoin and other virtual currency are not yet recognized as legal tender, and the tokens that “you ‘hold’ in your ‘wallet’ (account) is just an entry [on that electronic ledger].”<sup>7</sup>

One scholar, Celiza P. Bragança, gives an example of what this combination of symbols might look like “[000000000000000000000000052138b6fe93e686b52]” in her law review article exploring what exactly cryptocurrency is and what legislation is in place to regulate them.<sup>8</sup> This article explains the issues with using ledger IDs like the one above, when comparing it to a traditional record of account in a concrete banking institution. She explains that an individual’s

---

<sup>1</sup> United States v. Twenty-Four Cryptocurrency Accounts, 473 F. Supp. 3d 1, 3 (2020).

<sup>2</sup> *Id.*

<sup>3</sup> *Id.*

<sup>4</sup> Celiza Bragança & Louis L. Straney, *Cryptocurrencies and Tokens: What Are They and Who Regulates Them?*, 25 No. 1 PIABA B.J. 39, 40 (2018).

<sup>5</sup> *Id.*

<sup>6</sup> *Id.* at 42.

<sup>7</sup> *Id.*

<sup>8</sup> *Id.*

bitcoin “might exist in thousands of separate identical ledgers around the world,” but might only intend to reflect one transfer of one bitcoin between two separate parties.<sup>9</sup>

As of 2017, Bitcoin is one of the best performing virtual currencies.<sup>10</sup> The drastic rise and fall in price within Bitcoin investments has sparked heated debate and controversy, with some of the general public comparing virtual trading and currencies to the fluctuating popularity crazes of low-rise jeans or maximalist home décor. Bitcoin was first “coined” or created in 2009 by an entity using the alias “Satoshi Nakamoto.”<sup>11</sup> The idea proposed behind the invention was that “two willing parties” would be able to conduct a transaction with each other personally, curtailing the need for “trusted third part[ies],” and dodging regulations and the need for authorization and permittance from places like the Securities and Exchange Commission and other financial regulatory institutions.<sup>12</sup> Circulating bitcoin currently has a value of over \$200 billion, only surpassed by legitimate sovereign and legal tenders in the United States, the European Union, and Japan.<sup>13</sup> While virtual currency has enjoyed a rise in usage and popularity, a common theme in scholarly articles today begs the question: will it ever replace legal and sovereign currency?

### **III. The Pig Butchering Scam: Leading the victim to their proverbial slaughter.**

Although virtual trading has its advantages and entices investors of a wide variety of skill level, it has its dangers too. Federal and local investigative agencies struggle to provide victims of scams on these platforms any real or substantive relief. Special Agent Miles Faggert, of the

---

<sup>9</sup> Id. at 43.

<sup>10</sup> Id. at 40.

<sup>11</sup> Id. at 41.

<sup>12</sup> Id. at 42.

<sup>13</sup> Id. at 43.

Alabama Securities Commission has stated that many of his investigations into fraudulent platforms are frustrated by the lack of legislation that would allow prosecution of the perpetrators or remedies for their victims.<sup>14</sup> One scam in particular, the Pig Butchering Scam, is taking over the market today and has affected people everywhere across the United States.

The Pig Butchering Scam is essentially an online romance scam that targets “lonely” individuals looking for companionship, that are particularly susceptible to the type of fraud perpetuated in these types of scams. Generally, a scammer will target someone based on their social media accounts. These people will look for individuals that have recently suffered a loss, specifically of their spouse or a close loved one, or elderly people that do not seem to have any family that lives in close proximity or any family at all.<sup>15</sup> The scam begins when they obtain the victim’s phone number and send a text that is “intended” for someone else. The most common initial text message may be in “response” to a non-existent craigslist post, or a message stating that the scammer found the victim’s lost dog.<sup>16</sup> Once the victim responds to say that they have the wrong number, the scammer will initiate conversation and start working to gain the victim’s trust and develop a personal friendship.<sup>17</sup> This process takes great patience, and this scam could last over a year before the victim ever transfers any money or realizes that they have been lied to.

Usually, the process begins when, after the victim views the scammer as someone they trust and rely on, the scammer convinces the victim that they are proficient in cryptocurrency and can help them make great investments with “unbelievable returns.” This is where the victim will be convinced to transfer money from their bank account to a legitimate exchange platform like

---

<sup>14</sup> Interview of Special Agent Miles Faggert of the Alabama Securities Commission conducted by the author on April 11, 2023 (*Original transcripts on file with the author*).

<sup>15</sup> Information obtained during an internship completed by the author during the summer of 2022.

