EU CRYPTO CURRENCY REGULATION: CREATING A HAVEN FOR BUSINESSES OR FOR CRIMINALS?

Blake Hamil[*]

TABLE OF CONTENTS

[*] J.D. Candidate, University of Georgia School of Law, 2020, B.B.A. in Real Estate, University of Georgia, 2017.

I. INTRODUCTION

Crypto currencies, also known as virtual currencies, are revolutionary financial instruments that harness advanced and complicated technology to provide consumers and investors with an alternative value transfer system to fiat currencies. These virtual currencies have the power to significantly alter how the world pays for commodities and services, as well as how it invests in businesses. However, with this great power also comes increased risk, especially as it comes to the use of crypto currencies in money laundering schemes and criminal financing.[1] Across the globe, virtual currencies are used to fund criminal operations.[2] These risks have led countries like the United States to take a firmer stance on the regulation of virtual currencies, and it is because of these risks that the European Union needs to rethink its recent Anti-Money Laundering Directive.

This Note will discuss how the EU's current legal framework regulates virtual currencies. The discussion will focus on the EU's omission to regulate virtual currency administrators in contrast to the United States' treatment of virtual currency administrators under FinCEN and the Bank Secrecy Act. The discussion will begin with an overview of the background of virtual currencies and give an explanation of important terms and mechanisms within virtual currency use. Then, this Note will provide an overview of the United States' and the EU's current regulatory environment. Finally, this Note will analyze the risks inherent in the EU's current regulation and explain how revising its regulations will help mitigate these risks.

II. BACKGROUND

A. What Is a Virtual Currency?

The first virtual currency ever created was Bitcoin.[3] Satoshi Nakamoto is credited with Bitcoin's creation; however, Nakamoto's identity is unknown, and he has since disappeared from the public eye.[4] Nakamoto defined Bitcoin as a "decentralized peer-to-peer payment network that is powered by its users with no central authority or middlemen."[5] Simply put, virtual currencies like

---

[1] DANIEL HOLMAN & BARBARA STETTNER, ANTI-MONEY LAUNDERING REGULATION OF CRYPTOCURRENCY: U.S. AND GLOBAL APPROACHES (2019), https://www.allenovery.com/global/-/media/allenovery/2_documents/news_and_insights/publications/2019/5/anti-money_laundering_regulation_of_cryptocurrency.pdf?la=en-gb&hash=0EFC3BDA7C7604D7C841E074DC9C9AED.

[2] *Id.*

[3] *Frequently Asked Questions,* BITCOIN, https://bitcoin.org/en/faq (last visited Mar. 18, 2020).

[4] *Id.*

[5] *Id.*

Bitcoin are "limited entries in a database no one can change without fulfilling specific conditions."[6] To simplify even further, virtual currency can be described as "cash for the Internet."[7] This raises the question of what exactly differentiates virtual currency from your typical fiat currency. Fiat currency is "legal tender [that] is backed by a central government," and can "take the form of physical dollars, or it can be represented electronically."[8] Virtual currency, on the other hand, is not generally considered legal tender and is not "backed by a central government or bank."[9] Outside of these differences, however, fiat currency and virtual currency are not all that different. Both are mediums of exchange, both can be used to purchase goods and services or traded on exchange, and both are governed by economic factors like supply, demand, and scarcity.[10]

B. Blockchain Explained

The decentralized nature of virtual currency is what really makes it unique when compared to fiat currency.[11] This raises the question of how virtual currencies can be maintained without some sort of central middleman. The answer is virtual currency's utilization of "blockchain" technology.[12] Blockchain is essentially a public ledger that tracks every transaction in a virtual currency.[13] In the context of Bitcoin, blockchain is described as a "public ledger" containing "every transaction ever processed."[14] This ledger allows Bitcoin to maintain what the creators of Bitcoin call a decentralized platform to validate transactions.[15] Bitcoin utilizes what the company terms "miners" to validate transactions in lieu of a third party intermediary.[16] These miners are actually other Bitcoin users who have special software which allows their computers to validate these transactions, and in exchange, miners are

---

[6] Ameer Rosic, *What Is Cryptocurrency? [Everything You Need to Know!],* BLOCKGEEKS (Sept. 13, 2018), https://blockgeeks.com/guides/what-is-cryptocurrency/.

[7] BITCOIN, *supra* note 3.

[8] *The Difference Between Fiat Currency and Cryptocurrency,* CRYPTOCURRENCY FACTS (Oct. 31, 2019), https://cryptocurrencyfacts.com/the-difference-between-fiat-currency-and-cryptocurrency/.

[9] *Id.*

[10] *Id.*

[11] *Id.*

[12] BITCOIN, *supra* note 3.

