BITCOIN REGULATIONS AND INVESTIGATIONS:
A PROPOSAL FOR U.S. POLICIES

by

Jay Palmer Fawcett, CFE, CAMS

A Capstone Project Submitted to the Faculty of

Utica College

December 2016

in Partial Fulfillment of the Requirements for the Degree of

Master of Science in Economic Crime Management
Abstract

Bitcoins were conceptualized in 2008, which revolutionized the digital transfers of value within payment systems (Nakamoto, 2008). The advent of digital currencies revealed problems concerning anonymity embedded in bitcoins, consequently raising money laundering concerns. Regulators and law enforcement agencies struggle with addressing the money laundering issues inherent with bitcoin and digital currencies (Ajello, 2025). In response to these threats, agencies have issued various opinions regarding defining digital currencies within a financial framework. Regulator opinions concerning the applicability of bitcoins existing as currency, property, a commodity and commodity money contradict each other. Moreover, prosecutorial agencies attempt to fit digital currency exchangers under the regulations pertinent to money service businesses (MSB) (Mandjee, 2015; Sonderegger, 2015). This project provided an analysis of scholarly material, government publications, case law, and current trade information to examine a solution to the problem of money laundering through digital currency. This project revealed a need for a clear definition of bitcoin and digital currency within the context of U.S. laws and regulation to assist with investigations concerning illicit uses of digital currency. Furthermore, a need exists for new U.S. legislation specific to digital currency, which addresses money laundering and terrorist finance risks. Research revealed that digital currency regulations should mirror MSB regulations to curb peer-to-peer digital currency exchanges (Kirby, 2014). Additionally, FinCENs purview with financial crimes provides a unique position to assist law enforcement with digital currency investigations (FinCEN, 2014). A need exists for FinCEN to develop a blockchain analysis tool for law enforcement agencies and to assist with complex digital currency investigations (DHS, 2014). Keywords: Economic Crime Management, Financial Crime and Compliance Management, Paul Pantiani, virtual currency, cryptocurrency.
Acknowledgements

This capstone project would not have been possible without my extended support network, which assisted me through my entire Master’s degree pursuit. At the top of my list of people to acknowledge is my best friend, soulmate, and wife Charlotte. Without her unending support of this endeavor, I never would have made it through this journey. I must also acknowledge my parents, Pam and Chuck Goy for their constant accolades and support throughout my life and encouraging the vision to pursue my dreams in life.

The friendships that I have made in this program are unparalleled, especially those in the Cohort 36 “study group”. We have worked together cohesively during this program and had some fun along the way.

Joshua Lee, my friend, co-worker, and second reader, was an incredible help during the capstone process and during the entire program. I sincerely appreciate the feedback that Josh gave me on this project and enduring all of my questions and propositions about bitcoins! I must also acknowledge my capstone professor, Paul Pantani, for encouraging me to complete this capstone during the first eight weeks of the capstone course. Paul’s hard work of reviewing my submittals and giving timely feedback made this possible. I also want to thank the many professors that helped to refine my writing skills and impart their knowledge during this program.

Finally, my editor, Karen Pamer was a lifesaver during my project. Karen spent countless late nights editing my numerous capstone revisions and helping to develop my vision for this project, along with being a motivator, visionary, and tireless reader.
# Table of Contents

Bitcoin Regulations and Investigations: A Proposal for U.S. Policies ............................................. 1
  Purpose of the Study .................................................................................................................. 2
  Current Regulatory Environment .......................................................................................... 4
  Case Example ........................................................................................................................ 6
  U.S. Efforts to Control Money Laundering ......................................................................... 7
  Money Laundering Threats .................................................................................................. 9
  Literature Review .................................................................................................................. 11
    The Bitcoin Network and Bitcoins .................................................................................. 11
    Bitcoin Money Laundering Threats ............................................................................... 13
    Regulating P2P Transactions to Reduce Money Laundering Threats ........................... 20
    The Unclear Definition of Bitcoin ................................................................................... 29
    FinCEN Assistance with Bitcoin Law Enforcement Investigations ............................. 32
  Discussion of the Findings .................................................................................................... 35
    Bitcoin Threats .................................................................................................................. 36
    Regulatory Framework ....................................................................................................... 40
    Clarified Definition ............................................................................................................. 41
    Methods to Enhance Law Enforcement Investigations ................................................... 42
    Limitations of the Study ..................................................................................................... 43
    Summary ............................................................................................................................... 44
  Recommendations and Conclusion ....................................................................................... 45
    New Entity Definition ......................................................................................................... 46
    New Legislation .................................................................................................................... 48
    Reporting Requirements .................................................................................................... 49
    Definition of Digital Currency ........................................................................................... 50
    FinCEN Actions ................................................................................................................... 51
    Future Research .................................................................................................................. 51
    Conclusion ............................................................................................................................ 52
  References .............................................................................................................................. 53
  Appendix A – Acronyms ......................................................................................................... 63
  Appendix B – Bitcoin transactions ...................................................................................... 64
  Appendix C – Bitcoin transactions explained .................................................................... 66
Bitcoin Regulations and Investigations: A Proposal for U.S. Policies

The utilization of money laundering to obfuscate the origin of illicit proceeds is an insurmountable problem that is the basis for numerous law enforcement investigations in the United States. Constant development of new methods, used and exploited by criminals to hide proceeds from illegal activities, thwart efforts by investigators to identify and seize illicit assets. The continuous advent of new technology introduces new methods for criminals to mask illicit proceeds and present new challenges for investigators, regulators, and legislators (Ajello, 2015).

Advances in technology frequently outpace legislation and regulations leaving lawmakers and investigators coping with ways to address technological advancements that enable criminal activity. Crypto-currency, a form of digital currency, was introduced to the economy in approximately 2008 with the introduction of bitcoin. Today, more than 700 digital currencies exist on the open market (“Crypto-Currency,” 2016).

In 2008, a conceptual paper was released by a computer programmer, under the pseudonym Satoshi Nakamoto titled Bitcoin: A peer-to-peer electronic cash system. The concept was quite elaborate: introduce an anonymous global payment system based on a decentralized digital currency system where the network of users replaces the need for a centralized government issued fiat currency. In the paper, Nakamoto described the transaction process within the Bitcoin network and named the virtual coins bitcoins. The delineator for the two concepts is the network name begins with a capital (Bitcoin) and the digital coin does not have a capital (bitcoin) (Nakamoto, 2008).

Per the website blockchain.info, the Bitcoin network increased to more than 15.8 million bitcoins in circulation between 2009 through 2016 (“Bitcoins in,” 2016). The approximate aggregate stored value of bitcoin is $9.7 billion U.S. dollars (USD). During the 12-month period
preceding September 2016, approximately 310,000 bitcoin transactions were leveraged per day with an average daily value of $143 million USD (See Appendix B). Within the total of 310,000 daily transactions lies the number of bitcoins moved within the transactions, which averaged approximately 3,000,000 bitcoins daily during the prior 12 months (“Output value,” 2016). The value of one bitcoin fluctuated at approximately $600 USD in September 2016; however, the value frequently varies (“Bitcoin market,” 2016).

An important distinction lies in the difference between the common references to digital currency and virtual currency. Convertible digital currency is a medium treated as currency, which is stored and transferred electronically and easily converted to fiat currencies, such as U.S. dollars. Virtual currency may not directly translate to a currency value; often used as rewards in video gaming networks (Wagner, 2014). As digital currency continues to evolve, many sources use different names for bitcoin, including but not limited to the following: digital currency, virtual currency, cryptocurrency, convertible digital currency, and convertible virtual currency (Mandjee, 2015). In this case study, bitcoin and other convertible digital currencies that have similar architecture to bitcoin will be referred to as digital currency.

**Purpose of the Study**

The purpose of this research was to identify current shortcomings in U.S. policy, regulator guidance, regulations, and statutes that address money laundering as a crime and to determine how bitcoin can further be defined in these mediums. This could assist with successful prosecutions for the illegal use of bitcoins and other digital currencies. The study analyzed current U.S. policies; successful digital currency prosecution techniques; and proposals for further policy, legislation, and guidance for digital currencies. The focus of the research was bitcoin; however, most of the principles addressed transcend to other digital cryptocurrencies.
The study attempted to answer the following questions:

- What are the current money laundering threats presented by bitcoin use?
- How can U.S. peer-to-peer bitcoin transactions be regulated to remove the anonymity component of an informal money service business (MSB)?
- How has failing to clearly define bitcoin as a currency, commodity, property, or value transfer system impacted the enforcement of the illegal utilization of bitcoin?
- How could the Financial Crimes Enforcement Network (FinCEN) assist law enforcement with bitcoin investigations?

This study utilized an expansive spectrum of materials to leverage a comprehensive review of current sources on the rapidly evolving topic of digital currency. The sources included books, scholarly journals, consultations with law enforcement and prosecutorial subject matter experts, FinCEN guidance, government policy review, and recent web-based publications and transaction data. An extensive array of research data was utilized to encompass arguments for and against changes concerning regulations or policies involving digital currency and the possible impacts of digital currency in the realm of money laundering.

The findings of this study intended to assist lawmakers, regulators, prosecutors, and investigators with the threats involving digital currencies. The study focused on educating targeted readers with the deficiencies in current policies, regulations, and legislation as well as making recommendations for future updates in the regulation of digital currencies. Additionally, the study attempted to identify improvements to investigative procedures in investigations involving digital currency.
Current Regulatory Environment

When U.S. legislators drafted anti-money laundering statutes and regulations, digital currencies did not exist. The original intent of these laws and regulations was to mitigate the infusion of illicit currency into the economy and to prosecute criminals attempting to launder criminal proceeds. Presently, prosecutors and investigators attempt to adapt current laws, regulations, and policies to the medium of digital currency. The current laws and regulations are not designed for the challenges presented by digital currencies.

The U.S. has not reached a consensus across various regulatory and enforcement agencies regarding the definition of digital currencies and how they factor into the financial sector. The Financial Crimes Enforcement Network ([FinCEN], 2013) classified digital/virtual currencies under the regulations of a money service business (MSB), yet failed to define it as an actual currency. FinCEN stated that digital currencies are merely a medium of exchange. The Internal Revenue Service ([IRS], 2014) stated digital/virtual currency is a medium to store value and classified digital currency as property for taxation purposes. The U.S. Commodity Futures Trading Commission (CFTC) determined digital currencies are a commodity (Kalbaugh, 2016). The three aforementioned definitions of the interpretive guidance regarding digital currencies legal status are problematic for the enforcement of current money laundering regulations (Mandjee, 2015).

The inherent design of cryptocurrency and most digital currencies conceal the currency owner and anonymize transactions by eliminating a centralized currency issuer. Digital currency exchangers do not record transactions in the same manner as traditional banking institutions unless they register as a U.S. based digital currency exchanger. Digital currency exchangers are
similar in design to a foreign currency exchanger, yet they transact with the exchange of fiat exchange and digital currency (Franco, 2015).

Per Franco (2015), the Bitcoin blockchain maintains transaction history after completion of transactions. The blockchain is a public ledger that holds transactional records and balances of all bitcoin wallets on the network. The transaction history is connected to the identity of a digital wallet that the currency came from or went to and it does not identify the owner of the wallet or the bitcoins. In addition, the creation of new digital wallets further anonymizes the transactions through transfers between wallets. The digital currency wallet does not store user information, such as personally identifiable information (PII) about the owner of the wallet.