<sup>16</sup> *Id.*

<sup>17</sup> *Id.*

Bitcoin, Kraken, Nexo, Webull, or Crypto.com. The scammer will walk the victim through the steps and usually allow them to withdraw small amounts to maintain their trust before shutting down any transfers. After this, the scammer will tell the victim that the legitimate exchange platform has updated their domain name and have the victim transfer everything she has into a fraudulent site that often mimics any number of legitimate exchange platforms exactly in appearance and operation.

As time goes on, victims will invest more and more money without attempting a withdrawal at the instruction of the scammer. When the victim inevitably decides that it is time to enjoy the profit, they think they have made, the “website” or fraudulent platform will tell them that they must pay exorbitant amounts of money in taxes directly to the site in order to withdraw the money. The victims often have already put everything they have into these sites, and therefore cannot make the payment. The scammer will keep up the ruse for as long as they can, convincing the victims to borrow from friends and family to make the tax payments before she even realizes what is happening. By this point, most victims have invested retirement savings, emergency funds, business accounts, and personal accounts into the fraudulent site and are left with nothing. Once a scammer has determined that he will no longer be able to squeeze any more money out of his target, he disappears.

The problem with these types of scams is that they are virtually untraceable. When an investigation is opened, it can usually be determined that just one or two people are behind hundreds to nearly a thousand different fraudulent domain names.<sup>18</sup> These people could be using multiple email addresses, and several different wallet addresses that are used to store stolen money through virtual trade accounts.<sup>19</sup> It can take years to sift through all the different

---

<sup>18</sup> Id.

<sup>19</sup> Id.

variations of domain names that have cropped up to imitate any number of legitimate exchange platforms, and it can take just as long to connect with the people affected by these scams in an effort to organize all the data needed to build a case. Even after gathering transaction hashes, wallet addresses, and account IDs from the pool of victims, a successful investigation can usually only hope to shut down each fraudulent site named in a complaint. Even still, when these websites are shut down, three more can crop up in its place and undermine any hard work put forth by investigative agencies.

Special Agent Miles Faggert speaks a little about the obstacles he and his colleagues face at the Alabama Securities Commission:

The [ASC] is working towards the ability to go and seize cryptocurrency from identified suspect accounts that are held at cryptocurrency exchanges (Binance, Coinbase, Kraken, etc.). For the past year, we have been educating ourselves on how to trace cryptocurrency and how to serve legal processes such as subpoenas and search warrants to these exchanges. A large number of exchanges are located overseas and are not required to honor U.S. legal processes . . . [c]ases in which exchanges do not comply [currently] results in a closure of the case.<sup>20</sup>

While Alabama is one of the states working toward the ability to seize stolen funds from suspects utilizing legitimate exchanges, the legal hurdles will lengthen the process. For now, places like the Alabama Securities Commission issue cease and desist orders to the domain provider of websites on which the fraud is taking place. Special Agent Faggert tells us that these “cease and desist orders would state violations of not being registered in the state of Alabama and also

---

<sup>20</sup> Interview of Special Agent Miles Faggert of the Alabama Securities Commission conducted by the author on April 11, 2023 (*Original transcripts on file with the author*).

allege the fraud taking place.”<sup>21</sup> The only good this does generally is force the domain provider to suspend the website alleged in the order.

The Alabama Securities Commission is authorized under Section 8-6-15 of the Alabama Securities Act to open investigations into alleged cryptocurrency fraud if it views the cryptocurrency as an investment product.<sup>22</sup> While this section of the Alabama Code merely requires filing with the ASC, investigations into virtual fraud can also be authorized by Alabama’s “Elderly and Vulnerable Adult Financial Protection Act of 2021.”<sup>23</sup> Financial Exploitation in this article is defined as “the wrongful or unauthorized taking, withholding, appropriation, or use of money, assets, or property of an elderly adult . . . .”<sup>24</sup> A financial transaction is in relevant part defined as “a transfer or request to transfer or disburse funds or assets in an account.”<sup>25</sup>

Special Agent Faggert is working hard in Alabama to combat fraudulent activity in the industry, and advocates for the expansion of the rules and regulation under the Treasury Department’s Financial Enforcement Network and the Code of Federal Regulations, but he laments over the lack of action taken by other investigatory agencies, “as far as what other securities regulators are doing to seize cryptocurrency[,] the answer is nothing.”<sup>26</sup>

It may be hard to discern the difference between cryptocurrency scams and a number of financial scams that happen every day. While they may be similar in principle, traditional financial scams could come to a definitive end with a person being charged, hauled into court,

---

<sup>21</sup> Id.