[13] Arjun Kharpal, *Everything You Need to Know About Blockchain,* CNBC (June 29, 2018), https://www.cnbc.com/2018/06/18/blockchain-what-is-it-and-how-does-it-work.html.

[14] BITCOIN, *supra* note 3.

[15] *Id.*

[16] *Id.*

compensated with Bitcoin.[17] The validation process consists of miners ensuring that the users on each side of a transaction have the amount of Bitcoin they are transferring.[18]

C. Virtual Currency Business Entities

Today, there are thousands of virtual currencies, with Bitcoin commanding the largest market capitalization of all.[19] The proliferation of virtual currencies has led to the development of many businesses that deal with virtual currencies as a part of, or as their entire, business.[20]

There are several important entities that face potential regulation under anti-money laundering regulations. The first type of entity is the virtual currency "wallet." These wallets are a digital means to "store, send, and receive" virtual currencies.[21] Next are virtual currency exchanges, which exchange virtual currency for real currency, other funds, or other virtual currency.[22] Finally, we have virtual currency administrators, which are engaged in the business of "issuing . . . a virtual currency," and they have the "authority to redeem (to withdraw from circulation) the virtual currency."[23] Administrators will be important in the coming analysis of the EU's virtual currency regulation because entities involved in "initial coin offerings" (ICOs) qualify as administrators.[24]

D. Initial Coin Offerings

Briefly, an initial coin offering is a "fundraising mechanism in which new projects sell their underlying crypto tokens in exchange for Bitcoin . . . ."[25] This process is similar to initial public offerings in which companies sell shares of stock to investors, except for the fact that ICOs do not utilize an

---

[17] *Id.*

[18] *Id.*

[19] *All Cryptocurrencies,* COINMARKETCAP, https://coinmarketcap.com/all/views/all/ (last visited Mar. 18, 2020).

[20] HOLMAN & STETTNER, *supra* note 1, at 1.

[21] *What Is a Cryptocurrency Wallet?*, CRYPTOCURRENCY FACTS, https://cryptocurrencyfacts.com/what-is-a-cryptocurrency-wallet/ (last visited Oct. 25, 2019).

[22] *How Do MSBs and Virtual Currency Relate?,* CRYPTOCOMPLIANCE LLC, http://cryptocompliance.io/about-us/how-do-msbs-and-virtual-currency-relate/ (last visited Oct. 25, 2019) [hereinafter CRYPTO COMPLIANCE].

[23] *Id.*

[24] Sarah Hody, Jean-Jacques Cabou & Conor O'Hanlon, *FinCEN Is Watching ICOs for BSA Violations,* VIRTUAL CURRENCY REP. (Mar. 13, 2018), https://www.virtualcurrencyreport.com/2018/03/fincen-is-watching-icos-for-bsa-violations/.

[25] *What Is an ICO?*, NASDAQ (Aug. 10, 2017), https://www.nas daq.com/article/what-is-an-ico-cm830484.

underwriter to price the offering or locate buyers.[26] Most ICOs involve transactions in which investors send virtual currency to the fundraising entity's smart contract, and the smart contract then stores the investors' funds and distributes an equivalent value of the new token later.[27] Although this technology is relatively new, it has already been used to raise staggering amounts of money.[28] For example, the blockchain startup Block.one recently raised over $4 billion in an ICO that concluded in June 2018.[29] ICOs are also becoming increasingly popular, as the number of firms that completed ICOs jumped from forty-six in 2016 to 228 in 2017.[30] While there is much excitement surrounding this cutting-edge innovation in fundraising, ICOs are highly risky due to the infancy of most ICO entities and the unregulated nature of ICOs in most jurisdictions.[31] The proliferation of ICOs, the opportunity to raise such vast amounts of money, and the highly risky nature of these transactions amplifies the risks created by the complicated web of virtual currency administrators, exchangers, and wallet providers that dominate the virtual currency universe.[32] Countries across the globe have responded with a myriad of regulations varying in degrees of stringency.

E. The U.S.'s Stance on Virtual Currency

The United States has several regulatory bodies through which virtual currencies can be regulated. First, the Securities and Exchange Commission (SEC) has ruled that it can regulate virtual currencies and other similar tokens on the basis that they are considered securities.[33] Furthermore, the Commodity Futures and Trading Commission (CFTC) has defined virtual currencies as commodities and has determined it may regulate them as such.[34] Finally, the Financial Crimes Enforcement Network (FinCEN) has stated that it "regards

---

[26] *Id.*

[27] *Id.*; *see also Smart Contracts*, INVESTOPEDIA, https://www.investopedia.com/terms/s/smart-contracts.asp (last visited Oct. 8, 2019) (defining smart contracts as "self-executing contracts with the terms of the agreement between buyer and seller being directly written into lines of code").