Bitcoin transfers between individuals present numerous problems for investigators to trace the origin of funds used to purchase digital currency. Once fiat currency is utilized to purchase digital currency, it is easily transferable overseas or to other users to further launder funds. The FinCEN (2013) guidance defines transactors who exchange currency for bitcoins as an MSB. This designation requires the transactors to register as an MSB, follow all Bank Secrecy Act (BSA) guidelines including collecting PII on customers, and filing necessary transaction reports. Prosecuting MSB violations for entities failing to follow MSB guidelines set forth by FinCEN is frequently limited by prosecutorial discretion.

Illicit activity conducted on the dark web is primarily funded using bitcoins. Payment methods on the dark web marketplaces consist solely of digital currencies. The marketplaces on the dark web openly sell illegal drugs, child pornography, stolen PII, weapons, and other solicitations for criminal activity. Estimates on the amount of commerce conducted on the dark web are speculative, but the daily transactions from 2014 were estimated to exceed $650,000 USD. The Onion Router (TOR) further anonymizes transactions in the dark web marketplaces.
TOR, one of the only ways to access the dark web marketplaces, conceals the IP addresses of user’s computers (Marr, 2016).

The FinCEN (2013) guidance regarding enforcement of the illegal use of digital currencies focused on what is described as enforcement focus points for digital currency. This is the conversion point of fiat currencies to digital currency or digital currency to fiat currency and is the main focus of investigations. The guidance to investigate these gatekeepers as an MSB entity could create numerous prosecutorial challenges unless the individuals operating as an unlicensed MSB commit a specific unlawful activity (SUA).

**Case Example**

Silk Road, the dark web marketplace, provides the most notable case example involving the illicit use of digital currency. Between 2011 and 2013, Ross Ulbricht created and operated the Silk Road marketplace, which facilitated the sale of illegal drugs, child pornography, stolen PII, firearms, and provisions of illegal services (Kleiman, 2013). Silk Road was removed from the Internet by a forfeiture seizure order when Ulbricht was arrested. Investigators estimated the site facilitated the sale of illegal products and services totaling 9.5 billion bitcoins. At the time of the arrest, the value of bitcoins transacted during the two-year operation of the marketplace was estimated at approximately $1.2 billion USD (U.S. Immigration and Customs Enforcement [ICE], 2013). Additionally, at the time of the investigation, the total amount of bitcoins in circulation was 11.75 million coins. The Silk Road marketplace transactions were solely conducted with bitcoins (Kleiman, 2013).

During an IRS Bitcoin training event, IRS Criminal Investigations (IRS-CI) Special Agent Tom Klepper (personal communication, August 30, 2016), provided updated information regarding the current threat of bitcoin use in the context of dark web marketplaces. Klepper made
the distinction between the dark web and the darknet. The darknet involves marketplaces, which host criminal activity, on the dark web. Klepper advised of the existence of approximately 200,000 to 400,000 websites on the dark web and estimated that 90% of the sites host illegal activity. Klepper also provided current information regarding the amount of Internet traffic on the TOR network, which hosts the marketplaces. During the Silk Road investigation, the network activity consisted of 148,000 U.S. users per day and 900,000 users per day worldwide. Current network activity was noted at 362,000 U.S. users per day and 2,000,000 users per day worldwide. A formal directory of the marketplaces does not exist; however, Klepper also noted the identification of more than 50 marketplaces currently identified on the dark web. It is assumed there are many additional unidentified marketplaces.

**U.S. Efforts to Control Money Laundering**

In 2015, the United States Treasury issued the National Money Laundering Risk Assessment report, which cited estimates regarding the threat of illicit finance in the U.S. The report noted that more than $300 billion dollars were generated through illicit sources; however, these numbers include various elements of fraud, including health care fraud and tax fraud. More than $64 billion dollars of the estimate is attributed to the trafficking of illegal drugs (United States Department of the Treasury, 2015).

The Currency and Foreign Transactions Reporting Act of 1970, also known as the Bank Secrecy Act (BSA), requires the maintenance of a financial institutions customer transaction records to assist law enforcement with combating money laundering (Federal Deposit Insurance Corporation [FDIC], 2004). The USA PATRIOT Act of 2001 amended the BSA to strengthen the anti-money laundering (AML) provisions. The BSA requires the report of cash transactions over $10,000 USD, suspicious transactions, foreign banking activity, and the transportation of
more than $10,000 USD across U.S. borders. Reports generated from BSA requirements are maintained by FinCEN, under the U.S. Treasury, and disseminated to law enforcement for investigative purposes (FDIC, 2004).

An integral portion of the BSA requires financial institutions to maintain information regarding account holders of the institution. Institutions maintain what is typically referred to as a know your customer (KYC) program that entails recording information for the customer’s PII; including name, date of birth, social security number, address, and phone number. Financial institutions also typically gather biographical information on customers regarding employment or the type of business customers operate. Once institutions gather information regarding customers of the institution, BSA requires ongoing customer due diligence (CDD) protocols to identify money laundering activities (FDIC, 2004).

Before 1986, financial institutions were bound to BSA provisions; however, money laundering was not criminalized in the U.S. until the passage of the Money Laundering Control Act of 1986. The legislation criminalized the use or concealment of funds derived from a SUA by conducting a financial transaction. The legislation also included the transportation or transmission of illicit funds within the U.S. or abroad. Another important inclusion of the legislation was the criminalization of conducting any transactions to avoid state or federal reporting requirements, such as currency transaction reports (FinCEN, n.d.).

In 1990, The United States Department of the Treasury created FinCEN to act as a repository for all BSA reports created by financial institutions and to support law enforcement investigations of money laundering and financial-based crimes. The scope of FinCEN was expanded in 1994 to include the responsibility of issuing guidance and regulations in the scope of the BSA. While FinCEN is part of the U.S. Treasury, their responsibilities include crafting
regulations that fall under the BSA, ensuring compliance with the BSA by institutions, and issuing guidance for interpretations of existing money laundering regulations (FinCEN, 2006).

In the context of money laundering, a financial institution is broadly defined to include depository institutions and foreign correspondent banks as well as non-banking financial institutions. Non-bank financial institutions include business areas that are not typically considered to be involved in banking, such as casinos, securities brokers, and MSBs. FinCEN requires these institutions to follow reporting requirements and maintain customer transaction records and KYC information (FDIC, 2004).

FinCEN initially provided guidance regarding entities that are considered an MSB in 1997 and clarified the definition in 2009 (FinCEN, 2009). FinCEN defines an MSB in the following manner:

A currency exchange; an issuer, redeemer, or cashier of travelers’ checks, checks, money orders, or similar instruments; the United States Postal Service; a person involved in the transmission of funds; and any business or agency which engages in any activity which is determined by regulation to be an activity which is similar to, related to, or a substitute for these activities. (p. 22130, para. 8)

FinCEN created the definition of an MSB to include entities that provide transactions and services similar to a traditional banking institution, yet they do not meet FinCENs definition of a bank. Within the FinCEN guidance provided for MSB entities, all BSA regulations apply to an MSB in the same manner as they do to a traditional bank (FinCEN, 2009).

Money Laundering Threats

Bitcoins are currently acquired through various distribution channels, which conduct transactions in a manner similar to an MSB. Although some of these individual transactors and
entities conduct exchanges for bitcoins, many are not registered as an MSB. The unlicensed entities typically do not collect information on individuals for KYC purposes in the manner that licensed MSB entities operate. In this scenario, individuals can buy or sell bitcoins without the required data collection for reporting requirements and KYC purposes as required by FinCEN for MSB activity (FinCEN, 2013).

One of the most popular selling exchanges for bitcoins is Local Bitcoins (localbitcoins.com), an Internet marketplace on the clear web. On this website, users advertise to buy or sell bitcoins and normally conduct transactions with cash. Individuals that operate as an MSB through this type of exchange charge a 10-15% fee to the individual wishing to buy or sell bitcoins (“Buy and,” 2016). Registered bitcoin and digital currency MSB companies buy and sell bitcoins for an average 1-2% fee (Perez, 2015). Local Bitcoins remains popular, as KYC data is not collected in the transactions between individuals (Tuwiner, n.d.).

New emerging money laundering threats with bitcoins also include unlicensed bitcoin ATMs where bitcoins can be purchased with cash or gift cards (O’Connell, 2016). The ATMs either collect minimal KYC information, which is not verified, or they do not collect any KYC information. Most of the bitcoin ATMs are individually owned and operated and placed within businesses under separate ownership. An additional area of concern for bitcoin transactions involve various Internet-based exchanges of property for bitcoins (purse.io), overseas stored value cards and wire transfer services (uquid.com), and bitcoin tumbling services. Tumbling services conceal the true source and destination of bitcoin transfers by dividing the transfer into smaller payments transacted at the same time in the blockchain (Kleiman, 2013).
Literature Review

This project focused on the utilization of bitcoins in commerce and how the usage aligns with U.S. laws, policies, and regulations. The project also consisted of an analysis of investigations within the current money laundering laws and the challenges presented by bitcoins for investigators. The use of bitcoin is a perfect medium for criminals to transmit criminal proceeds locally or globally (Bryans, 2014; United States Department of Homeland Security [DHS], 2014). Regulators and investigators have struggled with the new premise of digital currency and the problems associated with this new form of electronic value transfer system (Ajello, 2015). Bryans (2014) noted that regulators demonstrated a lack of foresight with regulating digital currency.

In this portion of the project, the emphasis lies within the review of scholarly journals, government publications, and technology trade based information to answer the following questions: What are the current money laundering threats presented by bitcoin use? How can U.S. peer-to-peer bitcoin transactions be regulated to remove the anonymity component of an informal MSB? How has failing to clearly define bitcoin as a currency, commodity, property, or value transfer system impacted the enforcement of the illegal utilization of bitcoin? How could the Financial Crimes Enforcement Network (FinCEN) assist law enforcement with bitcoin investigations? Research examined current regulations, laws, and enforcement techniques as well as proposed changes to attempt to curb threats posed by bitcoins and digital currency in the U.S.

The Bitcoin Network and Bitcoins

The Bitcoin network, and the use of bitcoins as a value transfer system were created by Satoshi Nakamoto (2008) in a paper describing the concept. The premise involves creating a decentralized network where a central authority is not involved with creating, issuing,
controlling, or accounting for the digital currency. Bitcoins are referred to as convertible, digital cryptocurrencies. The currency is considered convertible as it is rapidly exchanged between the digital form and fiat currency. The intention behind bitcoins is to enable users to conduct peer-to-peer transactions, essentially anonymously, across the globe (DHS, 2014).

The Financial Action Task Force (FATF) issued money laundering guidance regarding bitcoins and other digital currencies. The FATF summarized bitcoin as “(1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but does not have legal tender status” (The Financial Action Task Force [FATF] 2015, p. 2, para. 2). The FATF also emphasized that bitcoins can further enable criminals to conceal the laundering of illicit proceeds. Kiviat (2015) cites that bitcoins are a medium of exchange, rather than a store of value, and as such facilitate money laundering. Kiviat also mentioned that bitcoins are utilized in the same way as fiat currencies, yet without the same regulations imposed on fiat currencies.

