VIRTUAL CURRENCIES AND THE IMPLICATIONS FOR U.S. ANTI-MONEY LAUNDERING REGULATIONS

by

Berkley A. Pamplin

A Capstone Project Submitted to the Faculty of

Utica College

August 2014

in Partial Fulfillment of the Requirements for the Degree of

Master of Science in
Economic Crime Management

ProQuest LLC.
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106 - 1346

Abstract

There is a general understanding in the financial and regulatory environment that virtual currencies pose a challenge for monitoring and combating money laundering. However, there is uncertainty of the exact threats that virtual currencies poses to U.S. anti-money laundering regulations. The purpose of this study is to examine the evolution of virtual currencies, clarify the threats that virtual currencies pose to U.S. anti-money laundering regulations, and determine if it is possible for the U.S. Government to regulate and monitor the use of virtual currencies to deter economic crime.

The methods of research for this study include a literature review of scholarly articles, case studies, statistical analysis, and Internet research from reputable sources. The results of this study will show that the primary reasons virtual currencies pose a threat to U.S. anti-money laundering regulations is due to the anonymity and decentralization of its structure. Any recent attempts at regulating these transactions have been met by the development of third party software that aids criminal organizations in circumventing new regulations. Unless there is a unified effort from world governments to understand how the currencies operate, understand the threats that they create, and to implement new and unique regulations specific to virtual currencies, then virtual currencies will remain the preferred decentralized payment method of most criminal organizations.

Keywords: Economic Crime Management, Capstone Project, Professor Raymond Philo, Crypto-currency, Bitcoin

Acknowledgments

Aristotle once said, “The roots of education are bitter, but the fruit is sweet.” I must agree with Aristotle because while earning my degree over the last six semesters, there were many times that I’ve had to miss events that were important to family and friends. I would like to extend my gratitude to all family and friends who were understanding and supportive throughout my educational journey. There were many difficult times while completing this program but with the support of family and friends I pressed forward and achieved a level of education that I never imagined. Thank you Mom, Dad, Crystal, Jason, Ryan, Jared, professor and mentor Gary Reynolds, consulting subject matter expert for this project Jared Graham, and my fellow classmates of Utica College Economic Crime Management’s Cohort 29.

Table of Contents

List of Illustrative Materials

Statement of the Problem

Evolution of U.S. Anti-Money Laundering Regulations

The act of camouflaging proceeds of illicit activity to make the source appear legitimate has been observed as long ago as 443A.D., when usury became a crime in the Roman Empire (Uribe, 2003). Roman Usury is the act of lending money at rates greater than allowed by the Roman Twelve Tables[1]. Lenders who committed usury would need to conceal the profits of the illicit interest to avoid punishment. This practice of disguising "dirty money" and integrating it into the legitimate financial system in now referred to as money laundering. However, this act was not labeled money laundering until the early 20th century when the tax evasion trial of the famous organized crime virtuoso Alphonse Capone pushed the practice into the lime light.

Capone was a mobster of the early 1920's who was infamous for importing alcohol that was illegally distilled during the prohibition in the United States, a practice known as bootlegging. It is estimated that Capone generated $100 million per year in the prime of his bootlegging, gambling, and prostitution operation (Gane-Mccalla, 2011). To integrate his illicit proceeds into the legitimate financial system Capone purchased several business fronts, many of them being Laundromats, which allowed him to mix his illicit proceeds with the legitimate revenue of the businesses and disguise the source of his income (International Bar Association, n.d.). Capone's technique led to many of the modern day money laundering methods and also the name, money laundering. During the time of Capone's criminal organization in the 20th century, the act of money laundering itself was not a crime, so Capone was ultimately convicted of tax evasion and sentenced to an 11-year prison term.

[1] "The Roman Twelve Tables were the Roman's earliest attempts at creating a code of law (Adams, 2009)." They were the earliest documented Roman laws composed by two separate commissions of 10-12 men.

The conviction of Capone backfired on regulators and law enforcement as it made criminal organization determined to better conceal their proceeds from illicit activity. Meyer Lansky was another infamous mob boss who developed methods of using banks in countries where financial regulation was almost non-existent to create shell companies, shell banks, and operate casinos to launder the funds from his crime family's operations. Lansky also operated several casinos, both legitimate and illegitimate in New York, Florida, New Orleans, Las Vegas, and Cuba. After the conviction of Capone, Lansky was one of the first to use offshore accounts like the numbered Swiss bank accounts, and banks in in Hong Kong, Israel, Switzerland, and various South American countries to move illicit funds out of the United States and into Europe to avoid tax prosecution (Madinger, 2011, p12). Lansky's methods of using shell companies and the financial systems of countries with minimal financial regulation are still used by modern criminal organizations. Since the days of Capone and Lansky, a constant evolution of the crimes being committed to generate illicit proceeds and the evolution of technology used to facilitate these crimes beckoned the need for legislation in the United States that would create standards and tools enabling law enforcement to track money movement in attempts to combat illicit activity.

In 1970, The United States Congress passed the Bank Secrecy Act (BSA), which was the first regulation directed towards controlling money-laundering activity. Although the BSA did not establish the act of money laundering as a crime it did mandate record keeping, record retention, and reporting standards for the financial industry that enabled law enforcement and regulators to identify the source, volume, and movement of currency through financial institutions within the United States (Financial Crime Enforcement Network (FinCEN), n.d.). The record keeping and reporting requirements that the BSA mandated include Currency

Transaction Reports (CTR) that require financial institutions to report cash transactions involving an amount over $10,000. It requires that the person conducting the transaction is properly identified, and requires specific retention of financial transaction records (FinCEN, n.d.). The BSA defines a financial institution in the United States very broadly to prevent many loopholes that criminal organizations may use to avoid these reporting requirements. Financial institutions as defined by the BSA include, but are not limited to (Federal Financial Institutions Examination Council (FFIEC), n.d.[a]):

- Depositor Banks both retail and commercial
- Agencies or branches of a foreign bank operating in the United States
- Credit unions
- Brokers or dealers registered with the Securities and Exchange Commission
- Investment companies
- Operators of credit card systems
- Insurance companies
- Dealers in precious metals, stones, or jewels, including pawn brokers
- Loan or finance companies
- A licensed sender of money or any other person who engages as a business in the transmission of funds, including any person who engages as a business in an informal money transfer system or any network of people who engage as a business in facilitating the transfer of money domestically or internationally outside of the conventional financial institutions system. Also known as a Money Service Business (MSB)
- Casinos
- Dealers of transportation such as automobiles, aircrafts, and boats

The definition was intentionally broad in attempts to include all methods that criminal organizations may use to launder their proceeds. As crime continued to evolve from the bootlegging, prostitution, and gambling of the 1920's-1950's a new era of drug smuggling entered the United States from the 1960's to present day. The peak of the 20th century drug smuggling was in the 1980's. It wasn't uncommon for criminal drug smuggling organization like the Colombian Medellin Drug Cartel headed by Pablo Escobar to earn up to $60 million per day (Miller-Llana, 2010). With such large amounts of cash revenue, money laundering was a necessity for these criminal organizations. The drug era of the 1980's led the U.S. Congress to pass the Money Laundering Control Act of 1986 (MLCA). The MLCA first established the act of money laundering as a federal crime, prohibited the structuring of cash transactions to avoid CTRs filing requirements, and required banks to establish and maintain procedures to monitor compliance with the BSA requirements (FinCEN, n.d.). The MLCA enabled law enforcement to pursue individuals and organizations because they have engaged in a financial transaction that involves proceeds from "specified unlawful activities." Establishing the act of money laundering as a crime enabled law enforcement to disassemble financial support networks of criminal organizations like the Medellin Drug Cartel.

As the 1980's gave way to the Internet and information age of the 1990's the exchange of information was becoming lighting fast and these Internet networks were creating a new global economy. New computer crimes emerged like hacking and large-scale theft of personal identity information. Hackers in Russia and China were able to defraud individuals in different countries while staying in the comfort of their home country. The Internet age brought a new level of security and anonymity to criminals.

Congress attempted to keep up with this evolving technology by passing the Annunzio-Wylie Anti-Money Laundering Act of 1992 (AWAML). The AWAML mandated the filing of Suspicious Activity Reports (SAR), which are filed to FinCEN, an agency of the U.S. Department of the Treasury, to document suspicious financial activity when the activity meets established reporting thresholds. AWAML also mandated identification verification of individuals conducting wire transactions and established record retention requirements for all wire transfers in the United States. The U.S. Congress also passed the Money Laundering Suppression Act of 1998 (MLSA). The MLSA requires MSBs to be registered by the owner or controlling person and also requires MSBs to maintain a list of businesses that are authorized to act as agents in connection with the financial services offered by the MSB (FinCEN, n.d.). The MLSA also made it a federal crime to operate an unlicensed MSB in the United States.

At the turn of the 21st century the United States was the world leader in its efforts to prevent money laundering and combat economic crime. U.S. anti-money laundering regulations were entering new territories and setting an example for other nations. However, in 2001, an event happened that changed the nation in many ways. The Al-Qaeda terrorist attacks on the World Trade Center on September 11th 2001, exposed loopholes in financial regulations that needed to be closed to reduce and track terrorism financing. By October 25th 2001, The USA PATRIOT Act passed the Senate by a vote of, 98 yes to 1 no, and on October 26th the bill was signed into law (The United States Senate, 2001).

The USA PATRIOT Act changed financial regulations in many ways, but those most important to this study include (FinCEN, n.d.):

- Criminalized the financing of terrorism

- Strengthened the customer identification requirement for financial institutions by requiring a documented customer identification and verification program (CIP).
- Prohibited financial institutions from transacting with foreign shell banks (banks that only exist on paper)
- Required financial institutions to have customer due diligence (CDD), and enhanced due diligence (EDD) procedures
- Increased civil and criminal penalties for money laundering

From the time the USA PATRIOT Act was passed in 2001, up to April 2010, law enforcement has prevented 30 terrorist attacks (Carafano, McNiell, & Zuckerman, 2010). However, it is not clear how many of the 30 can be directly attributed to the anti-money launder provisions of the USA PATRIOT Act. One thing is certain of the USA PARTRIOT Act in relation to money laundering; it helped make the tools of U.S. law enforcement and prosecutors the strongest they have been since money laundering became a crime in 1986.