[28] Alex Lielacher, *Top 10 Biggest ICOs (by Amount Raised)*, BITCOIN MKT. J. (Aug. 1, 2018), https://www.bitcoinmarketjournal.com/biggest-icos/.

[29] *Id.*

[30] Jia Wertz, *Are ICOs the New Startup Lifeblood?*, FORBES (Dec. 2, 2017), https://www.forbes.com/sites/jiawertz/2017/12/02/icos-new-startup-lifeblood/#38def61e525b.

[31] *Id.*

[32] *See generally Initial Coin Offerings (ICO's): Serious Risks*, DUTCH AUTH. FOR THE FIN. MKTS., https://www.afm.nl/en/professionals/onderwerpen/ico (last visited Oct. 31, 2019).

[33] Gina Conheady, *The EU Approach to ICO Regulation*, BLOOMBERG (Mar. 23, 2018) https://www.algoodbody.com/insights-publications/the-eu-approach-to-ico-regulation-a-friendlier-regulatory-framework-for-ico.

[34] *Id.*

developers as well as exchanges of [virtual currency] as 'money transmitters' for the purposes of the U.S. Bank Secrecy Act."[35] Because the European Union has adopted similar stances to the SEC and CFTC in regards to virtual currencies, the approach taken by the FinCEN will be the focus of this Note.

FinCEN's purpose is to "safeguard the financial system from illicit use, combat money laundering, and promote national security through the strategic use of financial authorities and the collection, analysis, and dissemination of financial intelligence."[36] It accomplishes this in two ways: (1) through counter-money laundering laws, such as the Bank Secrecy Act, that require reporting and recordkeeping by banks and other financial institutions, and (2) by providing intelligence and analytical support to law enforcement.[37] More specifically, FinCEN and the Bank Secrecy Act require money transmitters to do four things: (1) register with FinCEN, (2) have a risk-based know-your-customer and anti-money laundering program, (3) detect and report suspicious activity to FinCEN, and (4) maintain records relating to transmittals of funds in amounts of $2,000 or more.[38] FinCEN has stated that these regulations apply to money services businesses (MSBs).[39] In its 2018 letter, FinCEN declared that virtual currency exchanges and administrators are considered MSBs and are therefore subject to these requirements.[40] The application of these regulations to administrators of virtual currency is important because an administrator is engaged in issuing a virtual currency and has the authority to redeem the virtual currency.[41] In other words, these regulations apply not only to entities that exchange virtual currency for fiat currency, but also to entities partaking in initial coin offerings and entities that exchange virtual currency for virtual currency.[42] This distinction from the EU's approach to virtual currency regulation is important in preventing criminals from using virtual currencies for illicit purposes.

---

[35] *Id.*

[36] *Mission,* FIN. CRIMES ENF'T NETWORK, https://www.fincen.gov/about/mission (last visited Oct. 25, 2019).

[37] *Id.*

[38] PETER VAN VALKENBURGH, COIN CENTER REPORT, THE BANK SECRECY ACT, CRYPTOCURRENCIES, AND NEW TOKENS: WHAT IS KNOWN AND WHAT REMAINS AMBIGUOUS (2017), https://coincenter.org/files/2017-05/report-bsa-crypto-token1.pdf; *see also BSA Requirements for MSBs,* FIN. CRIMES ENF'T NETWORK, https://www.fincen.gov/bsa-requirements-msbs (last visited Oct. 25, 2019) [hereinafter *BSA Requirements*].

[39] *See BSA Requirements*, *supra* note 38.

[40] Letter from Drew Maloney, Assistant Sec'y for Legislative Affairs, U.S Dep't of the Treasury, to Senator Ron Wyden (Feb. 13, 2018), https://coincenter.org/files/2018-03/fincen-ico-letter-march-2018-coin-center.pdf.

[41] CRYPTO COMPLIANCE, *supra,* note 22.