Cryptocurrencies. Users of bitcoin and their bitcoin wallets comprise the Bitcoin network. The network maintains a ledger of bitcoin transaction activity. The wallets consist of a public key comparable to a checking account number and a private key comparable to a personal identification number (PIN). The difference in this comparison lies within the complex mathematical algorithm unique to the bitcoin wallets not typically utilized in checking account and pin numbers. Bitcoin wallets do not contain any PII regarding the owners of the wallets, which lends to anonymity (Levin, O’Brien, & Zuberi, 2015).

The Bitcoin ledger containing transaction history is the blockchain. Following a transaction of bitcoins between two users, the transaction details are stored in a block of the blockchain. The block is a pool of transactions, which await authentication by the Bitcoin network. The Bitcoin network users then verify the transactions in the block by completing a
complex mathematical algorithm. This mathematical algorithm is contained in the transactor’s wallet address. The available balance for the wallet is transmitted to the network once a transfer is initiated. The public key holds the information for the balance of the wallet (Franco, 2015).

Upon verification, the block is completed and the transaction’s new block is added to the blockchain. The transactions are irreversible after confirmation and addition to the blockchain (Franco, 2015). The blockchain is a public ledger of all bitcoin transactions in the Bitcoin network since the inception of the Bitcoin network. Every block in the blockchain is revalidated during the formation of each new block (DHS, 2014).

Bitcoin network users, known as miners, validate bitcoin transactions. Miners complete a new block within the blockchain approximately every ten minutes, with the goal to complete the new block before other miners. Miners receive new bitcoins for solving the block before other miners. Once the entire Bitcoin network confirms the solution to the aforementioned complex mathematical algorithm, the new block is published to the blockchain (See Appendix C). For miners to be effective, significant computing power is needed. As the block chain continues to grow, solving each block through cryptography becomes more difficult (Böhme, Christin, Edelman, & Moore, 2015).

**Bitcoin Money Laundering Threats**

The use of bitcoins has surpassed the daily transaction volume of PayPal and Western Union in the realm of monetary value transfers (Mandjee, 2015). The inherent design of bitcoins allows anonymity for users conducting transfers of value. Digital currencies, including bitcoin, provide a simple method for criminals to launder money (Bryans, 2014). Traditional methods of obtaining bitcoins through licensed MSBs do not eliminate the anonymity of bitcoins; however, the MSBs are required to maintain KYC information for transactions. New methods of obtaining
bitcoins facilitate placement of funds into bitcoins while maintaining anonymity and enabling money laundering. These methods include peer-to-peer transactions, unregistered bitcoin ATMs, and property exchange services for bitcoins (Ajello, 2015).

**Peer-to-peer transactions.** One emerging trend with the peer-to-peer (P2P) transactions of bitcoins involves consolidated classified listings on the Internet (Kleiman, 2013). The most popular website for P2P advertising is localbitcoins.com. Local Bitcoins provide the opportunity for users to buy or sell bitcoins through coordination of the sale on the website. The purchases of bitcoins transpire locally or globally through unlicensed exchangers. The transaction fee on Local Bitcoins averages 10-15% (“Buy and,” 2016). This is a drastic increase in comparison to the average transaction fee of 1-2% for licensed bitcoin MSB exchangers (Perez, 2015).

P2P transactions allow subjects with quantities of illicit cash to convert the cash into bitcoins anonymously. In a typical P2P transaction conducted in person with cash, an arrangement is set for a predetermined transfer number of bitcoins at the current bitcoin market rate. Both parties meet in a public place, typically with a wireless Internet connection, to complete the transaction. The seller of the bitcoins obtains the bitcoin wallet information from the buyer and initiates the transfer of bitcoins. Once confirmed in the blockchain, the seller receives the fiat currency. In a P2P transaction, KYC information is not collected. The buyer can successfully accomplish the placement phase of money laundering by introducing cash into the financial system without generating any FinCEN reports (DHS, 2014). In a survey of the P2P exchange site localbitcoins.com, listings of bitcoins noted cash and online exchangers in 249 countries and 73,136 U.S. cities (“Bitcoin statistics,” 2016).

P2P transactions can also benefit criminals who obtain bitcoins through the sales of illegal goods and services on the dark web (DHS, 2014). According to IRS-CI Special Agent
Tom Klepper, dark web transactors selling bitcoins want to convert bitcoins into cash quickly before there is a change in the bitcoin value. To maintain anonymity, criminals avoid exchangers and engage in P2P transactions. Transactors that are seeking a quick sale of bitcoins through P2P transactions also frequently encounter higher exchange rates of 10-15% (personal communication, August 30, 2016). Sonderegger (2015) noted that bitcoins fluctuate in value akin to highly volatile commodities; however, the value threat does not concern criminals utilizing bitcoins.

In addition to the aforementioned in-person transactions, other P2P schemes (methods of transfer) have emerged. Buyers in different geographical regions are directed to deposit fiat currency into the seller’s bank accounts, send a wire transfer, mail money orders, or simply mail currency. Certain transactors also accept gift cards for bitcoins or payments through the PayPal service (Ajello, 2015). Each of these methods elicits a level of risk for the buyer; however, most buyers have feedback ratings on websites, such as Local Bitcoins, to give buyers a level of assurance about transactions. In some of these cases, depending on the transaction amounts, the financial institutions involved in the transactions generate FinCEN reports (DHS, 2014).

**Overseas transfers.** Fiat currency, when converted to bitcoins, or another digital currency, enables simple overseas transfers outside of formal banking institutions. Users within a criminal organization can repatriate criminal proceeds to other countries without fear of interdiction or detection by law enforcement. Conversely, currency can be converted to bitcoins in foreign jurisdictions with limited money laundering controls, then transmitted to receivers in the U.S. Moreover, foreign and domestic actors may utilize bitcoins for terrorist funding. Transactions in foreign jurisdictions may be outside the reach of law enforcement for investigative purposes in certain jurisdictions (FATF, 2015).
Uquid is one example of a foreign company that engages in the conversion of bitcoins with possible money laundering implications. Located in Gibraltar, Uquid offers customers a prepaid Visa card solution without any KYC or AML processes, which allows for anonymity. The VISA cards are reloadable with bitcoins to make purchases, remove fiat currency from ATMs worldwide, and make wire transfers (“Uquid Card,” 2016). The U.S. Department of State deemed Gibraltar a jurisdiction of concern for money laundering (United States Department of State, 2016).

**Bitcoin ATMs.** The advent of privately owned ATMs that strictly sell bitcoins without collecting KYC information rose to popularity partially due to bitcoin users desire to remain anonymous and the rising popularity of illegal commerce on the dark web. Many of these ATMs only sell bitcoins to consumers for cash and few collect any PII from purchasers (Hyman, 2015). The first bitcoin ATM was introduced in 2014. As of 2016, there are approximately 640 in use worldwide (O’Connell, 2016). Moreover, bitcoin ATMs charge transaction fees between 10-15% to purchase bitcoins (“Buy and,” 2016). The ATMs provide a convenient source point for transactors to obtain bitcoins anonymously. A great number of bitcoin ATM users desire anonymity in these transactions to facilitate dark web transaction anonymity (Hyman, 2015).

In some states within the United States, these ATM services need to register as MSBs. ATM services registered as MSBs must abide by reporting requirements and collect KYC information. ATM transactions are not reliable in collecting KYC information, as there is not a verification process that can be accomplished at the ATM. Additionally, the identity of the transactor at the ATM can not be verified (Hyman, 2015).

If the ATM obtains KYC information during transactions, few companies conduct any due diligence procedures to verify the collected information. Some ATM institutions only
require the collection of a customer’s phone number, which may be a pre-paid, anonymous phone. Other companies take a photograph of identification cards; however, fraudulent identification cards are easily obtained on the dark web or from other criminal entities to evade KYC verification. ATM services are not able to verify the authenticity of identification cards, which negates KYC attempts (Hyman, 2015).

**Dark web transactions.** In the Silk Road case, investigators learned transactions for illegal goods and services exclusively utilized bitcoins. Bitcoins are the preferred payment method for dark web transactions as they maintain anonymity and conceal criminality. Buyers and sellers on the dark web often quickly convert bitcoins into fiat currencies after transactions. The turnover of bitcoins supports the notion that bitcoins are not a method of storing value, but merely a medium of exchange (Kiviat, 2015).

Small (2015) asserts that illegal enterprise activity on the dark web has created a new section of society willing to engage in buying and selling illegal items with bitcoins. Small emphasized that the anonymity component of the dark web and bitcoins enable those who would not normally entertain criminal behavior to engage in illegal activity on the dark web marketplaces. Lack of regulatory control of the dark web and digital currency further exacerbates the issues of these criminal enterprises.

**Bitcoin tumbling.** Since all bitcoin transactions post on the public ledger of the blockchain, bitcoin users have begun to utilize digital currency *tumblers* (Allison, 2015). Tumblers, also named mixers or laundry services, obfuscate bitcoin transactions between parties to make them less identifiable by law enforcement and other users on the network. Since the blockchain contains bitcoin transactions, users desire to mask their transmissions of bitcoins through tumblers to facilitate money laundering (Redman, 2016b).
Tumblers take multiple transactions and join them together for disbursement to payees through multiple senders. In this method, if person A was sending person B ten bitcoins, the bitcoins arrive from multiple senders. Person B may receive ten separate transfers, from multiple, completely different senders utilizing the tumbler, which equal ten bitcoins. In this manner, transaction masking occurs between the sender and receiver in the bitcoin exchange (Redman, 2016b).

Per IRS-CI Special Agent Tom Klepper, tumbling service fees vary between 5-15%. The fees increase based on the volume of coins tumbled. The use of multiple wallets for the output of tumbled coins also increases anonymity and incurs a larger fee (personal communication, August 30, 2016).

**Bitcoin property exchanges.** Purse.io is a website facilitating the exchange of property for bitcoins. The website allows for global and anonymous P2P unregistered bitcoin exchanges by manipulating purchases on Amazon, the popular retail website, which does not accept bitcoin payments. Users who want to purchase items on Amazon create a wish list of items on an Amazon account and list these items on the Purse marketplace. Wish lists are a built-in feature for Amazon, where users create a list of items they would like to purchase in the future or for others to purchase for the user. Customers who wish to purchase bitcoins find an item on an Amazon wish list and purchase the item on behalf of the subject with the bitcoins. The item is delivered directly to the subject selling the bitcoins (Cawrey, 2014).

A bitcoin transfer to the customer purchasing the Amazon item for the other party completes the transaction. The subject purchasing the item on Amazon pays full retail for the item on a wish list, yet the bitcoin seller gives the purchaser 15% less in bitcoin value for the item. In this manner, bitcoin purchasers pay a 15% transaction fee to obtain bitcoins in an
anonymous manner. Neither Purse nor Amazon conducts KYC or AML programs, which enhances the anonymity of the marketplaces (Cawrey, 2014).

**Emerging threats.** After investigators infiltrated the dark web marketplace Silk Road and seized bitcoins from its creator, Ross Ulbricht, bitcoin users have become concerned about the anonymity of bitcoins. Since the Bitcoin network ledger is publically available, users have begun to explore other digital currency options with increased anonymity. Monero, a new digital currency, has emerged and is more secure and anonymous than bitcoin (Wirdum, 2016).