<sup>22</sup> Ala. Code § 8-6-15, The Alabama Securities Act (1975).

<sup>23</sup> Ala. Code § 8-6-190, 195, Elderly and Vulnerable Adult Financial Protection Act (2021).

<sup>24</sup> Id.

<sup>25</sup> Id.

<sup>26</sup> Interview of Special Agent Miles Faggert of the Alabama Securities Commission conducted by the author on April 11, 2023 (*Original transcripts on file with the author*).



and being ordered to pay damages to the victim. Yet what can be done about a faceless name that could be located anywhere in the world, scamming unsuspecting people in a virtually unregulated arena?

#### **IV. What now? The United States government is struggling to find ways to “regulate the unregulatable”<sup>27</sup> with existing legislation.**

The cryptocurrency market is virtually unregulated, but there have been calls from representatives and citizens alike to do something about the rampant criminal activity that permeates the market at every level. While some investors fear that the government stepping in might stifle the industry’s growth, the call for amendments to current legislation or new laws has nevertheless gained traction over the years as more and more investors fall victim to fraudulent activity. One of the greatest obstacles to regulating the cryptocurrency market is lack of “statutory jurisdiction over the industry.”<sup>28</sup> In her article “Regulating the Unregulatable,” Becky Powell discusses one proposal in particular that former Congressman Michael Conway (TX) introduced called the “Digital Commodity Exchange Act (DCEA),” that would “give the Commodity Futures Trading Commission (CFTC) explicit jurisdiction over cryptocurrency when used as a commodity.”<sup>29</sup> Acts and legislation like these would give the federal government more freedom to monitor and supervise cryptocurrency based on how it is used and create the “societal trust that the industry needs to continue to develop successfully.”<sup>30</sup>

This act created the space needed to pass future legislation, and opened the door for prosecution of individuals who abused the market in the specific way in which the act defines

---

<sup>27</sup> Becky Powell, *Regulating the Unregulatable: The Digital Commodity Exchange Act’s Use-Based Approach to Cryptocurrency Regulation*, B.C. Intell. Prop. & Tech. F. 1 (2021).

<sup>28</sup> Id.

<sup>29</sup> Id.

<sup>30</sup> Id.

virtual currencies, but still falls short of encompassing all transactions that take place in the virtual world. The United States District Court for the Eastern District of New York has had one such occasion to prosecute fraud and crime under the jurisdiction of the Commodity Futures Trading Commission and the Digital Commodity Exchange Act.<sup>31</sup> The court here states that “virtual currencies are generally defined as ‘digital assets used as a medium of exchange.’”<sup>32</sup> While courts and the CFTC admit that “congress has yet to authorize a system to regulate virtual currency,” and that “U.S. law does not provide for ‘direct comprehensive U.S. regulation of virtual currencies,’” regulatory oversight of virtual tokens in specific settings – like when it is used as a commodity – is a step in the right direction.<sup>33</sup>

This paper explores the potential to punish individuals who commit fraud through virtual currency and to provide remedies to those victims who have been affected, but many have argued that this is not the best approach. The court in *McDonnell* emphasized the point that former President Roosevelt once made, stating:

“Roosevelt . . . continued to regard the judicial system as an ineffective arena for controlling giant corporations . . . . Regulation, he believed, promised a far better remedy. ‘The design should be to prevent the abuses incident to the creation of unhealthy and improper combinations [] instead of waiting until they are in existence and then attempting to destroy them by civil or criminal proceedings.’”<sup>34</sup>

While regulation might be synonymous with the saying “an ounce of prevention is worth a pound of cure” when viewed in this way, it is arguably a well-known truism that criminals are

---

<sup>31</sup> *CFTC v. McDonnell*, 287 F. Supp. 3d 213 (E.D.N.Y. 2018).

<sup>32</sup> *Id.* at 218.

<sup>33</sup> *Id.* at 220.

<sup>34</sup> *Id.* (quoting Doris Kearns, *The Bully Pulpit*, at 443 (2013)).

undeterred by regulation alone. The most popular purpose for punishment, deterrence, is better achieved by doling out consequences for actions when they are committed.