[42] *Id.*

F. The EU's Current Stance on Virtual Currency

The regulation of virtual currencies has been a hot topic for debate in the European Union, and as a result, the European Central Bank (ECB) issued an official opinion regarding virtual currencies on October 12, 2016. [43] The ECB is an important institution with regard to EU financial regulation, as it is tasked with defining and implementing monetary policy, conducting foreign exchange operations, holding and managing the euro area's foreign currency reserves, and promoting the smooth operation of payment systems.[44] The ECB analyzed a proposal definition that defined virtual currency as "a digital representation of value that is neither issued by a central bank or a public authority, nor necessarily attached to a fiat currency, but is accepted by natural or legal persons as a means of payment and can be transferred, stored or traded electronically."[45] The ECB further elaborated, "'virtual currencies' do not qualify as currencies from a Union perspective" nor are they "legally established currencies or money." [46] Despite the EU's hesitance to define virtual currency as a legal currency and subject it to the corresponding regulations, it has responded to Member-States' cries for increased regulation.[47] In July 2018, the EU passed the Fifth Anti-Money Laundering Directive (AMLD5).[48] This new regulation adds virtual currency wallet providers and entities engaged in services that exchange virtual currencies for fiat currencies to the "obliged" entities under its Anti-Money Laundering Directive.[49] This Anti-Money Laundering Directive requires obliged entities to identify and verify the identity of clients, monitor transactions, and report suspicious activity.[50] This is very similar to the United States' approach; however, as referenced earlier, there is a significant distinction in the EU's approach.

---

[43] Opinion of the European Central Bank 2016 O.J (C 459) 3, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016AB0049&from=EN [hereinafter ECB Opinion].

[44] *Tasks*, EUR. CENT. BANK, https://www.ecb.europa.eu/ecb/tasks/html/index.en.html (last visited Oct. 31, 2019).

[45] ECB Opinion, *supra* note 43.

[46] *Id.*

[47] Carlos Terenzi, *Spainish Congress Calls for New Regulations to Promote Blockchain Technology*, COINSTAKER (July 18, 2018), https://www.coinstaker.com/spanish-congress-calls-for-new-regulations-to-promote-blockchain-technology/.

[48] Juergen Krais, *EU: 5th EU Anti-Money Laundering Directive Published*, GLOB. COMPLIANCE NEWS (July 16, 2018), https://globalcompliancenews.com/eu-5th-anti-money-laundering-directive-published-20180716/.

[49] Council Directive 2018/843, art. 8, 2018 O.J. (L 156/43) 3 (EC) [hereinafter EU Directive].

[50] *Anti-Money Laundering and Counter Terrorist Financing*, EUR. COMM'N, https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/anti-money-laudering-and-counter-terrorist-financing_en (last visited Oct. 25, 2019).

The EU's AMLD5 does not apply to virtual currency administrators.[51] This means that entities that issue virtual currencies and entities that exchange virtual currency for other virtual currency will not be regulated under AMLD5.[52] This omission will leave the EU at risk of criminal entities working to subvert the goals of the Anti-Money Laundering Directive.

G. Money Laundering Defined

The concept of money laundering is complex, so a background understanding of this process is necessary to fully comprehend the important and difficult task of regulating it. FinCEN defines money laundering as "the process of making illegally-gained proceeds . . . appear legal."[53] This is a three-step process: (1) placement, (2) layering, and (3) integration.[54] During the placement phase, a money launderer will secretively introduce the illicit funds into a legitimate financial system.[55] Then the launderer creates confusion by layering transactions, which means moving the money around by transferring and wiring through different accounts.[56] Finally, the money launderer integrates the illicit funds into the financial system through additional transactions, until the money appears to be clean.[57] Money laundering can be used to "facilitate crimes such as drug trafficking and terrorism, and can adversely impact the global economy."[58]

III. ANALYSIS

A. General Risk Factors of Virtual Currency

There are several elevated anti-money laundering and criminal financing risks associated with virtual currencies. These risks include trafficking in illicit goods, hacking and identity theft, market manipulation and fraud, and the more general risks of money laundering and terrorist and criminal financing.[59] Regulators must consider these risks in detail and implement sophisticated regulatory systems to manage them.

---

[51] *Id.*

[52] Conheady, *supra* note 33.

[53] *History of Anti-Money Laundering Laws*, FIN. CRIMES ENF'T NETWORK, https://www.fincen.gov/history-anti-money-laundering-laws (last visited Oct. 7, 2019).

[54] *Id.*

[55] *Id.*

[56] *Id.*

[57] *Id.*

[58] *Id.*

[59] HOLMAN & STETTNER, *supra* note 1, at 31.

B. Illegal Trafficking

Virtual currencies are an ideal means for criminals to traffic illegal goods and services.[60] The anonymous and digital nature of virtual currency transactions has "facilitated the growth of 'darknet' online marketplaces in which illegal goods and services are traded."[61] This means that the purchase of goods and services like drugs, human trafficking, child pornography, and even organs are facilitated through the use of virtual currency.[62] An unsettlingly large portion of virtual currency users is associated with illegal activity.[63] For instance, researchers in 2017 found that approximately one-quarter of all Bitcoin users and forty-four percent of Bitcoin transactions are associated with illegal activity.[64] The risks created by virtual currencies in this context are best exemplified by the "Silk Road" marketplace.[65] The Silk Road marketplace was a website founded by Ross Ulbricht that operated similarly to Ebay. Buyers exchange Bitcoin for illegal drugs, weapons, and other products by making offers on listings advertised by sellers.[66] This marketplace became extremely popular due to its reliability, but this popularity ultimately led to its downfall as it placed itself in the crosshairs of an FBI investigation.[67] Although the Silk Road marketplace is no longer operational, it still illustrates a foreboding example of the power of virtual currencies in the wrong hands. It is estimated that over $1billion changed hands through the Silk Road, all of which was made possible by the anonymity of Bitcoin.[68]