Monero has technology built into the currency that automatically tumbles exchanged coins to make transactions more anonymous. Dark web marketplace sites, such as AlphaBay, have begun to accept Monero for transactions in addition to bitcoin. Most users obtain Monero on dark web marketplaces, which function as underground, unlicensed exchange sites. Users exchange bitcoins for Monero, and then use Monero to purchase illegal products and services on the dark web (Torpey, 2016).

Each of the aforementioned obfuscation methods are significant money laundering threats with the use of bitcoin by criminal enterprises. These activities further hide the source of illegal proceeds utilized by criminals, and conceal the true owner of a bitcoin wallet. Numerous government agencies and financial institutions have examined these methods and are attempting to explore options for reducing criminal utilization of bitcoins and digital currency (Mandjee, 2015).

Per IRS-CI Special Agent Tom Klepper, the fees charged in P2P bitcoin exchanges, ATM bitcoin purchases, and bitcoin property exchanges mirror fees charged in traditional currency money laundering transactions. Tumbling fees also match fees typically charged for
traditional money laundering. Each of these bitcoin based services intends to mask the identity of the owner of bitcoins (personal communication, August 30, 2016).

Regulating P2P Transactions to Reduce Money Laundering Threats

In 2013, FinCEN reacted to the money laundering threats of unregulated digital currencies and issued the guidance titled Application of FinCEN’s regulations to persons administering, exchanging, or using virtual currencies. In this guidance, FinCEN determined that subjects who administer or exchange virtual or digital currency are required to follow regulations of MSBs. The two-prong test provided by FinCEN (2013) for those who administer or exchange digital currencies involves entities that: “…(1) accepts and transmits a convertible virtual currency, or (2) buys or sells convertible virtual currency for any reason is a money transmitter under FinCEN’s regulations…” (p. 3, para. 1).

FinCEN (2013) asserts that a money transmitter, which falls under MSB guidelines, applies to “…a person that provides money transmission services, or any other person engaged in the transfer of funds” (p. 3, para. 1). FinCEN further delineates that the guidance is not specific to currency as it applies to a value that acts as a substitute for money and ultimately applies to digital currency. In the context of bitcoins, anyone who falls under the two-prong test provided by FinCEN, and acts as an administrator or an exchanger, must follow the guidelines of MSBs (FinCEN, 2013).

In 2014, the FATF issued the report Guidance for a risk based approach – virtual currencies. The FATF noted that anti-money laundering efforts should focus on areas where currency can enter the digital currency networks. In this guidance, the FATF suggests regulations aimed at digital currency exchangers require compliance with KYC and AML programs in the same manner as traditional financial institutions. The FATF also advises for digital currency
exchangers to register as an MSB with the appropriate government Financial Intelligence Unit (FIU), such as FinCEN (FATF, 2014).

**Requirements of MSBs.** The BSA requires an MSB to follow guidelines including registration, recordkeeping, and reporting. Pursuant to 31 U.S.C. § 5330, all MSBs are required to file registration paperwork with FinCEN, and renew the registration every two years. MSBs are also required to maintain records concerning: (a) expected business volume; (b) registered agents of the business; and (c) business ownership information (FDIC, 2004).

MSBs are also required to have a KYC program to collect PII on customers and an AML program to instill compliance and report suspicious activity. MSBs must also maintain records of currency exchanges exceeding $10,000 USD, including collecting PII on subjects conducting the exchange. MSBs are also required to complete currency transaction reports (CTR), reports for the international transportation of currency or monetary instruments (CMIR), and suspicious activity reports (SAR) where applicable. The thresholds for a CTR or CMIR are transactions exceeding $10,000 USD (FDIC, 2004).

**Criminal penalties for unlicensed MSBs.** Under 18 U.S.C § 1960, entities operating as an unlicensed MSB are subject to a five-year criminal sentence or financial penalties. MSBs who fail to register with FinCEN, or transmit funds that are proceeds from illegal activity or intended to promote criminal activity, are subject to punishment under 18 U.S.C. 1960. The statute also prescribes that MSBs must obtain a state license as an MSB, if required by the state, in the regions of operation (FinCEN, 2009).

**Enforcing MSB requirement for bitcoin exchangers.** Absent a federal prosecution for unregistered MSB violations, individual state legislation and regulations limit the actions of state prosecutors. State laws regarding MSB requirements are scattered and vary greatly by region.
Most states have varying definitions regarding the requirements for each money transmitter or MSB in the areas of registration including KYC, AML, and reporting. Moreover, arguments were proposed regarding the undue burden imposed on MSBs due to inconsistent regulations imposed by multiple state laws (Grossman & Rivkin, 2016; Lo, 2016).

**U.S. v. Faiella.** In *U.S. v. Faiella* (2014), The Southern District of New York prosecuted Robert Faiella for a violation of 18 U.S.C. § 1960 for operating as an unlicensed MSB and laundering bitcoins on the Silk Road dark web marketplace. Faiella alleged three important distinctions during his trial: (a) bitcoins are not money; (b) operating a bitcoin exchange does not facilitate transmitting money as prescribed in 18 U.S.C. § 1960; and (c) due to points one and two, he was not acting as a money transmitter. U.S. District Court Judge J. Rakoff ruled that bitcoin qualified as money and “Bitcoin can be easily purchased in exchange for ordinary currency, acts as a denominator of value, and is used to conduct financial transactions” (U.S. v. Faiella, 2014, p. 2, para. 2). This ruling gave the first definition of bitcoin considered akin to money in Federal case law.

It is important to note the circumstances of the Faiella case and the volume of the transactions. Faiella operated on the dark web marketplace Silk Road as a bitcoin exchanger and purchased bitcoins from co-conspirator, Charlie Shrem. Shrem operated a bitcoin exchange and sold bitcoins to Faiella. Faiella then sold bitcoins to Silk Road users at a profit and transacted as an MSB. Faiella sold over $1 million USD worth of bitcoins to Silk Road users. The bitcoins were then used to purchase illegal goods and services (U.S. v. Faiella, 2014).

At the conclusion of the case, Faiella was convicted of operating an unlicensed money service business. Faiella was offered a plea to the charge and the additional charge of conspiracy to commit money laundering under 18 U.S.C. § 1956(h) was dropped. Despite the volume of
transactions conducted by Faiella, four years in prison was the only consequence for the offense. Faiella and Shrem were ordered to forfeit $950,000 for their offenses (Raymond, 2015).

**U.S. v. Murgio.** In September 2016, a Memorandum and Order was filed in the United States District Court of the Southern District of New York in the case U.S. v. Murgio, et al. in response to pre-trial motions to dismiss the case. In U.S. v. Murgio, charges for 18 U.S.C § 1960 and 18 U.S.C. § 1956, in addition to other charges for operating a bitcoin money laundering operation, were levied against Anthony Murgio. The charges against Murgio alleged the opening of an unlicensed MSB bitcoin exchange called Coin.mx and subsequently exchanging currency to bitcoins for known criminals and laundering the proceeds from the activity. Murgio was also exchanging bitcoins into cash for known cyber criminals (U.S. v. Murgio, 2016).

Murgio filed a pre-trial motion that alleged charges for 18 U.S.C § 1960 did not apply. The basis for the motion was that bitcoins are not *funds* as prescribed in the statute and such the charge was not applicable. Additionally, Murgio alleged that he could not be a money transmitter, as he was not transmitting funds (U.S. v. Murgio, 2016).

United States District Judge Allison Nathan denied the motion based on three main premises. The first premise pertained to the language within 18 U.S.C § 1960 which defines money transmitting “…to include transferring funds on behalf of the public by any way and all means…” (U.S. v. Murgio, 2016, p. 4, para. 2). Judge Nathan asserted that the key term was *funds* in the argument and referred to a definition given by Webster’s Dictionary, which states that funds include “…available pecuniary resources…” (U.S. v. Murgio, 2016, p. 5, para. 4). Judge Nathan further stated that Webster’s Dictionary defines pecuniary as “…taking the form of or consisting of money” (U.S. v. Murgio, 2016, p. 5, para. 4). Further, Judge Nathan states that
Webster’s Dictionary defines money as “…something generally accepted as a medium of exchange…” (U.S. v. Murgio, 2016, p. 5, para. 4).

The second premise cited by Judge Nathan noted the prior case of U.S. v. Faiella that bitcoins qualify as money under federal law. Additionally, bitcoins qualify as funds and further quash the argument that 18 U.S.C § 1960 does not apply to bitcoins. The court further cited that Congress utilized statutorily broad language to address future money laundering threats while drafting 18 U.S.C § 1960 (U.S. v. Murgio, 2016).

The last premise addressed by the court was about prior guidance and rulings in relation to FinCEN, IRS, and the CFTC. Each of these agencies gave different perspectives regarding bitcoins and digital currency; however, the court rejected the context of the prior rulings. The court rebutted Murgio’s argument, specifically addressing citations from FinCEN, IRS, and the CFTC that failed to define the term funds (U.S. v. Murgio, 2016).

The final ruling of the court stated bitcoins fit the definition of funds, the definition of money, and 18 U.S.C § 1960 applied to bitcoin cases. The court also determined that Murgio fit the definition of an MSB due to the transfer of bitcoins to others in the form of a business transaction and making a profit from activities alleged in the indictment. The court also rejected Murgio’s allegation that funds should be more narrowly defined as currency (U.S. v. Murgio, 2016).

**New regulations for digital currency.** The Code of Federal Regulations (CFR), 31 C.F.R. § 1010.100(m) defines currency as “The coin and paper money of the United States or of any other country that is designated as legal tender and that circulates and is customarily used and accepted as a medium of exchange in the country of issuance” (Prentis, 2015, p. 621, para. 3). Given this definition, bitcoin does not fit within the parameters as currency. Additionally,
since bitcoin has a market cap of 21 million units and a continuous fluctuation in the value of each bitcoin, it will never be a customarily accepted medium of exchange (Prentis, 2015). The original concept of bitcoin was as a medium of exchange rather than as a currency (Kiviat, 2015).

The MSB statutes, specifically 18 U.S.C. § 1960, have the implied connotation of the involvement of U.S. currency. Since bitcoin may not fit the definition of currency, the MSB statute does not specifically apply to digital currency or bitcoin. FinCEN guidance has applied the MSB statute to bitcoin exchangers engaged in activities of an MSB; however, the guidance also does not define bitcoin as currency (FinCEN, 2013).

Notwithstanding the rulings in U.S. v. Faiella and U.S. v. Murgio, bitcoin has not been formally identified as money or currency by U.S. legislators or regulators. Bitcoin needs a specific legal classification for regulation and enforcement purposes. Specific mandates are needed to eliminate future confusion concerning the state of bitcoin (digital currencies) as being a currency, commodity, commodity money, or security (Mandjee, 2015).

Regarding whether bitcoin meets the requirements set forth in being a medium of exchange for an MSB, the MSB statute has a vague clause which states “…a person who engages as a business in the transmission of funds; and any business or agency which engages in any activity similar to, related to, or a substitute for these activities” (Levin et al., 2015, p. 336, para. 3). The Code of Federal Regulation, Chapter 31, describes a money transmitter as “… a person that engages in the acceptance of currency, funds, or other value that substitute for currency from one person and the transmission…to another location or person by any means” (Levin et al., 2015, p. 336, para. 3). Moreover, Levin et al. (2015) addressed that the MSB definition does not draw a distinction between digital currency and fiat currency.
As bitcoin and digital currency are utilized as a value transfer system, typically purchased with fiat currency, digital currency exchangers continue to fit the definition of an MSB in the spirit of the legislation. There is a need for new legislation and statutory definitions for bitcoin and digital currency specific to these mediums of exchange. Additionally, the existing MSB laws can be used as a guide for constructing and enacting new legislation and regulations for digital currency (Mandjee, 2015).