An Emerging Threat to U.S. Anti-Money Laundering Regulations

All U.S. anti-money laundering regulations have been developed around centralized fiat currency, regulated financial industries, and traditional means of moving money. The Internet has provided means to invent new methods of money transfer and new sources of currency. Virtual worlds that are designed to be worldwide-networked simulations of the physical world have created their own economies and their own currency. Centralized virtual currencies such as the Liberty Reserve have created an anonymous method to move large volumes of financial value while bypassing the requirements of U.S. anti-money laundering regulations. A new form of decentralized virtual currency called Bitcoin has created a peer-to-peer money transfer system that is not controlled by any authority but relies on a network of mathematical problem solvers to complete transactions and generate a public ledger system[2]. This mathematical based virtual currency has become known as crypto-currency. Bitcoin has recently become the center of media attention because of its potential to facilitate money transfers using a method never seen. John McAfee, the creator of the computer anti-virus program, McAfee, states about Bitcoin, "It will be everywhere, and the world will have to readjust. World Governments will have to readjust." Peter Theil, the co-founder of PayPal opined of Bitcoin, "I do think Bitcoin is the first [encrypted money] that has the potential to do something like change the world."

The problem this study will evaluate is whether or not these new forms of virtual currencies present a threat to US anti-money laundering regulation. Virtual Currencies like Bitcoin, the Linden Dollar, and the now defunct Liberty Reserve do not require authentication of customer's identity to establish an account, which allows the users to remain anonymous, and makes the transactions more difficult to trace back to an originator. Many financial experts believe that virtual currencies do present a major threat to money laundering regulation. "Unsurprisingly, the crypto-currency is an instant hit on the Darknet, its anonymity making a perfect tool for money laundering and criminal activity (McCormick, 2013)." This research will attempt to address the following questions:

- Does virtual currency present a threat to anti-money laundering regulation in the United States?
- How are virtual currencies being integrated into current U.S. anti-money laundering regulations?
- Are there any conflicting regulations?

[2] For a more in-depth understanding of the Bitcoin architecture, please visit this URL for an illustrative flow chart that explains each step and how the encryption process works. http://wordlesstech.com/wp-content/uploads/2013/05/How-a-Bitcoin-transaction-Works.jpg

- Is money laundering through virtual currency feasible?
- Are criminals already using virtual currencies to launder money?

Justification of the Problem

The amount of press and discussion that Bitcoin has received in the last two years has made a once unknown virtual currency the most well-known and commonly used virtual currency since its creation in 2008. Bitcoin may be the most well-known, but many other virtual currencies exist that are hardly known at all. The website coinmarketcap.com lists the market capitalization and price of 329 different virtual crypto-currencies currently in circulation including Bitcoin, Litecoin, NXT, Darkcoin, Peercoin, Ripple, Potcoin, Silkcoin, and many more (coinmarketcap.com, 2014). All of these lesser-known virtual currencies operate on the same decentralized peer-to-peer network that is secured by cryptographic architecture and mathematical proofs that was invented by the Bitcoin creator or creators, Satoshi Nakamoto. If Bitcoin is proven to be a threat to U.S. anti-money laundering regulations then all 329 of these new crypto-type virtual currencies will pose the same threat, and the user base is growing.

Since mid-2013, the number of existing Bitcoin wallets has increased eight times from under 1 million to over 5 million wallets (Rizzo, 2014). As of June 14, 2014 there are approximately 12.9 million Bitcoins in circulation with a price of $575 per coin, and a market capitalization of over $7 billion (coinmarketcap.com, 2014). In the 24-hour period ending June 14th 2014 at 19:00 pacific time, there were 53,500 transfers, consisting of 72,926 Bitcoins equivalent to approximately $41 million (blockchain.info, 2014). These statistics indicate the growing global interest and exposure to virtual currencies.

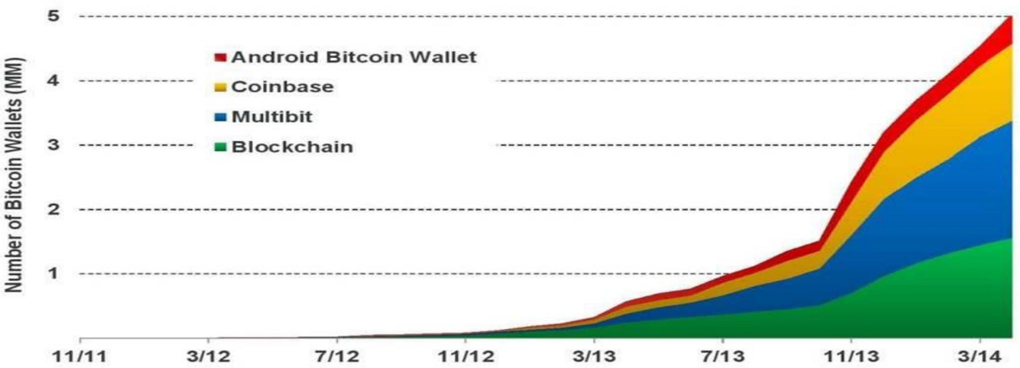

Table 1. Number of Bitcoin Wallets by Wallet Provider (Rizzo, 2014).

This growing interest and use of virtual currencies require an in-depth study and discussion into the potential threats that the virtual currencies present if they are used for nefarious purposes. Research and discussions must educate the U.S. Legislators so they can attempt to regulate virtual currencies within the best interest of the nation to combat these threats. "Economic crime and money laundering are occurring in many virtual worlds and to prevent them would have a positive impact… (Chambers, 2012)."

Current Deficiencies in Research

This study will show that virtual currency money laundering is a reality. In the literature review section of this paper, Liberty Reserve and the Silk Road will be discussed, which are two well-documented cases of virtual currency money laundering. One primary deficiency in current research is the discussion of how the current regulations for virtual currency interact with one another and the possibilities that they may conflict. Another deficiency is the lack of empirical and statistical data of the amount of money laundering that occurs through virtual currencies. Although, the anonymous nature of virtual currencies will make collecting statistical data difficult.

Purpose and Methods of Research

The purpose of this research is to evaluate the characteristics of virtual currency that present a threat to U.S. anti-money laundering regulations. The methods of research will include case studies and literature reviews of peer-reviewed scholarly articles, journal articles, and news articles from reputable news agencies. This project will also draw a conclusion of the threats presented to U.S. anti-money laundering regulations and will make recommendations on how the U.S. Government can strengthen regulation to reduce the use of virtual currencies for illicit purposes.

Literature Review

Defining Money Laundering

The Association of Certified Anti-Money Laundering Specialists define money laundering as taking criminal proceeds and disguising their illegal source in anticipation of ultimately using the criminal proceeds to perform legal and illegal activities. The process of money laundering involves three steps: placement, layering, and integration (FinCEN, n.d.).

Placement. The placement of funds refers to illegitimate funds being deposited into the legitimate banking system. The BSA established a requirement for financial institutions to file a report for any cash transactions over $10,000 to help identify and monitor placement, called a CTR. The BSA also set standards of identification required for the individual conducting the cash transaction. The USA PATRIOT Act of 2001 strengthened the BSA framework by enhancing the identification requirements for the customers of all financial institutions through the Know Your Customer (KYC) program. The KYC program is a combination of the two USA PATRIOT Act requirements of a CIP, and a CDD program. CIP as described above is a written customer identification program required of all financial institutions that establishes the minimum identification required to establish an account and how the customer's identity will be authenticated. CDD is a risk based approach to monitoring a customer's relationship by their financial institution (FFIEC, n.d.[b]). CDD intends to determine if the activity of an account is consistent with the customer's stated purpose of use for their account. These requirements of the BSA and USA PATRIOT ACT are designed to identify and monitor for the placement of illicit funds into financial institutions.

Layering. Layering is described as taking the illicit funds that have been placed into a financial institution and moving them around using several different accounts and transaction types. The objective of the layering process is to move the illicit money through many transactions to obfuscate the source of the funds, the placement of the funds into the legitimate financial system, the trail of the money movement, and the destination or integration of the funds. Layering is the "washing" portion of the laundering. The BSA established record keeping and retention requirements to create a paper trail of all the transactions in attempts to monitor and track the layering transactions.

Integration. After the layering process the money will appear as though it came from a legitimate source or will appear "clean" and the criminal organizations will integrate the laundered funds into the economy. The laundered funds will then be used for legitimate purposes or they will be used to continue the organizations criminal activity. With the source of the funds being disguised criminals can use the funds to purchase real estate, vehicles, businesses, or transfer the funds to other countries. Prior to 2001, not all financial institutions were required to have anti-money laundering programs. The USA PATRIOT Act expanded the requirement to all financial institutions, as defined above, to ensure all methods that criminal are using to integrate funds will be monitoring customer transactions to identify and report suspicious activity.

Case Studies of Money Laundering Through Virtual Currencies

The Silk Road (Bitcoin). The Silk Road was created to be an online peer-to-peer market place that anyone could access using the TOR network[3] and anonymously purchase any type or quantity of illegal drug. The only acceptable payment method in the Silk Road was the virtual currency Bitcoin. In the article, *How the Feds Took Down the Silk Road Drug Wonderland,* author Kim Zetter discusses how the Silk Road operated and how the FBI was able to locate the creator of the site and shut down the market place. In February 2011, the Silk Road launched on the TOR anonymizing network. The online market place was designed to be an anonymous e-store where "international sales of illicit drugs and other contraband were conducted with impunity and with the ease of buying cocktail stirrers or underwear on Amazon (Zetter, 2013)." The various types of contraband that Zetter states could be found on the Silk Road include all forms of illicit drugs, stolen credit and debit card numbers, fake IDs, counterfeit currencies, hacking tools and login credentials for hacked online accounts.

Approximately six months after the launch of the Silk Road, The Department of Homeland Security received an anonymous tip of the existence of the online market place (Zetter, 2013). A multi-agency task force was formed to investigate and shut down the Silk Road. The investigators knew that they were not going to be able to track down buyers and sellers by tracing the flow of the Bitcoin transactions because of the anonymity of the transactions. Instead investigators used the pseudonyms of the site's discussion forum and the interception of products being sent through the U.S. postal service to expose the identities of the users.