C. Hacking and Theft

Virtual currencies also create a high-risk target for hacking and theft.[69] Virtual currency wallets and exchangers provide hackers with attractive targets for fraud and identity theft.[70] If hacked, virtual currency wallets and accounts can be easily emptied to an anonymous account and then liquidated

---

[60] *Id.*

[61] Sean Foley, Jonathan R. Karlsen & Talis J. Putnins, *Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed Through Cryptocurrencies?*, OXFORD BUS. L. BLOG (Feb. 19, 2018), https://www.law.ox.ac.uk/business-law-blog/blog/2018/02/sex-drugs-and-bitcoin-how-much-illegal-activity-financed-through.

[62] HOLMAN & STETTNER, *supra* note 1, at 31.

[63] Foley et al., *supra* note 61.

[64] *Id.*

[65] HOLMAN & STETTNER, *supra* note 1, at 31.

[66] Andrew Norry, *The History of Silk Road: A Tale of Drugs, Extortion & Bitcoin*, BLOCKONOMI (Nov. 20, 2018), https://blockonomi.com/history-of-silk-road/.

[67] *Id.*

[68] *Id.*

[69] HOLMAN & STETTNER, *supra* note 1, at 32.

[70] *Id.*

with little hope of reversing the transaction after the hack is discovered.[71] Quantifying these risks, Ernst & Young found in a 2017 study that more than ten percent of initial coin offering proceeds are lost as a result of attacks.[72] In this research, Ernst & Young noted that both projects and investors are exposed to attacks, and that the frequency of such attacks is only expected to grow, due to the simplicity and effectiveness of these hacking efforts.[73] The Mt. Gox hack is a perfect example of what is at stake here. Mt. Gox was launched in 2010 by Jed McCaleb, and it quickly became the most popular Bitcoin exchange in the world.[74] In 2014, Mt. Gox stopped all Bitcoin withdrawals, and it was later discovered that hackers had stolen 744,408 Bitcoins belonging to customers and 100,000 belonging to the company.[75] Although the hack is still under investigation, it is presumed that most of the bitcoins were stolen from Mt. Gox's online wallets.[76] A security breach of this magnitude shows why virtual currency creates a target for hackers, and it shows the potential risks associated with underregulation of associated virtual currency entities.

D. Fraud

Virtual currencies also create a market vulnerable to manipulation and fraud.[77] Unregistered initial coin offerings and unlicensed virtual currency exchangers make it difficult to detect and deter insider trading, as well as market abuse such as front-running, pump-and-dump schemes, and more.[78]

---

[71] *Id.*

[72] EY, EY RESEARCH: INITIAL COIN OFFERINGS (ICOS) (2017), https://www.ey.com/Publication/vwLUAssets/ey-research-initial-coin-offeringsicos/$File/ey-research-initial-coin-offerings-icos.pdf.

[73] *Id.*

[74] Andrew Norry, *The History of the Mt Gox Hack: Bitcoin's Biggest Heist*, BLOCKONOMI (June 7, 2019), https://blockonomi.com/mt-gox-hack/ [hereinafter *Mt. Gox Hack*].

[75] *Id.*

[76] *Id.*

[77] HOLMAN & STETTNER, *supra* note 1, at 32.

[78] *Id.*; *see also Front-Running,* INVESTOPEDIA, https://www.investopedia.com/terms/f/frontrunning.asp (last visited Oct. 25, 2019) (defining front-running as a scheme in which a broker or other entity enters into a trade in which they have advanced knowledge of a non-publicized transaction that will influence the price of the asset); *Market Manipulation ("Pump and Dump") Fraud*, FED. BUREAU OF INVESTIGATION, https://www.fbi.gov/scams-and-safety/common-fraud-schemes/market-manipulation-pump-and-dump-fraud (last visited Oct. 25, 2019) (defining pump-and-dump schemes as a scheme in which a person or entity creates artificial pressure for a targeted security increasing the trade volume and ultimately allowing the fraud perpetrator to sell the security at an artificially inflated price).