**A. Give the people what they want: Proposals currently on the table could be the answer, but is there one perfect solution? Probably not.**

However courts across the United States feel about what needs to be done, there are recognized variations of possibilities to address the plethora of problems and criminal activity that the virtual currency market has encouraged. The *McDonnell* court listed a few to begin with that include:

(1) no regulation, (2) partial regulation through criminal law prosecutions of Ponzi-like schemes by the Department of Justice, or state criminal agencies, or civil substantive suits based on allegations of fraud, (3) Regulation by the Commodity Futures Trading Commission, (4) Regulation by the Securities and Exchange Commission (“SEC”) as securities, (5) Regulation by the Treasury Department’s Financial Enforcement Network (“FinCEN”), (6) Regulation by the Internal Revenue Service (“IRS”), (7) Regulation by private exchanges, (8) State regulations, or (9) a combination of any of the above.<sup>35</sup>

It is important to recognize all the different avenues that could lead to regulation, to recognize that the United States is not powerless to protect its citizens from instances of fraud, theft, and black-market criminal activity.

The first suggestion, which is implementing no regulation, could arguably be the easy way out. This an economically conservative view that champions the rights of United States consumers but fails to see the importance of protecting the investments and assets that people work hard to obtain. In support of this view, the court here cites Nikolei M. Kaplanov’s article

---

<sup>35</sup> *Id.* at 220, 221.

“Nerdy Money: Bitcoin, the Private Digital Currency, and the Case Against Its Regulation.”<sup>36</sup>

The article argues that “the federal government should refrain from passing any laws or regulations limiting the use of bitcoins, and applying any sort of regulation to bitcoin use [] would be ineffective and contrary to the interest of the United States consumers.”<sup>37</sup> Like the argument above stating that regulation alone might not be the *most* effective in deterring criminal activity in the virtual world, making the argument that no regulation at all would be in any way a solution is counter-productive to the goals and vested interest our government has in protecting its consumers. While implementing no regulation at all may be more attractive to big corporations and entities that can bounce back from theft and fraud, the middle-class dad of four or the retired elderly vet may not have the same luxury, and the losses could prove devastating.

The second suggestion, “partial regulation through criminal law prosecutions of Ponzi-like schemes by the Department of Justice, or state criminal agencies, or civil substantive suits based on allegations of fraud,”<sup>38</sup> supports more the notion that perpetrators of such activity will more than likely be citizens of the United States that can be reached by statutory jurisdiction already. This would be great when that is the case, but what can be done about citizens that have been victimized by overseas bad actors? It could be argued that this type of potential regulation is an even stronger argument against no regulation at all. Although the United States hales itself as the country of rights and freedoms, could regulations that supervise and limit overseas virtual transactions be the answer? If virtual investors were open to the idea, regulation of foreign transactions in conjunction with prosecution of criminal citizens here might be a good balance to address the unchecked crime and fraud. The court here provided two cases in support of this

---

<sup>36</sup> Id. at 220 (*quoting* Nikolei M. Kaplanov, *Nerdy Money: Bitcoin, the Private Digital Currency, and the Case Against Its Regulation*, 25 *Loy. Consumer L. Rev.* 111, 113 (2012)).

<sup>37</sup> Id.

<sup>38</sup> Id. at 220, 221.

argument. Both cases cited here, *Faiella* and *Lord*, involve underground black markets and fraudulent activities pertaining to the defendants' exchange business.<sup>39</sup> As noted above, cases like these do little to address the issue of preventing fraud like the Pig Butchering Scam.

Regulation by the CFTC might be the best course of action even without “concurrent oversight” by other regulatory agencies like the Securities and Exchange Commission. The court explores the “important role” that the CFTC has to play when implementing a “responsible regulatory strategy.”<sup>40</sup> The CFTC in 2015 made an important step in an effort to broaden its oversight abilities of virtual trading through an administrative order [the “Coinflip Order”], that showcased for the first time the CFTC’s desire to extend jurisdiction. Conrad Bahlke’s article “Recent Developments in the Regulatory Treatment of Bitcoin,” states:

On September 17, 2015, the [CFTC] issued an [administrative] order (the Coinflip Order) filing and simultaneously settling charges against Coinflip, Inc. (Coinflip) and its chief executive officer. In the Coinflip Order, the CFTC took the view for the first time that bitcoin and other virtual currencies are commodities subject to the Commodity Exchange Act (CEA) and CFTC regulations.<sup>41</sup>

Even so, this order is primarily focused on future trading abilities of corporations that would “make it possible to bet on bitcoin prices without buying the cryptocurrency.”<sup>42</sup> While this does give consumers the safer option of trading and betting through larger corporations without the risk of loss to one individual party, legislation has failed to consider the underlying motivation for the creation of virtual currency: direct transactions between two individuals without the need

---

<sup>39</sup> Id. (See United States v. Faiella, 39 F. Supp. 3d 544, 545 (S.D.N.Y. 2014) & United States v. Lord, No. CR 15-00240-01/02, WL 1424806, at \*2 (W.D. La. Apr. 20, 2017)).