There is a need for specific legislation to combat crimes perpetrated through bitcoin and digital currency. As digital currency is different from traditional currency, legislation needs to evolve with the advances of new technology. New legislation can enable clarity with definitions of digital currency and remove ambiguity for enforcement (Meredith & Tu, 2015).

Kiviat (2015) provided another definition of digital currency as a medium of exchange rather than a currency. Additionally, digital currency lacks comprehensive Federal regulations. Moreover, Kiviat addressed the need for legislators to propose regulations to mitigate digital currency risks. Small (2015) proposed that bitcoin and digital currency exchangers should be reclassified as a financial institution and thus be subject to the AML and KYC provisions of the USA PATRIOT Act.

**Enforcement of MSB statute for bitcoin cases.** The Federal MSB statute is an effective tool to target unlicensed bitcoin exchangers; however, the applicability of the statute in the realm of digital currency has not been clearly determined. One proposed strategy is the new definition for P2P bitcoin transactors as exchangers. Under this definition, a bitcoin exchanger would be subject to MSB regulations, and provide clarity to the applicability of the MSB statute to bitcoin and digital currency (Singh, 2015).

A second approach concerning the current MSB statute involves the problem of bitcoin
tumblers. Classifying tumblers as exchangers would enable the utilization of the MSB statute in cases of tumblers laundering bitcoins. This new classification for tumbling services would have the same effect as being subject to MSB regulations. Tumblers would be subject to AML and KYC procedures in addition to registration with FinCEN (Singh, 2015).

Kirby (2014) found that current MSB regulations, along with FinCEN guidance pertaining to digital currency, are an effective enforcement tool for unregistered P2P bitcoin exchangers. A need for concise and logical guidance from FinCEN for digital currency is also recommended. Kirby cited the need for regulators to focus on registered bitcoin MSBs, an entry point into the digital currency system. Kirby also noted that investigations could focus on data gathered by registered digital currency MSBs as they produce SARs prescribed by the BSA.

Strict regulations burden bitcoin exchangers and could force these entities to operate underground or in countries with lax money laundering controls. This is one argument against over regulation of bitcoin and other forms of digital currency. Forcing exchangers to operate in foreign jurisdictions through the implementation of excessive regulation could make law enforcement investigations more difficult (Sonderegger, 2015).

**New York Bitlicense statute.** New York’s Bitlicense legislation is the first state legislation regarding digital currency. It was codified under the New York Department of Financial Services Section 23 § 200, the statute specifically addresses bitcoin and other digital currencies. The Bitlicense statute outlines regulations for licensure of entities using digital currencies (“New York,” 2015).

The Bitlicense statute emulates FinCEN guidance regarding the treatment of digital currency exchangers. Bitlicense requires digital currency exchangers to register with the State of New York. The guidance further specifies digital currency exchangers maintain AML and KYC
programs. Bitlicense also requires entities that operate outside of New York, yet conduct business with residents or entities in New York, to obtain licensure with the State. The statute also requires entities to enact a cybersecurity program to protect digital currency held by the registered entity (“New York,” 2015).

AML requirements of Bitlicense require entities to file CTR and SAR reports to the State of New York, in addition to reporting to FinCEN. Applicants for a Bitlicense may not operate within the State of New York before approval by the State. Applicants must submit an extensive application including a non-refundable license fee of $5,000 USD, comprehensive business plan, financial history, policies and procedures, insurance and tax information, and biographical information regarding corporate officers (“New York,” 2015).

The New York Bitlicense regulation classifies activity requiring a license as *virtual currency business activity*. The classification covers the virtual (digital) currency activities of: (a) subjects or entities receiving virtual currency for transmission or transmitting it; (b) holding virtual currencies for others in a storage capacity; (c) acting as a business engaged in buying or selling virtual currency; (d) engaging in exchange services as a business; or (e) controlling, administering, or issuing virtual currency. The statute exempts merchants accepting virtual currency as payment, consumer’s utilization, and investors of virtual currency and some institutions already licensed under New York banking laws (“New York,” 2015). The statute also clearly defines virtual currency as “any type of digital unit that is used as a medium of exchange or form of digitally stored value or that is incorporated into payment system technology” (Hughes, 2014, p. 57, para. 3).

Bitlicense effectively forces businesses and individuals conducting MSB type services with digital currency to act in the same manner as a financial institution. Some enterprises in the
digital currency industry have expressed that Bitlicense is overbearing on innovation in the emerging markets of digital currency. Others have expressed that the cost of AML and KYC programs are too high for start-up companies in the digital currency arena. Proponents for Bitlicense have expressed that the regulation clearly defines digital currency and slightly expands on federal regulations for MSBs (Mandjee, 2015).

Hughes (2014) cited that Bitlicense requirements exceed federal requirements, and require mirrored FinCEN reporting to state agencies. Hughes also noted that Bitlicense requirements exceed those imposed on MSBs. Hughes added that Bitlicense appears to be overbearing for businesses engaging in the exchange of digital currency.

As of July 2016, only two entities had been able to obtain a Bitlicense in New York (Rizzo, 2016). The website Coindesk.com monitored the number of entities involved in digital currency and subject to Bitlicense in New York. As of August of 2015, Coindesk.com noted that nine exchangers applied for a Bitlicense and 15 entities ceased all operations in New York. Most of the entities that ceased operations did so shortly after the approval of Bitlicense in July of 2015 (“Bitlicense: Who,” 2015).

**The Unclear Definition of Bitcoin**

Multiple U.S. agencies proposed strategies and attempted to define digital currency classifications during the evolution of bitcoin. The agencies fit digital currency, including bitcoin, into their prospective legislative and regulatory frameworks based on individual definitions. The different agencies failed to reach consensus concerning definitions of digital currencies, including bitcoin. Regulatory guidance and case law have further compounded the imminent ambiguities regarding digital currencies (Sonderegger, 2015). Mandjee (2015) presented “…to date, no U.S. legislature or regulator has officially determined that bitcoin is a
currency, commodity, commodity money, or security” (p. 3, para. 6). Mandjee also noted that legislators used multiple definitions of bitcoin including digital currency, virtual currency, and cryptocurrency.

**FinCEN guidance.** In March of 2013, FinCEN issued interpretive guidance regarding virtual (digital) currencies in regards to how to comply with the BSA. The guidance defines digital currency as a medium of exchange, yet it did not define it as a currency. In the guidance, subjects that transact with digital currency and act as exchangers or administrators are subject to the rules and registration requirements of MSBs. Since the Bitcoin network is decentralized, the administrator requirement does not apply. If people engage in P2P transactions with bitcoins, they are subject to MSB requirements. Bitcoin miners and the use of bitcoins for commerce do not fit the MSB requirement (Prentis, 2015).

The FinCEN guidance defines digital currency as a convertible digital currency with, “…an equivalent value in real currency or acts as a substitute for a real currency” (Mandjee, 2015, p. 6, para, 5). Additionally, Mandjee addressed that bitcoin is not a traditional currency even though it functions similar to fiat currency. Mandjee cited the FinCEN definition of virtual (digital) currency as the most accurate by U.S. regulators. Sonderegger (2015) noted that FinCEN did not specify in the guidance how to classify bitcoins or digital currency.

**IRS guidance.** In 2014, the IRS issued Notice 2014-21 to address virtual (digital) currency. As noted by the IRS, virtual currency is a medium of exchange and a store of value that functions similar to fiat currency. In addition, the IRS specifically cited bitcoin as one of the currencies in question and referred to the FinCEN guidance regarding classification of virtual (digital) currency (IRS, 2014).

Despite the 2014 IRS guidance, Tsukerman (2015) noted the IRS deems digital currency
as property rather than currency. The IRS designation as property rather than currency is an inappropriate ruling regarding bitcoin by U.S. regulators as the designation negates the acceptance of bitcoin as currency. The ruling creates a wide array of tax implications for bitcoin investors and users of bitcoin. The value fluctuations of bitcoin and other digital currencies implicate users to liabilities for capital gains taxation and other tax liabilities (Tsukerman, 2015).

Slattery (2014) cited the need for IRS intervention with bitcoin and digital currency as they are a prime vehicle for tax evasion and movement of value to offshore tax havens. The 2014 IRS guidance notes three types of events that are taxable with the use of bitcoins: (a) purchases of goods (when a capital gain is realized due to bitcoin value increases); (b) wages paid to employees with digital currency; and (c) payments to independent contractors or service providers with digital currency. Per the IRS guidance, rewarded coins received by miners are considered taxable income (IRS, 2014).

CFTC ruling. In December of 2014, the CFTC Chairman Timothy Massad testified before U.S. Congress. Massad deemed that bitcoin and virtual currencies are subject to regulations set forth by the CFTC as a commodity. Massad noted bitcoin futures and swap contracts were akin to other commodity contracts. In addition, Massad cited the Commodity Exchange Act (CEA) for the applicability of the purview over bitcoin (Griffiths, 2015).

Griffiths stated “…the CEA’s broad definition of commodity, which is defined as certain agricultural goods and 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” is the framework for the bitcoin ruling as a commodity (2015, p. 325, para. 3). Prior to Massad’s testimony before Congress, the CFTC gave authorization to the first bitcoin swap exchange in the U.S. (Griffiths,
Prentis (2015) cites the consistency of the CFTC with the 2014 IRS guidance and claims that bitcoins fit the commodity definition.

**Securities and Exchange Commission (SEC) case.** In 2013, the Federal District Court in the Eastern District of Texas tried the SEC v. Shavers case. The defendant, Trendon Shavers, engaged in an investment business involving bitcoins called Bitcoin Savings and Trust. The business was ultimately a Ponzi scheme and the SEC brought a case against Shavers as they deemed the business was offering a security to investors (Griffiths, 2015). The question in the case was whether bitcoins met the requirements under the Securities Act of 1933 and the Exchange Act of 1934 to be determined as money (Prentis, 2015).

Investors gave Shavers bitcoins to invest and obtain a return on their investment. Shavers spent a majority of the invested bitcoins and lost a majority of the principle investments. The district court ruled that bitcoin is fungible as money, and that bitcoin was ultimately currency. The court also stated that bitcoin met the requirements under the Securities Act and the Exchange Act. After the ruling, many argued that bitcoins and digital currencies are also deemed securities (Prentis, 2015).

Griffiths (2015) cited that the SEC began to accept registration statements from companies desiring to offer bitcoin related securities. The Shavers ruling appeared to deem bitcoins as currency and as a security. Sonderegger (2015) noted, “…bitcoin investments meet the definition of an investment contract, and as such, are securities” (p. 192, para. 2).