Exemplifying the risk of market abuse is the rise of Bitcoin prices in 2017.[79] In a recent study, experts found that the meteoric rise of Bitcoin prices in 2017 can be attributed in part to price manipulation, using another virtual currency called Tether.[80] The researchers found that Tether was used to support the price of Bitcoin by noting the increases in the purchase of Bitcoin following large price falls.[81] This sort of complicated market manipulation scheme is a major risk inherent in virtual currencies due to investor interest and lack of understanding in these emerging currencies as well as a lack of transparency on the part of currency issuers.[82]

E. Money Laundering

Virtual currencies are attractive to money launderers for a multitude of reasons.[83] Certain characteristics inherent in virtual currencies make them prime targets for money laundering.[84] The characteristics that make virtual currency attractive to money launderers are the anonymity provided by the trade in virtual currencies on the internet, the limited identification and verification of participants, the lack of clarity regarding the responsibility for regulatory compliance and enforcement in cross-border transactions, and the lack of a central oversight body.[85] The trading of virtual currencies on the Internet is characterized by non face-to-face transactions, as well as anonymous funding and transfers.[86] In addition, the ability to rapidly and anonymously open accounts provides a low-risk means for potential money launderers to convert and consolidate cash.[87] These factors are attractive for an entity looking for a discreet way to launder money, and virtual currencies provide a means of doing so that is anonymous and difficult to trace.[88] In addition, virtual currency transactions take place entirely on the Internet; therefore, it would be simple to launder money through international cross-border systems.[89] Due to the varying regulations on virtual currencies worldwide and the complicated technology backing these currencies, regulators may be hesitant to bring

---

[79] John M. Griffin & Amin Shams, *Is Bitcoin Really Un-Tethered?*, SSRN (Nov. 5, 2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3195066.

[80] *Id.* at 33.

[81] *Id.* at 20.

[82] *Id.* at 2.

[83] HOLMAN & STETTNER, *supra* note 1, at 32.

[84] *Virtual Currencies: Key Definitions and Potential AML/CFT Risks*, FIN. ACTION TASK FORCE 1, 9 (2016), http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf [hereinafter FATF].

[85] *Id.*

[86] *Id.*

[87] HOLMAN & STETTNER, *supra* note 1, at 32.

[88] *Id.* at 26.

[89] FATF, *supra* note 84, at 9.

enforcement action against cross-border entities and transactions.[90] Finally, the decentralized nature of virtual currencies means there is no central oversight body to ensure that the currency is being used for legal purposes.[91] Initial coin offerings also provide the opportunity for criminal actors to launder money by using fraudulent means [92] to convert their virtual currency proceeds back into fiat currency. The danger of money laundering inherent in virtual currencies is very real, and is an area that regulators must address.

F. Criminal Financing

Finally, terrorist or other criminal networks utilize virtual currency to garner funding and transfer funds.[93] The same anonymity and ease of account creation that increases the risk of money laundering also allows terrorist groups to receive payment that otherwise might trigger red flags or sanctions.[94] In addition to these characteristics, the ease with which an entity can make cross-border payments with virtual currencies also appeals to terrorist organizations. [95] There is evidence that terrorist groups have already begun to take advantage of this technology.[96] For instance, terrorist groups in the Gaza Strip, Iraq, and Syria have begun implementing virtual currency technology, with recorded uses in Indonesia and the United States.[97] The potential for more widespread use by terrorist groups exists due to the increasing technological evolution of virtual currencies, as well as terrorist groups improving their infrastructure to support this technology.[98] This is a matter of global concern and requires proper regulation across the world to prevent terrorist groups from utilizing this technology to wreak havoc on our cities and countries.

In sum, virtual currency is a powerful technological tool that creates an elevated risk for certain criminal elements. These risks include trafficking illicit goods, hacking and identity theft, market manipulation and fraud, money laundering, and terrorist and criminal financing.[99] The United States and the European Union have both implemented regulation to help combat these risks,

---

[90] *Id.* at 9–10.

[91] *Id.* at 9.

[92] HOLMAN & STETTNER, *supra* note 1, at 32.

[93] *Id.*

[94] *Id.*

[95] Iwa Salami, *Terrorism Financing with Virtual Currencies: Can Regulatory Technology Solutions Combat This?*, TAYLOR & FRANCIS ONLINE (Sept. 15, 2017), https://www.tandfonline.com/doi/abs/10.1080/1057610X.2017.1365464?journalCode=uter20.

[96] Zachary Goldman et al., *Terrorist Use of Virtual Currencies: Containing the Potential Threat*, CENT. FOR A NEW AMERICAN SOC'Y (May 3, 2017), https://www.cnas.org/publications/reports/terrorist-use-of-virtual-currencies.

[97] *Id.*

[98] *Id.*

[99] HOLMAN & STETTNER, *supra* note 1, at 31–32.

and although the regulations implemented by the U.S. are not perfect, they better manage these risks than the regulations implemented by the EU.