<sup>40</sup> Id. at 222.

<sup>41</sup> Id. (see Conrad Bahlke, *Recent Developments in the Regulatory Treatment of Bitcoin*, No. 1 Intell. Prop. & Tech. L.J. 6 (2016)).

<sup>42</sup> Id.

for a trusted third party. This suggestion only attempts to protect initial experiments with virtual trading synonymous with “dipping your toe in the water.”

The court’s next suggestion, “regulation by the Securities and Exchange Commission (“SEC”) as securities,” is supported with a case most comparable to the issue we hope to address. In SEC v. Plexcorps, the plaintiff brought an action against a “recidivist securities law violator in Canada,” from “further misappropriated investor funds illegally raised through the fraudulent and unregistered offer and sale of securities . . . in a purported ‘Initial Coin Offering.’”<sup>43</sup> The defendants here offered the sale of securities but failed to file a registration statement with the Securities and Exchange Commission.<sup>44</sup> The securities or “tokenized currency” was offered to the general public promising investors the opportunity to “Take control of [THEIR] money!”<sup>45</sup> Investors were promised outrageous profits stemming from:

(i) the appreciation in value of the PlexCoin Token through investments PlexCorps would make with the proceeds of the PlexCoin ICO and based on the managerial efforts of PlexCorps’ team of supposed experts; (ii) the distribution to investors of profits from the PlexCorps enterprise; and (iii) the appreciation in value of the PlexCoin Tokens based on the efforts of PlexCorps’ “market maintenance” team, which included listing the token on digital asset exchanges.<sup>46</sup>

While this case involves a foreign corporation rather than an individual party, the facts here still apply. Citizens of the United States were scammed out of their own money and the investments they made in hopes of a profitable return. Instead of the victim’s funds going into the corporation to be traded and dispersed back to investors, the money put in instead went to a variety of wallet

---

<sup>43</sup> Id. at 221 (see SEC v. Plexcorps, 17-CV-7007, 2017 WL 5988934 (E.D.N.Y Filed Dec. 1, 2017)).

<sup>44</sup> SEC v. Plexcorps, 17-CV-7007, 2017 WL 5988934 (E.D.N.Y. Filed Dec. 1, 2017).

<sup>45</sup> Id.

<sup>46</sup> Id.

addresses all personally controlled by the defendants.<sup>47</sup> With the false advertising, promise of great return, and misappropriation of funds, this case is the closest a court has come to addressing the issue faced here. The court determined that the defendants had violated Section 17(a) and 10(b) of the Securities Act of 1933, and Rule 10b-5 of Title 17 of the Code of Federal Regulations by “engag[ing] in ongoing securities fraud.”<sup>48</sup> The complaint alleged that the defendants had further violated numerous other sections of the Securities Act and Title 17 of the Code of Federal Regulations by “engaging in the unlawful sale and offer to sell securities . . . .” to their victims.<sup>49</sup> The Commission sought relief in the following forms:

(1) a temporary restraining order and preliminary injunction against Defendants prohibiting them from future violations of [the Securities Act], and prohibiting [the defendant corporations] from participating in any offerings of unregistered securities or otherwise violating [any] sections [ of the Securities Act], and (2) an order (a) freezing Defendant’s assets; (b) permitting the Commission to conduct expedited discovery; (c) prohibiting Defendants from destroying or altering documents; (d) requiring Defendant’s to return to the registry of the Court any assets they have moved from U.S.-based accounts outside of the United States; and (e) requiring Defendants to provide verified accountings of investor proceeds.<sup>50</sup>

The Commission also sought final judgment that would order the defendants to pay damages from their “ill-gotten gains and to pay prejudgment interest thereon,” pay civil financial

---

<sup>47</sup> Id.

<sup>48</sup> Id.

<sup>49</sup> Id.

<sup>50</sup> Id.

penalties, and enjoin the defendants from “participating in an offering of digital securities” pursuant to several sections of the Securities and Exchange Acts.<sup>51</sup>

Section 17(a) of the Securities Act prohibits the “use of interstate commerce for [the] purpose of fraud or deceit.” The applicable law to this case and the problem presented in this paper spans over subsections one, two, and three of Section 17(a):

(1) to employ any device, scheme, or artifice to defraud, or (2) to obtain money or property by means of any untrue statement of a material fact or any omission to state a material fact necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading; or (3) to engage in any transaction, practice, or course of business which operates or would operate as a fraud or deceit upon the purchaser.<sup>52</sup>

If the government has determined that “blockchain based tokens” are securities, and fraudulent activity like the ones displayed in the case above are subject to the Securities and Exchange Acts, then this would arguably be the clearest path forward to relief for victims.<sup>53</sup> While scammers and criminals may deviate in the way they conduct their deceit, the end result can arguably be seen as the same here. Victims are robbed of their hard-earned money through false statements and misplaced trust in the perpetrator.