[3] TOR is run by a system of volunteers and is designed to bounce users' and websites' traffic through relays making the traffic extremely hard for anyone to identify the source of the information or location of the user (Dredge, 2013)

The task force was able to identify the sites creator “Dread Pirate Roberts” as Ross Ulbricht who was based in San Francisco, CA. However, the ability of investigators to identify Ulbricht was again, not the result of following a trail of transactions, or identifying an IP address. Law enforcement identified Ulbricht by a series of careless missteps by the creator. These missteps led to the arrests of large merchants and administrators of the Silk Road (Zetter, 2013). Other mistakes made by Ulbricht were simple, like Ulbricht using an obvious Gmail account on an online forum discussing the Silk Road that traced back to Ulbricht possibly being the creator.

Ulbricht was arrested in October 2013, and indicted in a federal court for narcotics trafficking conspiracy, continuing criminal enterprise, computer hacking conspiracy, and money laundering conspiracy (USA v. Ulbricht, 2014). The indictment states that “the defendant (Ulbricht), knowing that some of the property involved in certain financial transactions represented the proceeds of some form of unlawful activity, would and did conduct and attempt to conduct such financial transactions … with the intent to promote the carrying on of such specified unlawful activity” and therefore Ulbricht was charged with money laundering conspiracy (USA v. Ulbricht, 2014).

Bitcoin transactions were designed to be completely anonymous, but the result of the Silk Road investigation raises the question, can virtual currency users be identified and can the Bitcoin system be regulated? Investigators were able to perform forensic analysis of the Silk Road servers to identify a $2.9 million account held by Dwolla, a subsidiary of the world’s largest Bitcoin exchange, Mt.Gox, and two Wells Fargo accounts holding $2.1 million that were used by the administrators of the Silk Road (Zetter, 2013). Even though investigators located $5 million in fiat currency in the Dwolla account and the Wells Fargo account, another $28.5

million was discovered in a Bitcoin wallet tide back to Ulbricht, and investigators are not certain that all of Bitcoins owned by Ulbricht were contained in this one wallet (Greenberg, 2013b).

Liberty Reserve. Richard Webber, Head of the IRS Criminal Investigation Division, stated about Liberty Reserve, "If Al Capone were alive today, this is how he would be hiding his money (Perlroth, Rashbaum, and Santora, 2013)." Liberty Reserve is similar to Bitcoin because it is a virtual currency that is used as a means to convert fiat currency and transfer that currency between accounts and the virtual currency can then be converted back into a fiat currency. The primary difference between Liberty Reserve and Bitcoin is that Liberty Reserve was a centralized form of virtual currency meaning there was a central authority controlling its operation. Having a central authority is what lead to the downfall of the Liberty Reserve financial system.

In the article, *Online Currency Exchange Accused of Laundering $6 Billion,* New York Times authors Perlroth, Rashbaum, and Santora discuss how Liberty Reserve was founded, how the service operated, and why it was appealing to criminal organizations. Liberty Reserve was founded and incorporated in Costa Rica in 2006 by Arthur Budovsky who was an American citizen until 2011, when he renounced his citizenship. By operating in Costa Rica it allowed Liberty Reserve to avoid the rigorous U.S. anti-money laundering regulations.

According to the authors, Liberty Reserve did not accept cash or exchange its virtual currency to distribute cash, but instead worked with third party exchangers that were typically unlicensed MSBs based in Malaysia, Russia, Nigeria and Vietnam where there was little government oversight. The exchangers would accept or make cash payments by directly crediting and debiting their customer's Liberty Reserve account. Liberty Reserve was simply the online based system that provided means of transferring the Liberty Reserve virtual currency between Liberty Reserve accounts. The chart below provides a graphical representation of the Liberty Reserve architecture.

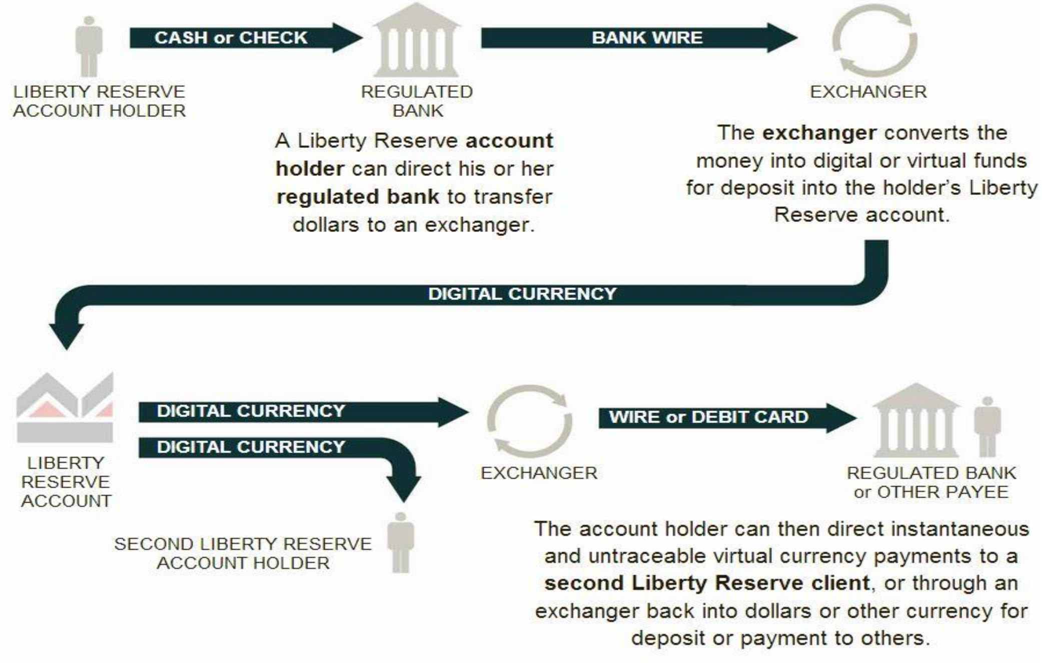
CASH or CHECK
BANK WIRE
LIBERTY RESERVE ACCOUNT HOLDER
REGULATED BANK
EXCHANGER
A Liberty Reserve **account holder** can direct his or her **regulated bank** to transfer dollars to an exchanger.
The **exchanger** converts the money into digital or virtual funds for deposit into the holder's Liberty Reserve account.
DIGITAL CURRENCY
LIBERTY RESERVE ACCOUNT
DIGITAL CURRENCY
DIGITAL CURRENCY
EXCHANGER
WIRE or DEBIT CARD
REGULATED BANK or OTHER PAYEE
SECOND LIBERTY RESERVE ACCOUNT HOLDER
The account holder can then direct instantaneous and untraceable virtual currency payments to a **second Liberty Reserve client**, or through an exchanger back into dollars or other currency for deposit or payment to others.

Figure 1. How Liberty Reserve's Currency Works (FinCEN, 2013b).

Liberty Reserve's currency system had traits that were desirable to criminal organizations. The first desirable trait of Liberty Reserve was anonymity. To establish an account, a customer only needed to provide a name, address, and date of birth, but there was no identity verification processes on behalf of Liberty Reserve to authenticate the identity of its customers. According to the authors, an undercover agent was able to open an account using a name like Joe Bogus and described the purpose of the account as "for cocaine" but Liberty Reserve never questioned this. The second trait that was desirable to criminal organizations was accessibility. Liberty Reserve customers were able to access their accounts online and authorize transactions within minutes. The authors described Liberty Reserve as a system "where money bounces between accounts from Cyprus to New York in the blink of an eye."

It was the USA PATRIOT Act that ultimately led to the demise of Liberty Reserve. In 2013, the founder and administrators were indicted in a U.S. Federal Court for conspiracy to commit money laundering, conspiracy to operate unlicensed money transmitting business, and operation of an unlicensed money transmitting business, which were made illegal by the MLSA and USA PATRIOT Act (USA v. Liberty Reserve, 2013). During Liberty Reserve's time of operation, $6 billion was laundered through the site that catered to criminals trafficking illegal drugs, stolen identities, child pornography, and many more forms of illicit activity (Perlorth, Rashbaum, Santora, 2013). The Liberty Reserve indictment has been cited as the largest money laundering indictment in the history of the United States.

Money Laundering Through Decentralized Virtual Currencies

Bitcoin is the most common decentralized virtual currency, which combines cryptography and a peer-to-peer architecture to avoid a central authority (Zetter, 2012). Bitcoin was the first crypto-type virtual currency created and is also the most commonly used. Bitcoin wallet exchange services like Blockchain.info, fastestcoins.com, bitstamp.net, coinbase.com, and cryptsy.com make using Bitcoins very easy for the average computer user. A wallet is created that represents the users Bitcoin address, also known as a public key. The owner of the wallet can exchange funds from their bank account into Bitcoin or exchange cash directly into Bitcoin by using a Bitcoin ATM, which are now available in many locations around the world (Wile, 2013).

Strengths of Decentralized Virtual Currencies. In the article, *FBI Fears Bitcoin's Popularity With Criminals,* author Kim Zetter analyzes a report that was leaked by the FBI in May of 2012, that expresses the FBI's growing concern of criminals using Bitcoin to move funds and the challenges it presents. The FBI sees the "Bitcoin payment network as an alarming heaven for money laundering and other criminal activity (Zetter, 2012)." The FBI's report focuses on how the anonymity of the Bitcoin system will create major challenges in locating the perpetrator of illegal activity.

Although less sophisticated users may be located by law enforcement through the IP addresses associated with a Bitcoin transfer, advanced users can implement techniques that will make their transactions untraceable. The leaked FBI report, which was marked as sensitive and not intended for public distribution, lists several ways that criminals can make their transactions untraceable (Zetter, 2012):

- Create and use a new Bitcoin address for each incoming payment.
- Route all Bitcoin traffic through an IP address anonymizer.
- Combine balances of old Bitcoin addresses into a new address to make new payments.
- Use specialized third party money laundering wallet service.
- Use a third party wallet to combine several addresses into one wallet.