IV. HOW THE U.S.'S REGULATORY APPROACH BETTER MITIGATES VIRTUAL CURRENCY RISKS COMPARED TO THE EU APPROACH

As noted earlier, in the United States, the Financial Crimes Enforcement Network is responsible for safeguarding the U.S. financial system from illicit use and combatting money laundering.[100] In terms of virtual currencies, FinCEN requires administrators and exchangers of virtual currency to: (1) register with FinCEN, (2) have a risk-based know-your-customer and anti-money laundering program, (3) detect and report suspicious activity to FinCEN, and (4) maintain records relating to transmittals of funds in amounts of $2,000 or more.[101] Due to FinCEN's inclusion of virtual currency administrators in this regulatory framework, it is in a better position to protect the U.S. financial system from the risks created by virtual currencies.

The primary difference between the U.S.'s regulatory scheme and the EU's is the fact that the U.S. regulates virtual currency administrators, as well as exchanges and wallets, whereas the EU's regulatory approach only reaches virtual currency exchangers and wallets.[102] The U.S. also regulates exchanges which exchange virtual currency for other virtual currency, unlike the EU, which only regulates exchanges which exchange virtual currency for fiat currency.[103] The importance of these distinctions is highlighted by the EU's underregulation in one important aspect of the virtual currency universe: the initial coin offering.[104]

The EU's failure to include virtual currency administrators in their anti-money laundering directive is important because many entities utilizing an ICO will not be regulated under AMLD5.[105] As explained earlier, an ICO typically involves an entity developing a new virtual currency and then selling tokens or coins to investors in exchange for another virtual currency, such as Bitcoin.[106] This means that these firms do not fall under the EU's AMLD5 because AMLD5 is limited to virtual currency exchangers who exchange virtual currency for fiat currency and virtual currency wallets.[107] In the U.S., on the other hand, a firm who uses an ICO will be seen as an administrator of

---

[100] *What We Do*, FIN. CRIMES ENF'T NETWORK, https://www.fincen.gov/what-we-do (last visited Oct. 25, 2019).

[101] *BSA Requirements*, *supra* note 38.

[102] HOLMAN & STETTNER, *supra* note 1.

[103] EU Directive, *supra* note 49; CRYPTO COMPLIANCE, *supra* note 22.

[104] Conheady, *supra* note 33.

[105] *Id.*

[106] Arjun Kharpal, *Tokenization: The World of ICOs*, CNBC (Apr. 12, 2019), https://www.cnbc.com/2018/07/13/initial-coin-offering-ico-what-are-they-how-do-they-work.html.

[107] EU Directive, *supra* note 49.

virtual currency because the firm is "issuing a virtual currency" and retains "the right to redeem [the currency]."[108] Therefore, entities utilizing ICOs would be regulated under the U.S.'s Bank Secrecy Act, while most of these entities would avoid regulation under AMLD5 in the EU.[109]

ICOs amplify the risks associated with virtual currencies in general.[110] Specifically, ICOs generally present heightened risks for fraud and theft, criminal financing,[111] and money laundering.[112] Regulation in the ICO and virtual currency administrator context is imperative to protect consumers, investors, and financial markets from these risks.[113]

The risk of fraud and theft is increased in the ICO context, and there are specific examples of the vulnerability of ICOs to hacking and theft.[114] Two examples of ICOs' unique vulnerability in this context are the Veritaseum and Coindash hacks.[115] Veritaseum is the issuer of a virtual currency called VERI, and in July 2017, its ICO was compromised, and a hacker stole over $8 million worth of VERI tokens.[116] The hacker purportedly exchanged all the VERI tokens for another virtual currency called Ether.[117] The ease with which this criminal was able to steal a substantial amount of virtual currency and then immediately "clean" it by exchanging it for a different virtual currency exemplifies the risks inherent in ICOs and virtual currencies, as well as the necessity of regulating entities participating in ICOs and virtual currency exchangers.

The Coindash hack is a similar fact pattern to the Veritaseum hack. Coindash was fundraising for a start-up venture through an ICO when a hacker was able to divert over $7 million worth of the virtual currency Ether to the hacker's own account.[118] Under the EU's AMLD5, ICO issuers such as

---

[108] Letter from Drew Maloney*, supra* note 40.

[109] *Id.*

[110] Obiamaka Madubuko & Margaret Ukwu, *Fintech in Focus: Anti-Money Laundering Regulatory Developments for Virtual Currencies and Initial Coin Offerings*, PAYMENT SYS. AND ELEC. FUNDS TRANSFERS GUIDE, https://www.westlaw.com/Document/I03c1d9e2343f11e8936db90bc1101f5d/View/FullText.html?transitionType=Default&contextData=(sc.Default)&VR=3.0&RS=cblt1.0 (last updated Sept. 13, 2018).