Statutes and acts like the ones mentioned above would most easily be amended to include digital currency and virtual trading. Here, one can argue that, like the PlexCorps case, Section 17(a) includes the devices and techniques employed in the Pig Butchering Scam. A scammer employs some variation of a romance scam – or scheme – to defraud their victim out of

---

<sup>51</sup> *Id.*

<sup>52</sup> 15 U.S.C.A. § 77q.

<sup>53</sup> CFTC v. McDonnell, 287 F. Supp. 3d 213, 221 (E.D.N.Y. 2018).



personals funds, they then obtain the victim's money by "means of untrue statements of a material fact" such as claiming great returns or safe investments, and finally engages in a practice that deprives the victim of the money they invested to constitute fraud and deceit.

The remaining forms of regulation that the court offers in this case: "regulation by the Treasury Department's Financial Enforcement Network ("FinCEN"), regulation by the Internal Revenue Service ("IRS"), Regulation by private exchanges, state regulations, or a combination of any of the above," have more of the same advantages and disadvantages as the more obvious solutions discussed above.<sup>54</sup>

Regulation by the Treasury Department's FinCEN is a great way to regulate the actual legitimate exchanges that allow investors to transfer their virtual tokens from their site to any fraudulent ones, but it still does not offer any relief for the victims such as recovering the money they lost or seeing the perpetrator punished. When discussing this proposal, it is important to note one thing in particular that frustrate investigations into fraud and theft like the Pig Butchering Scam. Big legitimate exchanges like Bitcoin, Coinbase, Kraken, and Crypto.com can receive complaints about fraudulent sites that mimic their look, color, operation, and logo, but disclaim any responsibility to fight against the transfer of their consumer's money to these fake sites. When records of these transfers are subpoenaed by investigate agencies from legitimate exchanges, many admit to being aware of the problem – mostly because victims reported the theft to the exchange first. While criminal sanctions might be hard to obtain against these legitimate exchanges because of things like disclaimers, and terms of usage contracts that require investors to absolve the exchange before they can begin their trading, regulations dictating their operation and transfer policies might help protect investors from scammers and thieves.

---

<sup>54</sup> Id.

Unfortunately, a case addressing an issue like the one discussed above has yet to be adjudicated, but the Court in *McDonnell* cites a case from the Northern District of California where the U.S. Attorney's office "assessed a \$110,003,314 civil money penalty against BTC-e [a virtual currency exchange] for willfully violating U.S. anti-money laundering laws."<sup>55</sup> If multi-national exchange platforms like this one can be held accountable for violating or disregarding U.S. laws, then it should be possible to hold overseas individuals accountable for purposely "conducting business" with United States citizens and scamming them out of their hard-earned money.

Regulation by the Internal Revenue Service would deal mostly with "how the IRS applies U.S. tax principles to transactions involving virtual currency," but does little to address scams and thefts of money that a U.S. citizen would have paid taxes on had he or she not been taken advantage of. Therefore, regulation by this entity would regulate an entirely different side of the virtual currency market, and not apply to issue we hope to address here.

Regulation by private exchanges involves the encouragement for exchange platforms to "self-police" in order to "protect investors from taking on too much risk and other dangers."<sup>56</sup> There are a variety of potential ways to achieve the extra protection investors need in a market that has historically been unregulated and unchecked since its inception. Private exchanges could vet sign-ups and accounts on their website that seems repetitive or automatically generated. Accounts with mostly numbers or random letters and symbols in their username could be required to self-authenticate with a valid email that has been in existence for at least 6 months to a year. Investors could be required to request any account transfer and complete a two-factor authorization process before being allowed to do so. Computer code could be generated to detect

---

<sup>55</sup> *Id.*

<sup>56</sup> *Id.*

at-risk accounts and wallet addresses and be made to warn investors to double-check their recipient before moving forward. The same code could also detect at-risk domain names and websites for investors who want to make a transfer outside of the exchange. Taking it a final step further, transfers could have the same waiting period that some transfers at concrete banking institutions do. This could be achieved by simply placing a “pending” or “hold” tag on the account waiting to make the transfer, so that there is an extra amount of time to discover fraudulent activity and reverse the damage before any currency is actually moved from one account to the other. All of these suggestions taken together are relatively simple but could make a big difference in the grand scheme of things. Combating fraud and theft on a website specifically made for the purpose of handling and transferring money should be a top priority. From a purely business standpoint, an interest in protecting investors should be a legitimate exchange’s best marketing platform when its purpose is to facilitate trust between the user and the entity in an effort to stimulate investor’s continued use of the platform.