Criminals may use these techniques in combination with establishing physical bank accounts in countries where financial regulation is minimal, creating an opportunity to move large amounts of money undetected and untraceable. A new product called Dark Wallet has bundled many of the anonymizing techniques listed above into a user-friendly money laundering system that can be operated by users of any skill level.

Dark Wallet. In the article, *Dark Wallet is About to Make Bitcoin Money Laundering Easier Than Ever*, author Andy Greenberg introduces the new Bitcoin wallet management system that was designed specifically to make Bitcoin transactions for illicit goods and services completely untraceable to law enforcement. The first version of Dark Wallet was released on May 1st, 2014 by a group of anarchist computer coders called unSystem (Greenberg, 2014a).

Dark Wallet is designed to eliminate law enforcement's ability to trace transactions through Bitcoin's public ledger called the blockchain. This is achieved by taking multiple users' transactions that are scheduled to occur at the same time so that when the transaction is recorded on the Bitcoin public ledger, the blockchain, it will give the transaction the appearance of only one Bitcoin addresses sending Bitcoins and one Bitcoin address receiving Bitcoins. In reality there may be several transactions involved. The process effectively erases any traceability in transactions. When a Bitcoin transaction occurs outside of Dark Wallet the blockchain will contain a linear record of "address a" sending Bitcoins to "address b". The developers Amir Taaki and Cody Wilson state about Dark Wallet, "when a coin passes through either a CoinJoin transaction or a stealth address, it becomes vastly more difficult to track, making taxation, regulation, and prosecution virtually impossible." The stealth address feature of Dark Wallet allows users to receive bitcoins to an encrypted bitcoin address that only the intended recipient can retrieve by using a private key. However the encrypted Bitcoin address that first received the transfer has not direct link to the intended recipient. It can be thought of as an anonymous P.O. box for bitcoins. The stealth address is another feature of the Dark Wallet that increases the anonymity of its users. All of these features are easily accessible through a graphical user interface that requires about the same computer skills as those needed to browse the Internet. The figure below shows the design of the user interface.

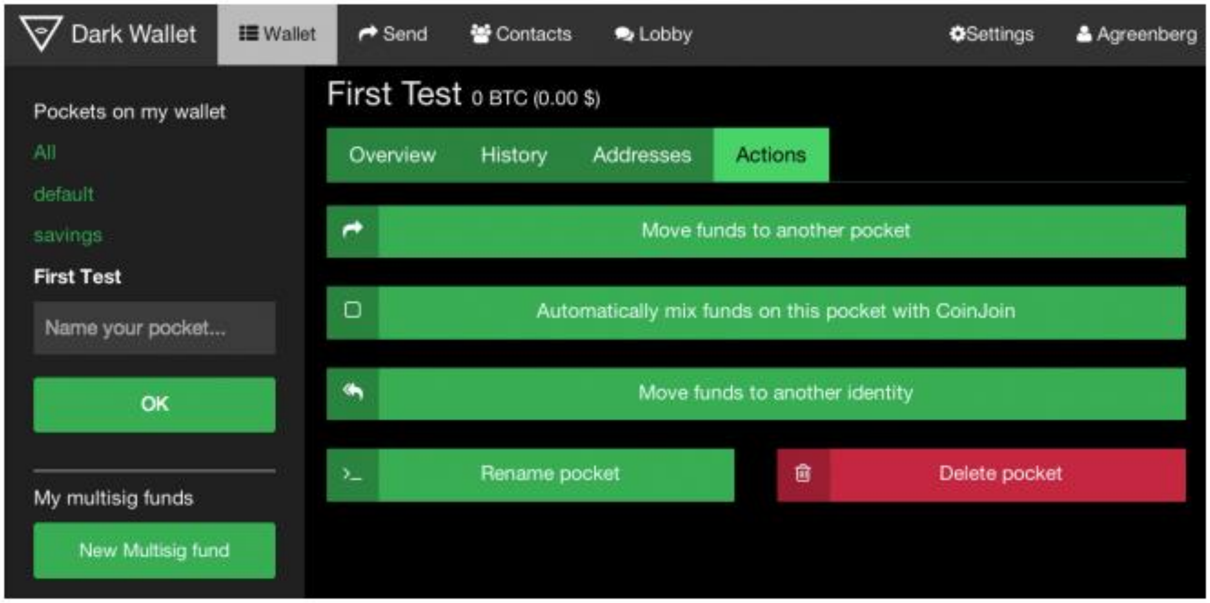

Figure 2. The Dark Wallet User Interface (Greenberg, 2014a).

The Darknet. The Darknet is defined as any network that operates clandestinely and hides the identity of its users (PC Magazine, n.d.). In the article, *Waiting for Dark: Inside Two Anarchists' Quest for Untraceable Money,* Wired Magazine author Andy Greenberg interviews anarchists and libertarians, Amir Taaki and Cody Wilson, about their quest to release the Dark Wallet and the "Dark Market". The Dark Market is a decentralized peer-to-peer online market place that will offer any product or service without limitation. There will not be a central server necessary for this market to operate, which will make it vastly more difficult for law enforcement to seize. Greenberg states that "snooping cops would have to collar users one-by-one to take down the market. The market will be similar to that of the Silk Road but will offer much more security to its users than the Silk Road. A study that was released by the nonprofit, Digital Citizens Alliance, revealed that over 40,000 mostly illegal products are now being sold through various online illicit markets that are hosted on the Darknet, which is more than twice as many as before the Silk Road's existence (Greenberg, 2014b).

The Darknet his home to more than online black markets like the Silk Road or the developing Dark Market. Computer hackers use the Darknet to fund their operations and sell their virus software that allows other hackers to breach secured networks. In the FBI intelligence assessment, *Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity,* the FBI's Directorate of Intelligence discusses the Bitcoin activity that has been identified on the Darknet:

- In October 2011, a cyber-criminal selling a powerful virus called ZeuS Botnet Trojan advised purchasers that the only method of payment accepted is Bitcoin, Liberty Reserve, or WebMoney.
- In June 2011, it was confirmed that the online market place Silk Road would only accept Bitcoin for payments.
- In June 2011, the FBI confirmed that a member of the hactivist group LulzSec was using Bitcoin to purchase a botnet. Although the FBI identified the activity, the identity of the hacker remained anonymous due to the precautions taken by the Bitcoin user.
- In June 2011, the hactivist group LulzSec reported that it had received over $18,000 in donations from supporters through Bitcoin.

The activity identified by the FBI in their article written in 2012 provides more examples of how Bitcoin is being used to launder money.

Limitations of Decentralized Virtual Currencies. In the article, *Virtual Money Laundering: The Case of Bitcoin and the Linden Dollar*, author Robert Stokes analyzes both the risk and draw of laundering funds using the Linden Dollar and Bitcoins. In the previous sections it was discussed how money laundering is possible by using virtual currencies like Bitcoin. Stokes makes the argument that although virtual currencies make a very attractive money-laundering platform due to the anonymity, decentralized nature, lack of face-to-face interaction, and ability to move funds across international borders without relying on heavily regulated financial institutions, it is still not the ideal opportunity for large volume money laundering. His argument is based on the low availability of funds and volatile fluctuations in the Bitcoin value. In March of 2012, when Stokes wrote the article there were 8.6 million Bitcoins in existence that were valued at just over $39 million. Stokes states, "If criminals were to suddenly employ BTC (Bitcoin) as a core money laundering mechanism it would be readily revealed through exchange rate fluctuations since this market is volatile." Now as of June 14th, 2014 there are approximately 12.9 million Bitcoins in circulation with a price of $575 per coin, and a market capitalization of over $7 billion (coinmarketcap.com). Counter to Stokes' argument, Bitcoin is beginning to reveal the value fluctuation that Stokes is referring to. The table below shows the variation in Bitcoin value since the first transaction in January 2009, through July 2014.

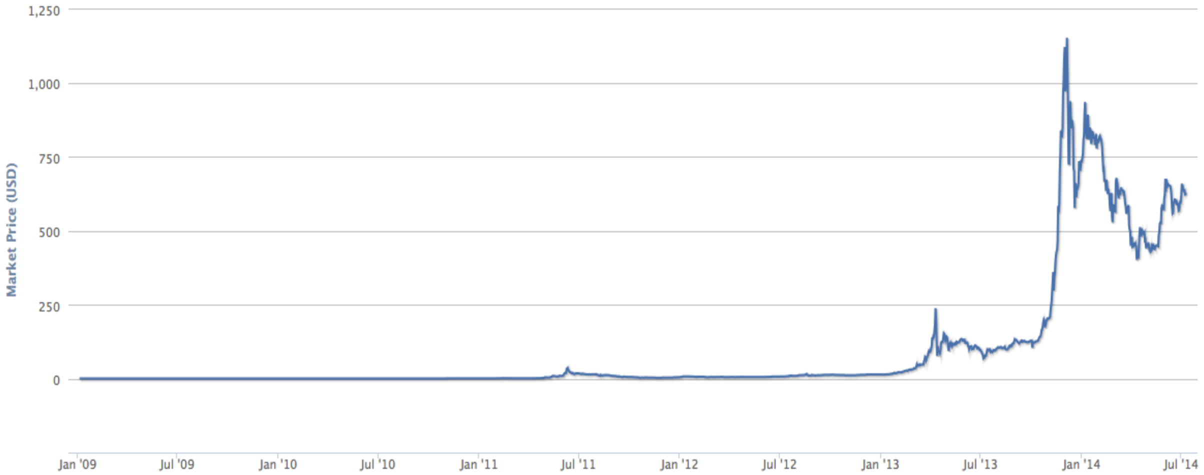

Table 2. Market Price of Bitcoin in U.S. Dollars (Blockchain.info, 2014).

Stokes' second argument for limitations of virtual currency money laundering is that as of 2012, Bitcoin was not widely accepted as direct payment for goods, which eliminates may typologies of money laundering. However, in 2014, there are over 70,000 merchants accepting

Bitcoin as payment (coindesk.com). One of the merchants now accepting Bitcoin as payment is the popular online variety store Overstock.com. By Overstock.com accepting Bitcoins they will allow criminals to anonymously buy high-value jewelry, technology products, clothing, and more high value items that have commonly been used by money launders as a method to integrate illicit funds. Bitcoin has recently become so commonly accepted by merchants that Richard Branson's commercial space flight venture is now accepting Bitcoins for payment (Belevdere, 2013).