**FinCEN Assistance with Bitcoin Law Enforcement Investigations**

FinCEN is the FIU for the U.S. and the primary regulating agency responsible for anti-money laundering. In addition to providing financial regulations and guidance, FinCEN is responsible for collecting, analyzing, and disseminating information to law enforcement in the
areas of financial crimes. The U.S. Department of the Treasury established FinCEN to bring together financial crime and financial industry experts to combat money laundering and terrorist financing. FinCEN is the primary data warehouse of all BSA information and dissemination to law enforcement partners (FinCEN, 2014).

According to the 2014-2018 FinCEN Strategic Plan, one of the key roles for FinCEN is to “develop and support effective technology systems to collect and analyze financial intelligence…” (p. 5, para. 5). As part of this goal, FinCEN’s objectives state a desire to continually design new technology systems to combat money laundering and terrorist financing. FinCEN also offers advanced research and analysis services for law enforcement (FinCEN, 2014).

Law enforcement shortcomings. In 2014, DHS issued a report on threats involving cryptocurrencies and digital currencies. In the report, the rapid evolution of digital currencies and the dark web are cited as problematic for law enforcement agencies due to the inherent anonymity and complexity of the investigations. The report also noted the advanced skill levels needed by investigators in these types of cases in addition to the need for sophisticated training and equipment (DHS, 2014).

DHS (2014) cites the absolute necessity of “advanced expertise, innovative technologies, and new methodologies to be able to fully investigate illicit activities using cryptocurrencies” (p.28, para. 1). In this realm, law enforcement needs to invest in the future by recruiting and retaining a cyber crime proficient workforce and enable investigators with proper technological tools. To pursue illicit digital currency use, investigators need forensic software tools and a digital currency transaction database (DHS, 2014).

Tropina (2016) noted that law enforcement is currently lacking training and expertise in
financial crimes as well as in the area of cyber crimes. The merging of financial crimes and cyber crimes in the areas of digital currency investigations involving the dark web further compounds the difficulties faced by law enforcement in these types of investigations. There is a need for law enforcement training, advanced technology, and software solutions to successfully investigate and prosecute digital currency crimes.

DHS (2014) recommends a centralized entity for data warehousing of leads and strategic information regarding digital currency. The entity should also act as a central point to disseminate training and investigative methods for digital currency cases. To be effective, dissemination needs to occur on the federal, state, and local levels of law enforcement. DHS referenced the need for constant research in the area of digital currency by a central authority or entity.

Meredith & Tu (2015) suggest tracking possible suspicious activity through the monitoring of bitcoin transactions on the public blockchain ledger. Identification of money laundering activity is possible by monitoring blockchain activity; however, the concern is a lack of KYC information on the bitcoin wallet holder. The only identifier in the blockchain is the public key to a wallet. This paradigm would be effective if information were known connecting a person to a specific wallet or public key.

**Blockchain analysis tools for investigators.** The partnership between DHS and Sandia National Laboratories dispelled the belief that bitcoin transactions provide absolute anonymity. The partnership exploited bitcoin transaction data stored in the blockchain for use in forensic investigations involving illicit bitcoin wallets. The new software intends to identify patterns in bitcoin payments and trace transactions to bitcoin wallets. The software will not identify the end user of a wallet, but may be able to trace illicit dark web transactions (Young, 2016).
New technology developed by Sandia National Laboratories could assist law enforcement with identifying money laundering schemes in digital currency, ransomware threats, and dark web transactions of illegal commerce. Sandia is developing the technology for DHS, but other federal law enforcement agencies may collaborate with DHS to use the technology. The goal of the software is to develop a graphical interface for investigators to track blockchain transactions and link previously identified aliases. The software has utilized known prior illegal bitcoin transactions and explored transactions matching the user’s wallet information in the blockchain (Padilla, 2016).

Chainalysis is another blockchain exploiting software utilized in investigations in a similar fashion to the Sandia product. Chainalysis has been successful in prior federal digital currency investigations. Block Seer, Ledger Labs, and Elliptic also offer competing blockchain analysis products and assist law enforcement with investigations (Redman, 2016a). The blockchain analysis products are congruent with DHS recommendations in regards to the need for advanced technologies in digital currency investigations. DHS also recommends storage of software solutions and accumulated data in a centralized data warehouse and liberal information sharing with law enforcement (DHS, 2014).

**Discussion of the Findings**

The purpose of this research was to explore the money laundering threats presented with the utilization of bitcoin and digital currency in the U.S. This project identified person-to-person transactions exploiting current money laundering regulations and anonymity within the illicit markets of the dark net with bitcoin. U.S. regulatory agencies offered differing opinions regarding how bitcoin and digital currency fit in their current regulatory frameworks. In addition, a small subset of case law provided varied definitions of digital currency. The research also
explored difficulties with law enforcement investigations presented by ambiguities with bitcoins and other digital currencies.

This project intended to identify a unified focus for application by U.S. regulators, legislators, and investigators involving illicit uses of bitcoin and digital currency. It also proposed to clarify methods to enhance or modify current regulations and legislation to provide comprehensive tools for investigators to use in illicit finance investigations concerning digital currencies. Finally, the study focused on types of additional regulations, if any, to address money laundering and exploitation of bitcoin and digital currency.

The Literature Review section consisted of scholarly, peer-reviewed research; however, since the field of digital currency is rapidly evolving, it also utilized information from government reports, subject matter experts, and trade journals. The research defined current exploitation methods of bitcoins for money laundering and the shortfalls of current regulations and legislation. The research also presented examples of court opinions from cases of illicit bitcoin use and revealed emerging technologies to support detection and enforcement of the presumed anonymous use of digital currencies. The Discussion of Findings section synthesized the findings from the Literature Review exploring basic digital currency themes including bitcoin threats, regulatory frameworks, clarified definitions, and enhanced methods for law enforcement investigations.

**Bitcoin Threats**

Many resources explained the inherent design of the Bitcoin network allows for divisive interpretations of the intent behind the Bitcoin architecture (Ajello, 2015; Kleiman, 2013; Mandjee, 2015). Regardless, cryptographic public and private keys remain as the only identifiers of bitcoins in the decentralized Bitcoin network. The network maintains a public ledger of all
bitcoin transactions, but these do not contain individual identifiers of PII. One of the founding design elements of the Bitcoin network is the lack of a centralized authority. This created a decentralized governance system, limiting control units in the Bitcoin network and allowing users anonymity (DHS, 2014; Small, 2015). The Department of Homeland Security (2014), in a study of digital currency, noted bitcoin is a perfect medium for criminals to transmit proceeds to confederates or other actors locally or globally.

The research noted bitcoins exchanged for fiat currency outside of traditional banking institutions monitoring systems present a major money laundering threat (Ajello, 2015; DHS, 2014; Mandjee, 2015; Small, 2015). Yearly totals for bitcoin transactions have the potential to surpass $52 billion USD, based on aggregate daily bitcoin transactions exceeding $143 million USD (“Output value,” 2016). The gross value of bitcoin transactions conducted outside traditional financial institutions increases the possibility for illicit use of bitcoins for money laundering. This credible threat for criminal financial activity presents a need for enhanced supervision of the Bitcoin network from U.S. regulatory and enforcement agencies (DHS, 2014).

The primary money laundering threat with bitcoin use lies within transactions conducted outside of registered MSBs. These unmonitored transactions allow bitcoin users to evade AML and KYC requirements and fundamentally remain anonymous during bitcoin transactions. Bitcoin transactions taking place through a registered MSB remove some of the anonymity (Ajello, 2015; DHS, 2014; Mandjee, 2015).

The research demonstrated that the greatest money laundering threat within bitcoin use is P2P exchanges by individuals functioning as unlicensed MSBs. The potential for actors to exchange currency for bitcoins without any formal data collection is limitless. As such, these transactions completed by unlicensed MSBs allow bitcoin users to evade FinCEN reporting and
KYC data collection. The research revealed P2P exchangers assist bitcoin users on the dark web to engage in illegal commerce. The dark web users quickly convert bitcoins back to currency after the completed transaction (Ajello, 2015; DHS, 2014; Kleiman, 2015; Mandjee, 2015; Small, 2015).

The unlicensed P2P exchangers essentially facilitate anonymous and illegal commerce on the dark web and in other forms of money laundering (DHS, 2014). Unlicensed P2P exchangers often charge customers a 10-15% fee for the exchange even though licensed MSB exchangers only charge a 1-2% fee (“Buy and,” 2016; Perez, 2015). The disparity in the fee is a typical amount charged by subjects engaged in money laundering for criminal organizations (DHS, 2014).

In the case U.S. v Faiella, Faiella laundered more than $1 million USD worth of bitcoins for persons engaging in illegal activity on the dark web. Faiella was found to be acting as an illegal MSB in this case, which further demonstrated the threats of illegal bitcoin MSBs. Faiella was just one actor that was able to launder $1 million USD in bitcoins in just under two years (U.S. v. Faiella, 2014).

In the case U.S. v. Murgio, the criminal indictment cites the laundering of more than $1.8 million USD worth of bitcoins by Murgio through Coin.mx over a 15-month period. According to the allegations, Murgio operated an illegal MSB and launder proceeds for known cyber criminals. The Murgio case is ongoing, but further demonstrates the threat of unlicensed bitcoin MSB entities supporting criminal organizations (U.S. v. Murgio, 2016).

P2P transactions are also prevalent through website classified sites, such as localbitcoins.com. These sites allow for online bitcoin transfers through the buy and sell listings for users not in the same geographical region. The site also allows users to arrange face-to-face
meetings for bitcoin exchanges. Research of localbitcoins.com revealed bitcoin buy and sell listings in 249 countries and 73,136 U.S. cities (“Bitcoin statistics,” 2016). These statistics added to the daily volume of bitcoin transactions amount to a large potential for money laundering of bitcoins through unlicensed P2P exchangers functioning as unregistered MSBs.

Overseas transfers of monetary value through the use of bitcoin are also a concern. P2P transactions involving overseas bitcoin transfers present increased threats due to the use of unlicensed exchangers for enhanced anonymity. These transactions can aid global criminal syndicates and terrorist organizations by providing anonymity during bitcoin exchanges (FATF, 2015).

Although limited in scale, bitcoin ATM and property exchange transactions can aid the facilitation of money laundering. Bitcoin ATMs enable users to obtain bitcoins anonymously, which are typically, and subsequently, used for the purchase of illegal items on the dark web. Bitcoin property exchanges also enable anonymity and typically serve the same function as the ATMs. Large scale money laundering conspiracies would not be effective with these methods (Cawrey, 2014; DHS, 2014; Hyman, 2015).

Bitcoin tumbling transactions obfuscate the blockchain trail of transactions creating a money laundering threat. The tumbling of transactions acts as a method of disguising exchanges of bitcoins from law enforcement and assists with criminals successfully evading capture after engaging in criminal activity. Bitcoin transaction tumbling assists in the completion of illegal activity by disguising exchanges of bitcoins from law enforcement. Unlike their unlicensed counterparts, licensed MSB bitcoin exchangers do not provide tumbling services (Allison, 2015; Redman, 2016b).
Regulatory Framework

U.S. laws and regulations address money laundering issues inherent with bitcoin; however, are not specific to digital currencies. The 2013 guidance from FinCEN addressed digital (virtual) currencies and attempted to clarify how bitcoin transactions fit the model of an MSB. This guidance referred to digital (virtual) currencies as a medium of exchange rather than defining it as a currency (FinCEN, 2013).