The court in *McDonnell* ends its list with a safety net: “a combination of any of the above.”<sup>57</sup> No explanation came with this suggestion, but one might argue that a combination of regulation by the CFTC, the SEC and the private exchanges could be the perfect recipe for at least some form of greater protection for virtual currency traders and investors. The CFTC has the power to extend its jurisdiction over virtual trading markets by declaring virtual currency a commodity subject to the regulations and practices of the Commission, as does the SEC by declaring virtual tokens a security subject to the provisions of the Security and Exchanges Acts. The statutes and acts mentioned above subject business dealings and trades within the virtual trading industry to penal criminal and civil proceedings, giving victims at the very least

---

<sup>57</sup> Id.

vindication through punishment for the ones who committed crimes against them. With the authority from statutes and acts like the Security and Exchange Acts and CFTC regulations, civil and administrative proceedings might be able to afford courts the opportunity to award damages to victims as well, like the *PlexCoin* case cited by the court under suggestion four, regulation by the SEC.<sup>58</sup> As noted above, self-regulation by private exchanges would help curtail the problem before it starts, providing greater protection and peace of mind to investors and reducing the risk of losing their money at all.

**B. Let's propose a change: Virtual trading scams should be included and applied to the *Howey* Test, so HOW would we apply it?**

The argument being made for the *Howey* Test stems from the argument to include virtual trading within the umbrella of regulation by the Securities and Exchange Commission. The issue presented by the court is immaterial to the problem here, because it was an action seeking to prevent the use of “mails and instrumentalities of interstate commerce” to promote the sale of securities. However, the test that was created here provides a solid rule-based argument for inclusion of our issue. The court in *Howey* gives some important background to preamble the test it formulated for determining whether an investment contract constitutes a security. While it recognizes that the term “investment contract” is historically undefined by the Securities Act many state courts have “broadly construed [the term] so as to afford the investing public a full measure of protection.”<sup>59</sup>

By including the term “within the scope of the Securities Act,” Congress would narrowly construe the meaning of the term and follow several court precedents that applied the definition

---

<sup>58</sup> Id. (see *S.E.C. v. PlexCorps*, 17-CV-7007, 2017 WL 5988934 (E.D.N.Y. Filed Dec. 1, 2017)).

<sup>59</sup> *S.E.C. v. W.J. Howey Co.*, 328 U.S. 293, 297 (1946).

to “a variety of situations where individuals were led to invest money in a common enterprise with the expectation that they would earn a profit solely through the efforts of the promoter or of someone other than themselves.”<sup>60</sup> Although this case was adjudicated in the late 1940’s, its principles can still be applied to the virtual trading industry today. The Court defined an investments contract, within the Securities Act, as a “contract, transaction or scheme whereby a person invests his money in a common enterprise and is led to expect profits solely from the efforts of the promoter or a third party . . . .”<sup>61</sup> If we can break this definition down into separate elements, one can argue that scams that run in similar operation and scheme to ones like the Pig Butchering scam fall under the definition.

The transfer of money between the unsuspecting victim to the scammer’s wallet address is a transaction to purchase additional bitcoin for what a victim thinks will be exchanged back into legal tender. A common enterprise is any number of the exchange platforms the victim and the scammers use to transfer money between the two. The promoter is the scammer, that leads the victim to believe he will obtain the “unbelievable returns” typical of the promises a scammer will advertise to the victim.

Now that the case has been made to include virtual trading scams within the definition of an investment contract for purposes of the Securities Act, one can argue that the *Howey* test applies for the purposes of an enforcement action. This follows logically because the court simply broke down the definition into four elements like we did above. If the argument can be made to include the virtual trading market within the scope of the Securities Act under the definition adjudicated here, the industry is now subject to the laws and regulations of the Securities and Exchange Commission, and jurisdiction over bad actors is more easily reached.

---

<sup>60</sup> Id. at 298.

<sup>61</sup> Id. at 298, 299.