In 2014, decentralized virtual currency has evolved tremendously and criminal organizations are latching on to Bitcoin as their primary payment method, which is demonstrated by examples like the Silk Road and new products like the Dark Wallet. As the criminals and hackers see the potential to freely move money through Bitcoin, they are working diligently to make the desirable traits of Bitcoin stronger.

The Feasibility of Money Laundering Through Virtual Currencies

In the article, *Money Laundering and Terrorism Financing in Virtual Environments: A Feasibility Study,* authors Angela S.M. Irwin, Jill Slay, and Kim-Kwang Raymond Choo analyze the suitability of virtual environments for conducting money laundering. The authors found that virtual currencies like Bitcoin and the Linden Dollar can be used to launder money and supply terrorism finance because of the high levels of anonymity, low levels of detection, and the reduction of risk associated with laundering through centralized and legitimate financial institutions.

The authors explain how a variety of virtual money laundering scenarios started to appear in online virtual economies such as Second Life and Entropia Universe. These virtual economies were created as a result of massively-multiplayer online games (MMOGs) that allow players to exchange fiat currency for the game's own virtual currency, which can be used to purchase various features within the game. As the potential for money laundering became known to the creators of these virtual worlds the risks were reduced significantly by introducing new terms of service and in the case of Entropia, the creator registered as a real-world bank, which subjected the virtual world to the corresponding anti-money laundering regulations. However, in the case of Bitcoins the closure of these loopholes is not possible because a central authority does not control the crypto-type virtual currency.

The authors tested the feasibility of money laundering through MMOGs and it was found that it is possible, though very complex. One method involved buying visa prepaid cards, using the cards to purchase MMOG virtual currencies using hundreds of player accounts, reselling the virtual currency to other users, and using an MSB in a foreign country to transfer funds to an account at a legitimate and regulated financial institution. The need for multiple player accounts is to compensate for transaction limits and avoid raising red flags to the game administrators due to high transaction volume and little game interaction. This money laundering method is time consuming, requires significant effort from multiple third parties, and may present red flags to the central authority of the virtual world. This same method was reevaluated as a means to transfer funds to finance terrorism. The study found that the most feasible form of money laundering through MMOGs is the funding of terrorism because there is a lesser amount of funds needing to be moved and the transactions happen less frequently than compared to the money laundering of a large-scale criminal organization.

Current U.S. Virtual Currency Regulations

FinCEN. On March 18th 2013, FinCEN released guidance FIN-2013-G001 that explains the application of FinCEN's regulations for those administering, exchanging, or using virtual currencies. In the article, *For Bitcoin, Square Peg Meets Round Hole Under the Law,* author Peter Henning analyses several prosecution scenarios and determines if the applicable laws will cover Bitcoin activity. Henning analyzes the definition of financial transaction and financial institution as described by 18 US Code § 1956 Laundering of Monetary Instruments. The statute describes a financial transaction as involving monetary instruments coin or currency of the United States or of any other country (Henning, 2013). This definition would not apply to Bitcoin as the currency is decentralized and not backed by any country. Financial Institution is described in the statute as banks, brokerage firms, and MSBs that transmit money. Bitcoin is not a bank or a brokerage firm, however, the FinCEN guide does stated that Bitcoin exchanges or administrators are now classified as a MSB and are subject to the U.S. anti-money laundering regulations. The guide states:

> The Financial Crimes Enforcement Network is issuing this interpretive guidance to clarify the applicability of the regulations implementing the Bank Secrecy Act ("BSA") to persons creating, obtaining, distributing, exchanging, accepting, or transmitting virtual currencies. Such persons are referred to in this guidance as "users," "administrators," and "exchangers," all as defined below. A user of virtual currency is **not** an MSB under FinCEN's regulations and therefore is not subject to MSB registration, reporting, and recordkeeping regulations. However, an administrator or exchanger is an MSB under FinCEN's regulations, specifically, a money transmitter, unless a limitation to or exemption from the definition applies to the person. An administrator or exchanger is not a provider or seller of prepaid access, or a dealer in foreign exchange, under FinCEN's regulations (FinCEN, 2013a).

The FinCEN guide's definitive classification makes it very easy to identify those who are subject to the regulations of the BSA. Under this guidance, Bitcoin administrators and exchangers are required to report transactions that will include the identity of the Bitcoin user (Henning, 2013). Those that mine Bitcoins to eventually sell them or are the administrator of a trading venue will qualify as a financial institution (Henning, 2013).

FinCEN's guide is an expansion of definitions to include certain users of virtual currencies but there are still loopholes that can be exploited. If those using Bitcoin for nefarious purposes want to avoid being subject to U.S. anti-money laundering regulations they can establish an exchange or administer the exchange in a country where financial regulations are minimal. If the users of Bitcoin want to avoid the strict identification requirements of Bitcoin exchangers in the U.S. they can also use exchangers or wallet services in countries with minimal financial regulation. Once the fiat currency is converted to Bitcoin, the user is free to transfer the funds without worry of being monitored for suspicious activity as is required by the BSA and USA PATRIOT Act. Until these loopholes can be closed, Bitcoin will remain an enticing option for money launderers and criminals.

Internal Revenue Service. On March 25, 2014 the U.S. Internal Revenue Service (IRS) issued notice 2014-21 as guidance on how the IRS will apply tax law to virtual currencies and virtual economies. In the article, *A Close Look at the IRS' Bitcoin Guidance,* Law360's author Bryan Smith reviews the IRS notice and how it will affect Bitcoin users and MMOG players that use virtual currencies. According to Smith, there was uncertainty whether the IRS would apply tax principles to virtual currency as property or foreign currency. The notice clarifies that the IRS has adopted the definition of virtual currency based on the FinCEN guidance released in 2013, which stated that virtual currency is a store of value but is not legal tender in any jurisdiction.

Therefore, the IRS will consider and tax virtual currencies as property, similar to stocks and bonds. This classification will subject virtual currencies to capital gains tax, unearned income tax, and ordinary income tax. This will also allow U.S. prosecutors to charge individuals and corporations with tax related crimes if virtual currencies are not properly accounted for and taxed.

The implications are many with this new classification of virtual currency. Bitcoin miners will be subject to taxation if they sell their earned bitcoins to exchangers for a returned value and Bitcoin investors that store value in the currency system will be subject to tax on any increase in value over that of the value of the initial purchase price. Exchangers, who are now required to register as an MSB under the FinCEN guidance, have been advised by the IRS to treat virtual currency as noncapital assets for taxation purposes. The question of whether or not these two guidances released by the two departments within the Department of the Treasury, FinCEN and the IRS, conflict with each other will be addressed during the discussion of the findings section of this paper.

New York State. On July 17, 2014, the State of New York released a proposal for regulations that govern the operation of virtual currency businesses within the state. In the article, *New York Proposes Bitcoin Regulations,* Time.com author Jacob Davidson discusses the effects of the proposal by The New York Department of Financial Services. This proposal would apply to both decentralized and centralized virtual currencies similar to Bitcoin and Liberty Reserve but will not cover virtual currencies used in MMOGs (Gavejian, 2014).

The new rules would require businesses in the state to apply for a license to operate the virtual currency business. The stated issued license has become known as a Bitlicense. This requirement applies to companies that store, control, buy, sell, transfer, or exchange virtual currency. The Superintendent for the N.Y. Department of Financial Services stated, "These regulations include provisions to help safeguard customer assets, protect against cyber hacking, and prevent the abuse of virtual currencies for illegal activity, such as money laundering." Davidson explains that the proposed regulations will expose the virtual currency businesses in the State of New York to similar anti-money laundering requirements as registered MSBs are subject to from the U.S. Federal Government.

Summary of Regulations. The three documented attempts at regulation from FinCEN, the IRS, and the State of New York are the first attempts by U.S. Regulators at legitimizing virtual currency as a method of payment in the U.S. These attempts have expanded the definitions of existing U.S. anti-money laundering regulations to incorporate virtual currencies. While these regulations are new, more time will be necessary to measure their affect on virtual currency money laundering. The sheer magnitude of the money laundering discussed in the case studies above, question whether it is feasible to regulate virtual currencies at all.

Practicality of Regulations Against Virtual Economic Crime

In the article, *Can You Ever Regulate the Virtual World Against Economic Crime;* author Dr. Clare Chambers provides a valid argument about the challenges of regulating virtual currencies. The article is more specific to the virtual in-world currencies of the MMOG's but the arguments can also be applied to all virtual currencies. The two main issues to regulating virtual currencies that Chambers discusses are the legal jurisdiction over the Internet and the anonymity of the virtual currency's owner. The anonymity of virtual currency has been discussed in previous sections but the jurisdiction over the internet is a relevant topic to discuss further.

The internet is the overarching network of individual networks. The network flows freely between states, countries, and contents. This free flow of information and commerce creates an issue for regulating the contents and its users. As Chambers states, it is not that the internet is absent of laws, however, the laws between jurisdictions do not align and are piecemeal. This creates a barrier to the necessary regulation for preventing online economic crime or enforcing regulations. Each country decides to regulate the internet according to their values and moral code.

An example provided by Chambers is, in Germany it is illegal to import, purchase, or distribute items of Nazi relevance. If an individual in the United States is distributing Nazi materials to citizens in Germany via the Internet, does Germany then have jurisdiction to prosecute the American Citizen who has the right to distribute the material established by The Constitution of the United States? There is not a centralized authority over the internet that can establish uniform regulation or uniform enforcement of Internet laws.

Chambers discusses many barriers to regulating virtual economic crime throughout the article but the most important can be summarized within a few questions:

- Who can govern the Internet?
- Who holds the democracy to decide what is right and wrong within the virtual worlds (or virtual currencies)?
- Can you implement laws within the internet and thus virtual worlds?
- How can you impose laws onto a virtual world (or virtual currency) which crosses boarders and jurisdictions?
- Where can people who have committed a wrong in a virtual world be held accountable?