Despite AML, KYC, and PII requirements, MSB regulations concerning data collection and reporting requirements directly translate to digital currency issues (FinCEN, 2009). MSB exchangers are required to collect KYC information on customers and file specific FinCEN forms for suspicious transactions or transactions that exceed $10,000 USD (FDIC, 2004; FinCEN, 2013). U.S. v Faiella and U.S. v. Murgio demonstrate that individuals or organizations acting as an unlicensed MSB are subject to criminal and civil penalties.

State regulations of unlicensed MSBs engaging in bitcoin transactions vary greatly. The research noted MSBs attempting to engage in the legal exchange of bitcoins encounter problems with inconsistent state laws. MSBs are also subject to a Federal criminal indictment for noncompliance with state MSB registration requirements (DHS, 2014; Grossman & Rivkin, 2016; Lo, 2016).

The research regarding regulations derived from government research, journals, and subject matter experts provided a common suggestion to pursue unlicensed MSB bitcoin exchangers. In an effort to legitimate bitcoin transactions and collect PII of conductors, the researchers advised strict enforcement of P2P exchangers. In this manner, investigators could attempt to remove anonymity in bitcoin transactions (DHS, 2014; Kirby, 2014; Levin et al., 2015; Mandjee, 2015; Meredith & Tu, 2015).
**Bitlicense.** In 2015, New York State passed a regulation specific to digital currency termed the Bitlicense statute. The legislation set out specific registration and licensing requirements for any entities engaging in bitcoin commerce within the state, or entities with customers in the state. The requirements were similar to existing federal requirements for MSBs, but were also more stringent in other areas. Bitlicense gave a specific definition of what constituted licensure as virtual currency business activity. These definitions did not leave any gray area for interpretations. In contrast, current federal guidance and regulations allow for ambiguities and various interpretations (Hughes, 2014; “New York,” 2015).

Some authors cited Bitlicense is overbearing on smaller companies since AML and KYC programs are costly (Hughes, 2014; Rizzo, 2016). As of August 2015, 15 bitcoin exchangers ceased operations in New York due to the Bitlicense registration requirements. Only two entities had passed the Bitlicense registration process and were operating as licensed bitcoin exchanger in New York State as of July 2016 (“Bitlicense: Who,” 2015).

**Clarified Definition**

A common theme in the research demonstrated a lack of congruity in the definition of digital (virtual) currency within the framework of varying U.S. policies. Each regulatory agency appeared to view bitcoins and digital currency through a lens consistent with the purview of each agency. Different regulatory agencies deemed digital currency as either a currency, commodity, commodity money, or a security. There has been no official designation for digital currency by a U.S. legislature or regulatory agency to date (Griffiths, 2015; Mandjee, 2015; Prentis, 2015; Sonderegger, 2015; Tsukerman, 2015).

The framework of varying U.S. policies originated from limited regulatory guidance and minimal examples in case law (Mandjee, 2015; Sonderegger, 2015). Research revealed that
digital currency, including bitcoin, is considered a value transfer system and akin to currency. Since federal law only recognizes fiat currency issued and recognized by governments to fit the definition of a currency, regulators must determine how digital currency fits within existing laws and regulations (Ajello, 2015; Kleiman, 2013; Mandjee, 2015).

Per the three case law examples noted in the Literature Review, bitcoins are ultimately the same as currency or money within the definition of federal laws. U.S. v. Faiella cited bitcoins qualified as money within the context of MSB legislation due to ease of conversion from fiat currency and usability in financial transactions (U.S. v. Faiella, 2014). U.S. v. Murgio noted that bitcoins qualify within the statutory definitions of funds and money (U.S. v. Murgio, 2016). SEC v. Shavers deemed bitcoins are akin to currency due to the similarity of transactions between fiat currency and bitcoin transfers. (Griffiths, 2015). These three cases concluded that bitcoins are ultimately the same as money or currency within the constructs of federal law.

**Methods to Enhance Law Enforcement Investigations**

The 2014 DHS report concerning virtual (digital) currency, which specifically addressed bitcoins, noted shortcomings in current law enforcement efforts to pursue the illegal uses of digital currency. The report also cited law enforcement difficulty in pursuing dark web investigations involving illegal commerce. One of the themes of the DHS report addressed a lack of understanding concerning advanced technology and the subsequent difficulty completing the complex investigations (DHS, 2014).

DHS noted a lack of resources, training, and knowledge specifically required for digital currency and dark web investigations. There is a lack of adequate training amongst law enforcement investigators related to investigating crimes involving advanced technology or illicit
finance. The merging of the two areas further convolutes the advancement of criminal investigations in the area of digital currency (DHS, 2014).

Advanced tools and data management were deemed necessary for success in digital currency investigations. Specifically, advanced software and technology tools are imperative for successful investigations involving digital currency and the dark web. A centralized data warehouse of information involving investigative leads is also critical for investigators (DHS, 2014).

FinCEN, the FIU for the U.S., is tasked with assisting law enforcement investigators in the area of financial crimes. One of FinCEN’s strategic goals emphasizes the agencies desire to provide technology systems for the analysis and collection of financial data. FinCEN also provides the function of advanced research and analysis in the realm of financial investigations for law enforcement agencies (FinCEN, 2014).

Numerous companies have emerged with advanced technologies to trace bitcoin transactions through the public ledger system of the bitcoin blockchain. The software offered in the private sector allows tracing of bitcoin transactions back to the originating wallets. The information compiled is further compared to intelligence driven datasets to identify end users of bitcoins. The technology is also capable of removing anonymity of transactions through the continued use of bitcoin tumbling services (Padilla, 2016; Redman, 2016a; Young, 2016).

Limitations of the Study

Bitcoin and digital currencies are rapidly evolving fields of study in the same manner as any technology driven ideology. As such, new methods of money laundering through digital currency are also evolving rapidly. The offerings of services and exchanges for bitcoins, such as purse.io and uquid.com, both offer new and innovative ways for users to exchange bitcoins.
anonymously. New methods continue to emerge due to gaps in regulations and laws concerning digital currencies (DHS, 2014; FATF, 2015).

In the same manner, case law available for review relevant to digital currencies is limited in 2016 since few cases have been successfully prosecuted involving digital currency. Appellate court and Supreme Court venues have not tried cases involving digital currency. Furthermore, the possibility remains for higher courts to overturn the lower level court decisions and correlating case law. Until finalization of case decisions at the higher levels of the U.S. court system, the definitions and guidance regarding digital currencies remain open for interpretation by regulatory agencies.

Statistical data regarding the number of investigations specifically dealing with digital currencies or the dark web is not readily available. Additionally, a comparative analysis of financial forensics training or computer crime based training offered to law enforcement was not available. Quantifying the number of law enforcement investigators equipped to investigate digital currency or dark web related cases was not achievable in this study with the research used for the case study.

This study was also limited in the scope of current plans for combating digital currency by FinCEN other than published guidance by the agency. Other plans for legislation or regulations forthcoming in the U.S. was not located by the research conducted. All theories in the research pointed this case study towards the improvement of current regulations, policy, and investigations regarding digital currency.

**Summary**

The research demonstrated a need for clear guidance and regulations for the improved enforcement and regulation of digital currency and bitcoin. In order to address the threat of
digital currency, a succinct definition of how digital currency fits into the financial system is necessary. An enforceable legislation is essential for bitcoins and digital currency in order to successfully combat money laundering through digital currency (Ajello, 2015; Kleiman, 2013; Mandjee, 2015).

The regulations and tools available to law enforcement lag behind advancements in technology. Centralized entities, such as FinCEN, are necessary to assist with technologically advanced investigations. FinCEN, as the FIU within the U.S., is tasked with developing tools to thwart financial crime and collecting data concerning suspected illicit uses of financial instruments. Investigative agencies need to address the specific needs of technologically advanced crimes and budget accordingly for the allocations of manpower and resources for these types of cases (DHS, 2014).

**Recommendations and Conclusion**

The Discussion of Findings presented the current shortcomings and disparity between U.S. policy, regulator guidance, regulations, and statutes addressing money laundering as a crime. Analysis of the varied determinations on bitcoin definitions produced differing results. Proposed changes for law enforcement investigations provided some clarity to enhancing investigators methods of enforcement in bitcoin cases.

The research demonstrated digital currencies pose a valid money laundering threat within the United States. Bitcoin is currently exploited on the dark web in the context of illicit commerce. Moreover, bitcoin and other digital currencies can exploit BSA regulations that exist to prevent money laundering (Ajello, 2015; DHS, 2014; FATF, 2015; Mandjee, 2015).

Acceptance and use of digital currency has increased exponentially since the development and implementation of bitcoin in 2008. Although daily bitcoin transaction values
only equal $143 million USD as of October 2016, these values have steadily increased since 2008 (“Output value,” 2016). Since January 2015, the daily U.S. transaction value has increased by nearly $100 million USD (“Estimated USD,” 2016).

As the U.S. government struggles to define and regulate digital currency, case law has offered a direction for the definition of digital currency within current regulatory guidelines. Digital currency aligns within some constructs of federal law; however, a need exists for new legislation specific to digital currency. In addition, digital currency needs a concise definition with regard to how it fits within federal regulations (Ajello, 2015; Kleiman, 2013; Mandjee, 2015).

The research demonstrated traditional law enforcement methods are inadequate for addressing the threats posed by digital currency. A great number of law enforcement agencies lack training and resources to address digital currency threats. Moreover, the investigation of financial crimes and technology related crimes are problematic for many law enforcement agencies (DHS, 2014; Tropina, 2016). A need exists for FinCEN to expand investigative efforts in the realm of digital currency. Law enforcement investigations in areas concerning digital currency could benefit from FinCEN assistance. FinCEN also has the capabilities in place for data warehousing information collected pertaining to digital currency money laundering gathered from BSA data (FinCEN, 2014).

**New Entity Definition**

In order to address new digital currency legislation, there is a need for a new definition for entities acting as an MSB for digital currency (DHS, 2014; FATF, 2015; Kleiman, 2015; Lo, 2015; Mandjee, 2015; Meredith & Tu, 2015; Tropina, 2016). The author proposes a new designation for the entities, which delineates them from MSBs as a *Digital Currency Business*
(DCB). This designation would designate digital currency exchangers as a separate business and eliminate the applicability of the MSB designation under 18 U.S.C. § 1960. A designation of a DCB must include subjects or businesses that conduct any of the following transactions: (1) transmit digital currencies; (2) buy and sell digital currencies for a profit; (3) perform tumbling transactions with digital currency; or (4) engage in property exchange transactions in a manner similar to a currency exchanger. This new designation provides needed clarity with digital currency transactors yet maintains recommendations of treating exchangers in the same manner as an MSB (DHS, 2014; FATF, 2015; Hyman, 2015; Kirby, 2014; Kiviat; Lo, 2016; Mandjee, 2015; Meredith & Tu, 2015; Singh, 2015).

Any entity deemed as a DCB must follow all BSA recordkeeping, KYC, and AML requirements prescribed under the USA PATRIOT Act. DCBs would be required to file the same FinCEN reports required of MSBs along with ensuring AML and KYC compliance. DCBs would also need to register with FinCEN and renew the registration every two years. DCBs should also register with each state requiring registration of MSBs until individual states enact similar DCB designations or registration. These recommendations also mirror requirements of MSBs but delineate the prescribed actions of a DCB (Hyman, 2015; Kirby, 2014; Kiviat; Lo, 2016; Mandjee, 2015; Meredith & Tu, 2015; Singh, 2015).