[111] *Id.*

[112] Saheli Choudhury, *It's a Very Good Time to Be A Money Launderer, and You Can Thank Cyrptocurrencies*, CNBC (Aug. 5, 2017), https://www.cnbc.com/2017/08/04/icos-may-be-seen-as-securities-by-u-s-and-singapore-regulators.html.

[113] *Id.*

[114] Madubuko & Ukwu, *supra* note 110.

[115] *Id.*

[116] Jeremy Nation, *Veritaseum Hacked,* ETH NEWS (July 24, 2017), https://www.ethnews.com/veritaseum-hacked.

[117] Wolfie Zhao, *Veritaseum Founder Claims $8 Million in ICO Tokens Stolen*, COINDESK (July 26, 2017), https://www.coindesk.com/veritaseum-founder-claims-8-million-ico-token-stolen/.

[118] Wolfie Zhao, *$7 Million Lost in CoinDash ICO Hack*, COINDESK (July 20, 2017), http

Vertiaseum and Coindash will not be subject to AMLD5 regulations, which could have helped prevent these sorts of hacks from occurring.[119] While it is a difficult task to eliminate these sorts of risks entirely, the U.S. has shown that applying the BSA can help to prevent these sorts of breaches from occurring.[120]

The way in which the U.S. prevents criminals from taking advantage of virtual currencies is exemplified by the enforcement action against Ripple Labs.[121] In 2015, FinCEN brought its first enforcement action against a virtual currency entity, Ripple Labs, Inc.[122] The consequences of the action were severe, as Ripple Labs was issued a fine of $700 million for selling its virtual currency without registering with FinCEN or implementing an anti-money laundering program.[123] This action was brought despite there being no allegation of fraud or theft.[124] This shows that the U.S. has an advantage by regulating ICOs and other virtual currency companies under the BSA because it allows the U.S. to prevent fraud, theft, and other crimes before they happen.[125] The EU, on the other hand, will be forced to wait until these crimes occur. The best way to mitigate the potential harms associated with virtual currencies may be to ensure that these entities are complying with regulations before the harm occurs.

In addition to the concerns regarding fraud and theft, the influx of new ICOs in the market also creates a heightened risk for money laundering.[126] ICOs present two possible vehicles for money launders.[127] First, the launderers may exchange dirty money for ICO investors' tokens, thereby "cleaning" it.[128] Second, money launderers could invest their dirty funds (directly or through another virtual currency) into an ICO that does not have "robust know-your-customer practices."[129] The first method of money laundering is actually protected by the AMLD5 regulations because this sort of exchange would occur on a fiat currency to virtual currency exchange.[130] However, the second method could be unregulated under the AMLD5 because it can take the form of a virtual currency for virtual currency exchange.[131] In contrast, the

---

s://www.coindesk.com/7-million-ico-hack-results-coindash-refund-offer/.

119 Letter from Drew Maloney, *supra* note 40.

120 Madubuko & Ukwu, *supra* note 110.

121 *Id.*

122 *Id.*

123 *Id.*

124 *Id.*

125 *Id.*

126 Choudhury, *supra* note 112.

127 *Id.*

128 *Id.*

129 *Id.*

130 EU Directive, *supra* note 49, at 8–9.

131 *Id.*

BSA would require all U.S. ICOs to maintain know-your-customer practices, as well as registration with FinCEN.[132] Therefore, the U.S. regulations will work to prevent both of the primary vehicles of money laundering through ICOs, whereas the EU will leave one vehicle under-regulated.

V. CONCLUSION

Virtual currencies are complex and constantly evolving, and a myriad of business entities have started dealing in them over the past several years.[133] With this complexity comes the risk that bad actors will exploit these virtual currencies in attempt to subvert the traditional regulations placed on money laundering and criminal financing.[134] These risks are particularly pervasive in the budding ICO market.[135] The U.S. has responded to these risks by applying its Bank Secrecy Act to virtual currency administrators.[136] While the EU has improved its regulatory protection with the advent of the AMLD5 regulations, it needs to go a step further and make its anti-money laundering regulations applicable to virtual currency administrators. This expansion will give the EU the authority it requires to prevent the exploitation of virtual currencies and ICOs. The risks presented by criminal exploitation of virtual currency are real, and the EU should address these risks by taking a firmer stance in its anti-money laundering regulations.

---

[132] Letter from Drew Maloney, *supra* note 40.
[133] HOLMAN & STETTNER, *supra* note 1, at 8.
[134] *Id.*
[135] Madubuko & Ukwu, *supra* note 110.
[136] Letter from Drew Maloney, *supra* note 40.