### **C. Down to the wire: The Securities and Exchange Commission's Fraud by Wire statute could be the perfect hook.**

Section 1343 of the United States Code covers and defines “Fraud by Wire, Radio, or Television” and is more popularly known as the “Wire Fraud Statute.” It states in relevant part that:

Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication . . . any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined . . . .<sup>62</sup>

After establishing jurisdiction, enforcement actions within this statute against perpetrators of fraud against victims within the virtual trading industry could be argued for. Scams like the Pig Butchering scam could conceivably fall under this statute because of the way the scammers operate their scheme and how it would apply to the statute. A scammer “devised or intend[ed] to devise any scheme or artifice to defraud” in order to “obtain money . . . by means of false or fraudulent pretenses, representations, or promises.” The scammer devises a scheme in which they convince the victim to transfer money into fake accounts directly linked to their wallet addresses, in an effort to defraud them of their money and assets. The scammer uses writings, signs, signals, pictures, and sounds through the use of texts, faked social media accounts, and altered video chats in order to carry out their scheme and convince the victim to wire transfer money into one exchange or more, whether that exchange is legitimate or otherwise, for the ultimate purpose of theft.

---

<sup>62</sup> 18 U.S.C.A. § 1343 (2008).

The enforcement for this statute is a fine under Title 18 or a term of imprisonment for not more than 20 years. Fines are the path forward to obtain relief for the victims and punish and deter the scammer from engaging in similar future conduct. Obviously, imprisonment serves the same goal of deterrence and punishment, and would give the victim some feeling of vindication and peace of mind that the person who did this to him or her will have to face the consequences for what they did.

## **V. The Proposal: The Securities and Exchange and Commodity Futures Trading Commission, Private Exchange Regulation, *Howey* Test, Wire Fraud Mash-up.**

While new legislation might make enforcement and regulation much clearer, getting new laws passed is a cumbersome and arduous process that could get buried in years of debates and hearings. The virtual trading market is steadily growing larger by the day and the issues it is plagued with is a problem now.

Allowing attorneys to make the argument that virtual trading and currency should be included within the scope of existing legislation allows for, albeit a less clear path, but a shorter one to relief for victims and regulation of the industry. The different avenues discussed above offer a variety of solutions to a variety of problems, and the solution is not just confined to addressing the one issue explored here.

The argument ends by proposing that misdeeds like the Pig Butchering Scam and others be within the jurisdiction of the Securities and Exchange Commission, Commodity Futures Trading Commission, and the Wire Fraud Statute, giving the United States Government the jurisdiction they need to try cases like these and ones similar to cases like the *PlexCoin* case with international bad actors. Defining virtual tokens as a security and a commodity opens the door for additional regulation that the industry would now be subject to in order to conduct business in

the United States and give U.S. investors the peace of mind they deserve when letting go of the money they have earned. Encouraging legitimate exchange platforms to self-regulate addresses the problem at the root and might help prevent a portion of it from happening at all. Defining the trade of virtual currency as an investment contract would subject the individual practice to the applicability of the *Howey* test and give more strength to the argument that it belongs within the scope of Securities and Exchange Acts. Finally, arguing for the applicability of schemes like the Pig Butchering Scam fall within the conduct punishable by the United States Code's Wire Fraud statute allows enforcement actions against perpetrators of fraud within the industry and is one step toward closure and support to the victims.

**VI. Wrapping up: Relief for victims is never that far away, and current legislation provides us with the tools we'll need to protect and advocate.**

While this paper discussed several legal arguments and proposals for the regulation of cryptocurrency, it is worth concluding with the many heart-felt policy arguments thinly veiled throughout the discussion above. With every new and shiny profit-driven market that comes to fruition over the years, it always in the best interest of society to protect what America and its people passionately believe in – the American Dream. This industry is just another avenue and opportunity that people have the freedom to participate in, that might help them achieve what they're working toward. Whether it is hopeful parents fighting to send their child to college, an elderly grandmother hoping to have a little extra cushion in her retirement fund, or a family fighting to provide their children with experiences they never had, people need and deserve to have trust in the institutions they engage with. Like every other entity and industry that deigns to do business within our borders, the virtual trading market requires regulations that prioritize and protect our citizens' diversity of interests.



Victims of the Pig Butchering Scam and other scams of a similar nature deserve justice and relief for the harm they suffer, and the United States needs to send a strong message to overseas bad actors that it protects its citizens from harm with zealous advocacy. Allowing the Securities and Exchange Commission and the Commodity Futures Trading Commission to include scams and schemes like these within its scope and jurisdiction would send a message of unity against fraud and encourage deterrence of that conduct by domestic and foreign bad actors alike. Finally, arguing that the virtual trading market is applicable to the Wire Fraud Statute by classifying intentional misconduct within the virtual realm as punishable under its scope provides justice for victims that expect it as a citizen of the United States. These changes should be advocated for and implemented now rather than later, because the virtual trading market is one that will prove difficult to keep pace with as it continues to expand its reach.