Discussion of Findings

"Cyber-crime is one of the fastest growing areas of crime, as more and more criminals exploit the speech, convenience, and anonymity that modern technologies offer in order to commit a diverse range of crime… Interpol has acknowledged that there is a real threat of financial crime being committed over the Internet (Chambers, 2012).” During the discussion of the evolution of money laundering earlier in this study it became apparent that regulations are passed as a reaction to crime. Regulation will always lag behind the evolution of the crime and the means to commit the crime. As new regulations are passed criminal organizations will evolve rapidly to exploit any remaining loopholes, or develop new methods entirely.

The peer reviewed articles, business articles, and case studies discussed in the literature review show that virtual currencies provide criminal organizations a method to bypass many of the requirements and controls set forth by U.S. anti-money laundering regulations. The three types of virtual currencies discussed, decentralized crypto-currencies, centralized virtual currency, and virtual currencies used in MMOG’s offer different means of moving money. However, the features of these virtual currencies that are a threat to U.S. anti-money laundering regulations can be grouped into two categories, anonymity and decentralization.

Anonymity

As was stated by Feuer while he explained the ideology behind the creation of Bitcoin, the crypto-currency was created by the person or group Satoshi Nakamoto, as a frustrated reaction to the financial crisis that affected the world economy in 2008. Bitcoin was designed to be a method of moving money between two individuals “directly, anonymously, and outside of government control (Feuer, 2013).” The system was designed to only identify users by an alphanumeric serial number to maintain users’ anonymity.

Bitcoin. Anonymity is a major threat to almost all U.S. anti-money laundering regulations. A primary intention of the USA PATRIOT Act was to strengthen the CIPs and require all financial institutions to document and authenticate customer identities. In addition to the identity requirements, the USA PATRIOT Act requires customer due diligence (CDD) and enhanced due diligence (EDD). CDD and EDD require financial institutions to monitor their customer's activity to identify suspicious activity. CIP combined with CDD and EDD have become known as Know Your Customer (KYC). The ability to use Bitcoin is open to anyone with a computer. There is no requirement to provide identification that will be authenticated to establish the customers as a legitimate user. There is also no central authority of Bitcoin that regulators can sanction for not establishing a CIP. In addition to the lack of customer identification, the FBI has identified several methods that criminals can use to mask their transaction activity and make their Bitcoin use more anonymous.

One method identified by the FBI is creating a new Bitcoin wallet address for every transaction. The argument has been made that Bitcoin transactions are not anonymous because all transactions are published on the blockchain, also known as the public ledger. The blockchain is accessible to anyone. The FBI's observation that creating a new address for every transaction will avoid creating a detectable trail that could alert law enforcement to criminal activity within the blockchain. The inability to monitor activity is a direct threat to the CDD and EDD requirements of the USA PATRIOT Act. The FBI also talks about routing Bitcoin traffic through an IP address anonymizer.

Anonymizers will route user's traffic through many servers and change the IP address and location of the user's activity. An IP address is a set of numbers that identify an Internet user. The user's Internet Service Provider (ISP) assigns the IP address, so if law enforcement can identify an IP addresses, they can subpoena the identity and location of that IP address through the ISP. Anonymizers are designed to hide user activity online and will effectively eliminate that risk for criminals. There are also anonymizing programs that were specifically designed for

Bitcoin. The FBI refers to these in their leaked document as specialized money laundering services and third party e-wallets that combine several Bitcoin addresses into one wallet.

The Dark Wallet is one of these third party wallet services that was discussed in the literature review. The Dark Wallet was created by two anarchists, Amir Taaki and Cody Wilson, to be "a piece of software designed to allow untraceable, anonymous online payments using the crypto-currency Bitcoin (Greenburg, 2014b)." The software will eliminate any identifiable trail of transactions between Dark Wallet users. This is done by bundling several transactions into one single transaction and completing the transfer so that anyone monitoring the blockchain will not see individual transactions. They will see one transaction, when in reality that one transaction represents multiple transactions occurring at once. The threat that this poses to U.S. anti-money laundering regulations is again, the inability to follow a money trail and identify illicit funds. If the Dark Wallet would have been available to the buyers and sellers of the Silk Road all transactions would have been unidentifiable by law enforcement. A very powerful statement made by author Andy Greenburg summarizes the intent behind Dark Wallet, and also the threat that it poses to U.S. anti-money laundering regulations:

> "Taaki and Wilson see in Bitcoin's stateless transactions the potential for a new economy that fulfills the crypto-anarchist dream of truly uncontrollable money. They envision a digital payment network that circumvents every authority's attempts to tax it, seize it, censor it, track it, or imprison those who would use it to trade in contraband like weapons, drugs, and even abhorrent services like murder-for-hire and child pornography (Greenburg, 2014b)."

The Dark Wallet is still under development but once it is operational and offered to criminals it will be an effective means of facilitating money movement to aid criminal organization in money laundering.

Liberty Reserve. Liberty reserve was a form of centralized virtual currency that was an obvious threat to U.S. anti-money laundering regulations. There was not one U.S. anti-money laundering regulation followed by Liberty Reserve. As discovered by reading the DOJ's indictment of the corporation and its founders, the service was created to provide criminals with a means to launder money. For customers to establish an account with Liberty Reserve they were only required to provide a name, address, and date of birth. However, Liberty Reserve did not authenticate the identities of it users. Accounts were able to be opened with pseudonyms and false addresses without being questioned (Perlroth, Rashbaum, & Santora, 2013). The central authority over Liberty Reserve did not monitor user activity to identify unusual activity, or gather intelligence as to where the source of the funds were originating.

The reason that Liberty Reserve was such an obvious threat to U.S. anti-money laundering regulations is it lacked a KYC program and it was also operating as an unlicensed MSB. Liberty Reserve did not have CIP established and it did not meet the CDD and EDD requirements of the USA PATRIOT Act. Liberty Reserve was non-compliant with the MLSA which would require the corporation to register in the U.S. as an MSB because although the corporation was located in Costa Rica, Liberty Reserve was holding accounts and conducting transaction for 200,000 American customers. Liberty Reserve was such a threat to U.S. anti-money laundering regulations that the founders of Liberty Reserve were indicted on charges of conspiring to commit money laundering and conspiring to operate an unlicensed money transmitting business (USA v. Liberty Reserve, 2013). The virtual currency provider was shut down by U.S. Federal Authorities in May of 2013. One founder has pled guilty to money laundering and conspiracy charges on October 31, 2013 (Department of Justice, 2013). From Liberty Reserve's creation in 2006, until the time it was shut down in 2013, the virtual currency facilitated 55 million transactions and laundered $6 billion of illicit funds (Cloherty, 2013).

MMOGs. The study of the feasibility of money laundering suggested that money laundering is possible through virtual currencies used in MMOGs. The study was not conclusive as to the volume of money that can be laundered through MMOGs and the study did not provide examples of money laundering cases that have been facilitated through MMOGs. Terms of service and transaction limitations reduce the risk of large scale money laundering through these virtual environments but often, criminal organizations do not need to launder large quantities of cash. Therefore, MMOGs do present a minor threat to U.S. anti-money laundering regulation. The Oklahoma City bombing only cost $4,000 to carry out, the attack on the U.S.S. Cole required only $10,000, and the London subway bombing required only $14,000 (Federal Bureau of Investigations, 2013). Using MMOG's virtual currency to anonymously transfer funds that are intended to finance terrorism is feasible for smaller scale attacks. However, the complexity, the amount of time necessary to transfer the funds, and the fact that MMOGs have a central authority, does significantly reduce the treat that MMOG virtual currencies pose to U.S. anti-money laundering regulations.

Decentralization

Bitcoin. Bitcoin is the only virtual currency of the three discussed in this study that is completely decentralized. Bitcoin is a peer-to-peer network that does not have one central authority that controls or regulates the use of the currency or that can monitor user activity for suspicious behavior. The entire system relies on a network of miners who authenticate the transactions and prevent duplicate spending by solving complex mathematical equations to validate transactions. The decentralization is what creates the greatest barrier to enforcement of U.S. anti-money laundering regulations. The decentralization also increases the threat that Bitcoin poses to U.S. anti-money laundering regulations because law enforcement cannot shut down the currency for violating the regulations, as was done to Liberty Reserve and the Silk Road. The U.S. Department of the Treasury's FinCEN has attempted to control Bitcoin by regulating the exchangers and classifying the exchangers as MSBs.

Cases of Virtual Currency Money Laundering

The Liberty Reserve was a blatant case of money laundering through a virtual currency. The method of Liberty Reserve money laundering was to offer users an account that could be established through an anonymous pseudonym. Another, more relevant case of virtual currency money laundering that was the Silk Road. The Silk Road was an open market for the purchasing and selling of illegal narcotic drugs. The only acceptable form of currency that could be used on the Silk Road was Bitcoin. In the two and a half years that the Silk Road was in operation, the site generated $1.2 Billion in revenue and generated $80 million in commission for its operator (Greenberg, 2013a). The current regulations and guidance that has been offered by financial regulators focuses on the exchangers of virtual currency and the administrators, but they do not address the money laundering activity that does not pass through an exchange or MSB. "A majority of the Bitcoin activity does not occur within the traditional banking system (Henning, 2013)."

Existing Regulations

FinCEN. After FinCEN released its guidance on virtual currencies several types of virtual currency users are now classified as MSBs, which subjects them to the requirements of the BSA, MLCA, AWAML, MLSA, and the USA PATRIOT Act. The definition of MSB has been expanded to include administrators or exchangers of virtual currencies. This will affect many MMOG's that exchange fiat currency for their in-game virtual currency and operates in the United States. Crypto-currencies do not have a centralized administrator or any authoritative body to enforce these requirements upon. Instead the United States Government has been enforcing the requirements upon virtual currency exchange businesses that deal in Bitcoin. In early 2014, the CEO of Bitinstant exchange and wallet service was arrested on money laundering charges because its users had ties to activity on The Silk Road (Pagliery, 2014).