This author proposes the definition of DCB activity correlate with the Bitlicense legislation. Bitlicense defines virtual currency business activity as: (a) subjects or entities receiving virtual currency for transmission or transmitting it; (b) holding virtual currencies for others in a storage capacity; (c) acting as a business engaged in buying or selling virtual currency; (d) engaging in exchange services as a business; and (e) controlling, administering, or issuing virtual currency. Since the activities denoted in Bitlicense are very specific, they do not
allow for areas susceptible to misinterpretation regarding license requirements (Hughes, 2014; “New York,” 2015). The DCB adaptation should include the designation of digital currency business activity.

**New Legislation**

Research in this study noted the primary money laundering threat with bitcoins lies with unregulated P2P exchanges (Ajello, 2015; DHS, 2014; Mandjee, 2015). New legislation, specific to the threat of unlicensed P2P exchanges, could mitigate illicit finance through the medium of digital currency. Researchers noted a need for specific legislation to regulate P2P exchanges to control digital currency money laundering threats (Kiviat, 2015; Mandjee, 2015; Meredith & Tu, 2015; Singh, 2015; Small, 2015). The researchers also noted the best way to alleviate money laundering through digital currency involved targeting unlicensed exchangers of digital currency (DHS, 2014; Kirby, 2014; Levin et al., 2015; Mandjee, 2015; Meredith & Tu, 2015).

New legislation specific to digital currency is imperative for clarity amongst regulators and law enforcement investigators. A law specific to digital currency with provisions similar to 18 U.S.C. § 1960 and New York’s Bitlicense legislation would provide a solution (Mandjee, 2015; Meredith & Tu, 2015). The proposed digital currency specific legislation should address and enhance all key points of 18 U.S.C. § 1960 and Bitlicense including: (a) requiring all DCBs to register with FinCEN in the same manner as an MSB; (b) require any foreign DCBs conducting business with U.S. customers to follow domestic DCB regulations; and (c) require DCBs to follow registration requirements of individual state MSB requirements if a similar DCB provision does not exist in the state (DHS, 2014; FATF, 2015; Hyman, 2015; Kirby, 2014; Kiviat; Lo, 2016; Mandjee, 2015; Meredith & Tu, 2015; Singh, 2015). A need also exists for sentence enhancements for entities violating the DCB regulation for the purposes of illicit
activity including money laundering and terrorist finance (Kirby, 2014; Kleiman, 2015; Tsukerman, 2015).

**Reporting Requirements**

For consistency, the recommended DCB reporting requirements would match MSB reporting requirements of the BSA. A demonstrated need for new FinCEN reports specific to DCBs to assist with tracking illicit digital currency activity also exists. To align with a proposed new entity definition and regulations for DCBs, reporting requirements should also mirror MSB requirements (Hyman, 2015; Kirby, 2014; Kiviat, 2015; Lo, 2016; Mandjee, 2015; Meredith & Tu, 2015; Singh, 2015). This author proposes the following new reports pertaining to DCB activity:

- Suspicious Activity Report (SAR)
- Currency Transaction Report (CTR)
- Reports for the international transportation of currency or monetary instruments (CMIR)

**Suspicious activity report.** Currently, MSBs have an industry specific SAR designated as a SAR-MSB (FinCEN, 2009). The creation of a SAR-DCB would denote digital currency involvement in the suspicious activity. The new designation would be consistent with previous SAR reports and assist with analytical review of SAR data specific to digital currency.

**Currency transaction report.** Under current regulations, MSBs are required to file CTR reports for cash transactions exceeding $10,000 USD (FinCEN, 2009). DCBs will be required to file CTR reports in the same manner as MSBs. An additional field in the current CTR form would benefit in the delineation between fiat currency and digital currency. In this manner, the CTRs will be searchable specific to DCB activity.
Report for the international transportation of currency or monetary instruments. In the same method described for the CTR, specific field designations in CMIR reports are necessary for research needs of digital currency related CMIR forms. Since digital currency poses a threat of overseas illicit finance, this designation is imperative. Additionally, the CMIR designator will assist investigators in money laundering cases and terrorist financing investigations.

Definition of Digital Currency

In the need for clarity with digital currency, Congress should determine a designation and concrete definition. Multiple researchers noted that the U.S. did not clearly define digital currency (Griffiths, 2015; Mandjee, 2015; Prentis, 2015; Sonderegger, 2015; Tsukerman, 2015). The best term to encompass all previous definitions would be Digital Currency. The definition should include: virtual currency, digital currency, cryptocurrency, and convertible cryptocurrency. These terms represent most forms of digital currency, which store and transfer a value digitally.

Federal law only acknowledges fiat currency, which is issued, and recognized, by governments to fit the definition of a currency. Regulators must determine how digital currency fits within existing laws and regulations (Ajello, 2015; Kleiman, 2013; Mandjee, 2015). Additionally, digital currency needs to be considered a store of value, which is easily spent and converted to fiat currency (Kiviat, 2015). Prior case law in U.S. v. Faiella and U.S. v. Murgio further illustrate the commonality of digital currency to fiat currency (U.S. v. Faiella, 2014; U.S v. Murgio, 2016). As such, a digital currency definition should not align with property, commodity money, or as a commodity (Griffiths, 2015; Mandjee, 2015).
**FinCEN Actions**

FinCEN continues to proactively work with law enforcement investigators pursuing financial crimes. FinCEN also houses all collected BSA data pertaining to potential money laundering case leads (FinCEN, 2014). As such, FinCEN would be the optimum agency to house data collected on suspected illicit DCB activity.

Given FinCEN’s purview with financial crimes, they are in a unique position to assist law enforcement with digital currency investigations. Multiple private sector companies are developing blockchain exploration tools to trace bitcoin transactions (Padilla, 2016; Redman, 2016b; Young, 2016). It is necessary for FinCEN to collaborate with a provider of a blockchain exploration tool and share the collected data with federal, state, and local law enforcement entities. FinCEN could introduce a blockchain exploration tool and a digital currency investigative solution in a similar manner to how FinCEN allows agencies access to reports collected pursuant to the BSA (DHS, 2014).

**Future Research**

Digital currency, akin to technology, continues to evolve on a daily basis. As new digital currencies develop, designers exploit areas to avoid law enforcement intervention in conjunction with illicit finance. One currency, Monero, was cited for having a built-in tumbling technology (Torpey, 2016; Wirdum, 2016). Analysis of emerging digital currencies could benefit development of legislation, definitions, and regulations.

The project did not examine the laundering methods within licensed MSBs. A potential exists for laundering digital currency within a licensed MSB where users may exchange different types of digital currencies to layer the currency (e.g. bitcoin and Monero). The research conducted did not provide any definitive sources on this proposition.
Case law defining bitcoins as money, such as U.S. v. Faiella and U.S. v. Murgio, have yet to be reviewed by appellate courts. These rulings, and future rulings pertaining to digital currency must be reviewed and analyzed for any changes in judicial opinions regarding digital currency. Future court rulings may change the conclusions reached in this project.

**Conclusion**

One of the main principles explored in this project involved the use of bitcoins and digital currency for money laundering and illicit finance. As demonstrated, bitcoins are exploited as vehicles to launder funds. Digital currency is a rapidly evolving field, which exceeds the definitions and policies of currency as defined by legislators, regulators, and investigators.

Bitcoins and digital currency have a potential for beneficial use outside of illicit finance; however, methodologies to curtail the money laundering potential of digital currencies is necessary. Implementation of new legislation and a clear definition regarding digital currency could manage the current exploitation of bitcoins. A concise definition of digital currency in conjunction with new legislation would remove ambiguity and assist investigators.

Emerging technology for blockchain analysis is crucial for investigations involving digital currency. Implementation of a FinCEN hosted blockchain analysis tool for all U.S. law enforcement partners will assist in curbing digital currency use for illicit finance. Additionally, FinCEN can provide skilled analysts to assist law enforcement investigations for digital currency cases.
References


55


## Appendix A - Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AML</td>
<td>Anti-Money Laundering</td>
</tr>
<tr>
<td>ATM</td>
<td>Automated Teller Machine</td>
</tr>
<tr>
<td>BSA</td>
<td>Bank Secrecy Act</td>
</tr>
<tr>
<td>CDD</td>
<td>Currency Transaction Report</td>
</tr>
<tr>
<td>CEA</td>
<td>Commodity Exchange Act</td>
</tr>
<tr>
<td>CFR</td>
<td>Code of Federal Regulations</td>
</tr>
<tr>
<td>CFTC</td>
<td>The U.S. Commodity Futures Trading Commission</td>
</tr>
<tr>
<td>CMIR</td>
<td>Report of International Transportation of Currency or Monetary Instruments</td>
</tr>
<tr>
<td>CTR</td>
<td>Currency Transaction Report</td>
</tr>
<tr>
<td>DCB</td>
<td>Digital Currency Business</td>
</tr>
<tr>
<td>DHS</td>
<td>Department of Homeland Security</td>
</tr>
<tr>
<td>FATF</td>
<td>Financial Action Task Force</td>
</tr>
<tr>
<td>FDIC</td>
<td>Financial Crimes Enforcement Network</td>
</tr>
<tr>
<td>FinCEN</td>
<td>Financial Crimes Enforcement Network</td>
</tr>
<tr>
<td>FIU</td>
<td>Financial Intelligence Unit</td>
</tr>
<tr>
<td>HSI</td>
<td>Homeland Security Investigations</td>
</tr>
<tr>
<td>ICE</td>
<td>Immigration and Customs Enforcement</td>
</tr>
<tr>
<td>IMF</td>
<td>International Monetary Fund</td>
</tr>
<tr>
<td>IRS</td>
<td>Internal Revenue Service</td>
</tr>
<tr>
<td>IRS-CI</td>
<td>Internal Revenue Service - Criminal Investigations</td>
</tr>
<tr>
<td>KYC</td>
<td>Know Your Customer</td>
</tr>
<tr>
<td>MSB</td>
<td>Money Service Business</td>
</tr>
<tr>
<td>PII</td>
<td>Personally Identifiable Information</td>
</tr>
<tr>
<td>PIN</td>
<td>Personal Identification Number</td>
</tr>
<tr>
<td>P2P</td>
<td>Peer to Peer</td>
</tr>
<tr>
<td>SAR</td>
<td>Suspicious Activity Report</td>
</tr>
<tr>
<td>SUA</td>
<td>United States</td>
</tr>
<tr>
<td>TOR</td>
<td>The Onion Router</td>
</tr>
<tr>
<td>U.S.</td>
<td>United States</td>
</tr>
<tr>
<td>USA PATRIOT Act</td>
<td>Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001</td>
</tr>
</tbody>
</table>
Appendix B – Bitcoin Transactions

Number of bitcoins transacted daily between October 2015 and September 2016 (“Estimated transaction,” 2016).

Total number of bitcoins transacted daily between October 2015 and September 2016 ("Output value," 2016).

USD value of daily bitcoin transactions between January 2009 and September 2016 ("Estimated USD," 2016)
Appendix C – Bitcoin transactions explained

Visualization of the bitcoin transaction process (Palacio, B., Peck, M., Romero, J., 2013).