Although virtual currency exchangers and administrators have been identified at MSB's, the virtual currency users are not subject to U.S. anti-money laundering requirements. Therefore the users are able to circumvent the FinCEN guidance by using exchangers and financial institutions located in countries with minimal financial regulation. For the technologically advanced virtual currency users, there are methods to purchase, use, and store the currency without the use of the popular exchange and wallet services that are available online. The wallet source code[4] is open source, which means it is available to anyone on the Internet and can be used to create a wallet that is only available to its creator. An example of a wallet created by the open source code is Coinpunk and it can be viewed at this site: http://coinpunk.org/beta.html.

On March 18, 2013, when FinCEN released guide FIN-2013-G0001 it could be interpreted that the U.S. Department of the Treasury was recognizing Bitcoin as a currency and money transfer system. However, on March 25, 2014, the IRS released its own guidance on how it will apply U.S. tax principles to virtual economies and virtual currencies. The IRS will treat Bitcoin as property, not as a legal tender (Smith, 2014).

[4] Source code is defined as a text listing of commands to be assembled into an executable computer program. It is the blue prints of a computer program. More information is available at http://www.techterms.com/definition/sourcecode

IRS. The IRS has issued its own guidance for investors, miners, exchanges, and users of virtual currency as a method of payment. The guidance applies the U.S. tax principles to virtual currencies in several ways but most importantly "the receipt of virtual currency in exchange for goods or services is payment in property, with the fair market value of the virtual currency included in income on receipt and such value becoming the recipient's tax basis in the virtual currency (Greenberg, Langhirt, & Plewa, 2014)." The meaning is that IRS will treat virtual currencies as property, similar to stocks and securities and will apply capital gains tax, unearned income tax, and ordinary income tax. The fact that the IRS is defining virtual currency as property conflicts with the FinCEN guidance which is regulating virtual currency as money by requiring exchanges to register as an MSB. MSBs are defined as a licensed sender of money, or any person who engages in a business that facilitates the transfer of money domestically or internationally. The IRS's classification of virtual currency as a property also conflicts with the New York State's recent release of its own virtual currency regulations.

New York State Regulation. On July 18, 2014, New York State's financial regulators released a proposal for the first state level regulation of virtual currency. The proposal is seen as very strict and compromising by Bitcoin backers. The regulation is similar to FinCEN's by requiring business that deal in virtual currency to apply for a license to operate. The license, known as a Bitlicense, would require that the business have anti-money laundering programs similar to the CDD and EDD requirements of the USA PATRIOT Act. They would be required to have a CIP that gathers and retains identifying information of its customers and requires Bitcoin businesses to take reasonable steps to validate the identity of its customers. The business must also establish a cyber-security program to protect its consumers from virtual theft and hacking (Alvarez, 2014). The regulations also propose a record retention program requiring the virtual currency businesses to document and retain transaction records for a minimum of ten years.

Reaction to Regulations. There has been a strong reaction to the regulatory guidance and proposals released by U.S. Regulators. The libertarians, hackers, and anarchists who view virtual currencies such as Bitcoin as a means to avoid the imposing regulations of the BSA, MLCA, AWAML, MLSA, and the USA PATRIOT Act are reacting with the creation of the Dark Wallet, the Dark Market, and the Silk Road 2.0[5]. There is still much uncertainty on how U.S. prosecutors will handle cases because of the conflicting guidance of FinCEN and the IRS.

Recommendations and Conclusions

Recommendations

Consolidating Guidance and Proposals. The release of the FinCEN guidance, IRS guidance, and the New York State proposal for regulation on virtual currencies indicates that regulators do recognize the threat virtual currencies poses to U.S. anti-money laundering regulations. For regulations of virtual currency to be successful, it will require decisions and proposals that are consistent, supported by experts, and consistent application of the regulations to all methods of virtual currency use. This study has found that the guidance offered by the U.S. financial regulators has lacked consistency and support. Two administrative departments of the U.S. Department of the Treasury, the IRS and FinCEN, cannot agree if virtual currencies like Bitcoin should be classified as money or property. If they cannot agree, it cannot be possible to apply the regulations consistently.

[5] The Silk Road 2.0 is a new online drug market that has been created as a peer-to-peer system that will be more difficult for law enforcement to cease. Little scholarly information is available because there is still uncertainty around the market and its creation. More information is available at http://www.telegraph.co.uk/news/uknews/crime/11004862/Dark-net-drugs-adverts-double-in-less-than-a-year.html

It is recommended that all regulators come together to discuss how new regulations can be formed specifically for virtual currency money laundering. Existing anti-money laundering regulation can serve as a framework for new regulation dedicated to virtual money laundering but the two cannot merge into one. Author Peter Henning's title of the article, *For Bitcoin, Square Peg Meets Round Hole Under the Law",* suggests that regulators are attempting to force virtual currencies to fit into existing anti-money laundering regulations. Decentralized virtual currency like Bitcoin is the first virtual currency that does not have a central authority to enforce regulations upon. The idea of enforcing U.S. anti-money laundering regulation upon the exchanges, wallet services, and mining network is a temporary solution but it does not seem sustainable in the long term while virtual currencies continue to evolve.

Sentencing Enhancements for the Criminal Use of Virtual Currency. U.S. Regulators and Legislators must explore the option of enhancing penalties of the underlying criminal activity that leads to act of money laundering to deter the nefarious used of virtual currency. Current regulation proposals do not provide a deterrent to the use of virtual currency during the commission of a crime. For example, if Bitcoins are used to purchase a controlled substance, regulators can explore the option of adding an enhanced punishment to the controlled substance charge if Bitcoin was used to facilitate the criminal act. This may be a suitable alternative to directly regulating Bitcoin money laundering. If a criminal knows they could face an additional twenty years in prison for using Bitcoin during a criminal act, they may think twice about using Bitcoin.

Recommendations for Future Research

Virtual currencies are evolving and so are the means to use them while committing a crime. Anarchists like Amir Taaki and Cody Wilson have made it clear in their message to the public that their intention with the creation of the Dark Wallet and the new peer-to-peer Dark Market is to provide a means for absolute free will. The FinCEN guidance does not apply to individual users, therefore, unless users are storing Bitcoin and transacting through a regulated exchange that is subject to the U.S. anti-money laundering regulations, there will be minimal monitoring of individual user activity.

Future research must also consider how traditional money laundering methods such as the formation of shell companies, shell banks, and the establishment of accounts at financial institutions in foreign countries with lax financial regulation will be used in combination with virtual currencies to place illicit proceeds back into the traditional financial system. The possibility of criminal organizations establishing a financial presents in countries like Cypress or Switzerland where financial confidentiality is protected will allow criminal organizations in the U.S. to use virtual currency exchangers that are not subject to U.S. anti-money laundering regulations. As the Darknet, Dark Wallet, and illicit online market places continue to evolve, they must be studied and understood to allow U.S. regulations to evolve with these new means of committing crimes.

Conclusion

In conclusion, the objective of this study was to answer whether or not virtual currencies present a threat to U.S. anti-money laundering regulation, to discuss how virtual currencies are being integrated into current U.S. anti-money laundering regulations, to address if the current attempts to regulate virtual currencies conflict, to address if virtual currency money laundering is feasible, and to determine if criminal organizations are presently using virtual currencies to launder money. This research found that virtual currencies do pose a threat to U.S. anti-money laundering regulations. The greatest threat is Bitcoin because of the 3rd party software available to enhance the anonymity of the users, the lack of a central authority to enforce anti-money laundering regulations, and the growing acceptance of Bitcoin as a direct payment by merchants.

Third party software like Dark Wallet will effectively eliminate the ability to monitor the activity of Bitcoin users. The argument has been made that Bitcoin transactions are not anonymous because the flow of transactions can be monitored through the blockchain, which is a public ledger viewable by everyone online. However, Dark Wallet eliminates that trail by mixing multiple transactions into one entry in the blockchain. The Dark Wallet will intentionally make the CIP, CDD, and EDD requirement of the USA PATRIOT Act impossible to impose as well as the SAR filing requirement of the AWAML.

The second greatest threat to U.S. anti-money laundering regulation is centralized virtual currency like Liberty Reserve. Liberty Reserve was created specifically to facilitate money laundering.

This research determined that MMOGs do present a threat to U.S. anti-money laundering regulations but it was inconclusive as to how much of a threat exists within these virtual economies. Transaction limitations, monitoring of user activity, and the existence of a central authority that can be penalized for lack of oversight has greatly reduced the threat that of large scale money laundering through the virtual economies of MMOGs. As the discussion of the findings suggests, money laundering to fund terrorist attacks that require little financing such as the Oklahoma City bombing and the attack on the USS Cole is feasible through MMOG virtual currencies. Therefore, MMOG virtual currencies do pose a threat to the USA PATRIOT Act. In attempts to mitigate these threats the U.S. Department of the Treasury and the State of New York have issued proposals and guidance information as to how Bitcoin is to be integrated into current anti-money laundering regulations.

FinCEN, The State of New York, and the IRS are attempting to integrate virtual currencies into existing U.S. anti-money laundering regulation in two ways, requiring exchangers and businesses dealing in virtual currency to register as MSBs, or in the IRS' case, classifying virtual currencies as property, which will then be subject to capital gains tax, unearned income tax, and ordinary income tax. The two approaches do seem to conflict in how the U.S. Department of the Treasury is defining virtual currency. Although FinCEN's and the IRS' classification of virtual currencies conflict, their attempts at regulation do not fail to meet the objective of combating money laundering. However, if the U.S. Department of the Treasury desires to regulate virtual currency into a legitimate payment method, consistency in how the laws are applied must be achieved to relieve uncertainty in the market.

As was discussed, the U.S. Department of the Treasury must consolidate and agree upon the classification of virtual currency in order to create consistent application of existing regulations before more money laundering services like Liberty Reserve take advantage of the regulatory uncertainty.

These case studies in this research have determined that money laundering through virtual currency is feasible and is happening although both Liberty Reserve and the Silk Road have been shut down. New online drug markets such as the Silk Road 2.0 and the Dark Market are currently, or will soon be, in operation and the creators are better prepared to prevent a shutdown by learning from how law enforcement shut down the original Silk Road.

Money laundering and the criminal organizations are always evolving. As was recommended by the findings, regulators need to create a completely new regulatory framework specifically for virtual currencies as opposed to integrating the currency into existing regulations. Decentralized virtual currencies such as Bitcoin have created a new regulatory challenge and the focus of the regulation may need to shift from money laundering, to reducing the underlying crime that creates the need to launder the money. Jon Matonis, the executive director of the Bitcoin Foundation, offers this insight that regulators may want to consider, “Every measure is met with a countermeasure. If governments push too hard to control crypto-currencies, more than they do with old-fashioned cash, bitcoiners will turn to more anonymous payment tools or even integrate their features directly into the bitcoin protocol (Greenberg, 2014b).”

References

Adams, J.P. (2009). The Twelve Tables. California State University Northridge. Retrieved from http://www.csun.edu/~hcfll004/12tables.html

Alvarez, E. (2014). New York wants Bitcoin exchanges to be heavily regulated. Engadget. Retrieved from http://www.engadget.com/2014/07/18/new-york-cryptocurrency-regulations/

Association of Certified Anti-Money Laundering Specialists (ACAMS). Risks and methods of money laundering and terrorist financing. ACAMS English Study Guide p13. Retrieved from http://files.acams.org/pdfs/English_Study_Guide/Chapter_2.pdf

Belvedere, M. J. (2013). Richard Branson: Buy your space flight with Bitcoin. CNBC Online. Retrieved from http://www.cnbc.com/id/101220710

Blockchain.info. (2014). Currency stats: Bitcoin currency statistics. Retrieved from https://blockchain.info/stats

Carafano, J. J., McNeill, J. B., & Zuckerman, J. (2010). 30 terrorist plots foiled: How the system worked. The Heritage Foundation. Retrieved from http://www.heritage.org/research/reports/2010/04/30-terrorist-plots-foiled-how-the-system-worked

Chambers, C. (2012). Can you ever regulate the virtual world against economic crime?. Journal of International Commercial Law and Technology. Volume 7 (No. 4) 339 – 349. Retrieved from http://www.jiclt.com/index.php/jiclt/article/view/168/166

Choo, K. K. W., Irwin, A. S. M., & Slay, J. (2014). Money laundering and terrorism financing in virtual environments: A feasibility study. Journal of Money Laundering Control. Volume 17 (No. 1), 50-75.

Cloherty, J. (2013). Black market bank accused of laundering $6B in criminal proceeds. ABC World News. Retrieved from http://abcnews.go.com/US/black-market-bank-accused-laundering-6b-criminal-proceeds/story?id=19275887

Coindesk.com (2014). What can you buy with Bitcoins? Retrieved from http://www.coindesk.com/information/what-can-you-buy-with-bitcoins/

Coinmarketcap.com. (2014). Crypto-currency market capitalizations. Retrieved from https://coinmarketcap.com/index.html

Davidson, J. (2014). New York Proposes Bitcoin Regulations. Time.com. Retrieved from http://time.com/money/3004751/new-york-bitcoin-regulations-benjamin-lawsky/

Department of Justice (2013). Co-founder of Liberty Reserve pleads guilty to money laundering in Manhattan Federal Court. Office of Public Affairs. Retrieved from http://www.justice.gov/opa/pr/2013/October/13-crm-1163.html

Dredge, S. (2013). What is TOR? A beginner's guide to the privacy tool. The Guardian. Retrieved from http://www.theguardian.com/technology/2013/nov/05/tor-beginners-guide-nsa-browser

Federal Bureau of Investigations. (2012). Bitcoin virtual currency: Unique features present distinct challenges for deterring illicit activity. Intelligence Assessment.

Federal Bureau of Investigations. (2013). Terror financing. Tracking the money trails. Retrieved from http://www.fbi.gov/news/stories/2013/july/terror-financing-tracking-the-money-trails/terror-financing-tracking-the-money-trails

Federal Financial Institutions Examination Council. (n.d.[a]). Bank Secrecy Act anti-money laundering examination manual appendix d: Statutory definition of financial institution. Retrieved from https://www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_104.htm

Federal Financial Institutions Examination Council. (n.d.[b]). Bank Secrecy Act anti-money laundering examination manual: Customer due diligence – overview. Retrieved from https://www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_013.htm

Feuer, A.(2013). The Bitcoin ideology. The New York Times. Retrieved from http://www.nytimes.com/2013/12/15/sunday-review/the-bitcoin-ideology.html?pagewanted=all&_r=0

Financial Crimes Enforcement Network. (2013a). Application of FinCEN's regulations to persons administering, exchanging, or using virtual currencies. Retrieved from http://www.fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html

Financial Crimes Enforcement Network. (2013b). Notice of finding that Liberty Reserve S.A. is a financial institution of primary money laundering concern. Retrieved from http://www.fincen.gov/statutes_regs/files/311--LR-NoticeofFinding-Final.pdf

Financial Crimes Enforcement Network. (n.d.) History of anti-money laundering laws. Retrieved from http://www.fincen.gov/news_room/aml_history.html

Gane-McCalla, C. (2011). Top 10 richest gangsters of all time. News One. Retrieved from http://newsone.com/1505845/top-10-richest-gangsters-of-all-time/

Gavejian, J.C. (2014). NY Department of Financial Services proposes virtual currency rule. The National Law Review. Retrieved from http://www.natlawreview.com/article/ny-department-financial-services-proposes-virtual-currency-rule

Greenberg, A. (2013a). End of the Silk Road: FBI says it's busted the web's biggest anonymous drug black market. Forbes Magazine. Retrieved from http://www.forbes.com/sites/andygreenberg/2013/10/02/end-of-the-silk-road-fbi-busts-the-webs-biggest-anonymous-drug-black-market/

Greenberg, A. (2013b). FBI says it's seized $28.5 million in Bitcoins from Ross Ulbricht, alleged owner of silk road. Forbes Magazine. Retrieved from http://www.forbes.com/sites/andygreenberg/2013/10/25/fbi-says-its-seized-20-million-in-bitcoins-from-ross-ulbricht-alleged-owner-of-silk-road/

Greenberg, A. (2014a). Dark wallet is about to make Bitcoin money laundering easier than ever. Wired Magazine Online. Retrieved from http://www.wired.com/2014/04/dark-wallet/

Greenberg, A. (2014b). Waiting for dark: Inside two anarchists' quest for untraceable money. Wired Magazine. Retrieved from http://www.wired.com/2014/07/inside-dark-wallet/

Greenberg, M., Langhirt, J. H., & Plewa, D. (2014). Bitcoin is property, not currency, IRS says – Notice leaves many open questions about convertible virtual currencies. DLA Piper. Retrieved from http://www.dlapiper.com/en-us/us/insights/publications/2014/04/bitcoin-is-property-not-currency/

Henning, P.J. (2013). For Bitcoin, square peg meets round hole under the law. DealBook by the New York Times Online. Retrieved from http://dealbook.nytimes.com/2013/12/09/for-bitcoin-square-peg-meets-round-hole-under-the-law/?_php=true&_type=blogs&_r=1

International Bar Association (n.d.). Money laundering: 1.2 the history of money laundering. Anti-Money Laundering Forum of the International Bar Association. Retrieved from http://www.anti-moneylaundering.org/Money_Laundering.aspx

Madinger, J (2012). Money laundering: A guide for criminal investigators (3rd ed.). Boca Raton, FL: Taylor & Francis Group.

McCormick, T. (2013). The Darknet: A short history. Foreign Policy Magazine. Retrieved from http://www.foreignpolicy.com/articles/2013/12/02/the_darknet?wp_login_redirect=0

Miller-Llana, S. (2010). Medellin, once epicenter of Colombia's drug war, fights to keep the peace. The Christian Science Monitor. Retrieved from http://www.csmonitor.com/World/Americas/2010/1025/Medellin-once-epicenter-of-Colombia-s-drug-war-fights-to-keep-the-peace

Pagliery, J. (2014). Bitcoin exchange CEO arrested for money laundering. CNN Money. Retrieved from http://money.cnn.com/2014/01/27/technology/security/bitcoin-arrest/

PC Magazine. (n.d.) Encyclopedia: Definition of Darknet. PCmag.com. Retrieved from http://www.pcmag.com/encyclopedia/term/40718/darknet

Perlroth, N., Rashbaum, W.K., Santora, M. (2013). Online currency exchange accused of laundering $6 billion. New York Times. Retrieved from http://www.nytimes.com/2013/05/29/nyregion/liberty-reserve-operators-accused-of-money-laundering.html?pagewanted=1&_r=0

Rizzo, P. (2014). Mary Meeker's internet trends report finds 'extraordinary interest' in Bitcoin. Coindesk Online. Retrieved from http://www.coindesk.com/mary-meekers-internet-trends-report-finds-extraordinary-interest-bitcoin/

Smith, B. (2014). A closer look at the IRS' Bitcoin guidance. Law360. Retrieved from http://www.law360.com/articles/524285/a-close-look-at-the-irs-bitcoin-guidance

Stokes, R. (2013). Virtual money laundering: The case of Bitcoin and the Linden Dollar. Information & Communications Technology Law. Volume 21 (No. 3) 221-236.

The United States Senate. (2001). US Senate roll call votes 107th Congress – 1st session: On passage of the bill (H.R. 3162). Retrieved from http://www.senate.gov/legislative/LIS/roll_call_lists/roll_call_vote_cfm.cfm?congress=107&session=1&vote=00313

Uribe, R. (2003). Changing paradigms on money laundering. The Observer News. Inter-American Observatory on Drugs.

USA v. Liberty Reserve S.A., No 13CRIM368 (U.S. District Court Southern District of NY 2013)

USA v. Ross William Ulbricht, No 14CRIM068 (U.S. District Court Southern District of NY February 04, 2014)

Wile, R. (2014). Bitcoin ATM founder: We already have orders from 30+ countries. Business Insider. Retrieved from: http://www.businessinsider.com/cyprus-bitcoin-atm-guy-responds-2013-4

Zetter, K. (2012). FBI fears Bitcoin's popularity with criminals. Wired Magazine. Retrieved from http://www.wired.com/2012/05/fbi-fears-bitcoin/

Zetter, K. (2013). How the feds took down the Silk Road drug wonderland. Wired Magazine. Retrieved from http://www.wired.com/2013/11/silk-road/