Mabunda, S. (2018). Cryptocurrency: The new face of cyber money laundering.
2018 International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD): Durban, South Africa.
http://dx.doi.org/10.1109//ICABCD.2018.8465467

Cryptocurrency: The new face of cyber money laundering

Sagwadi Mabunda

Abstract
Virtual currencies are on the rise and so is money laundering. While there are efforts to combat money laundering through various intergovernmental bodies, many have expressed concern over the rise of virtual currencies. Some cryptocurrencies such as Bitcoin have played a major role in the proliferation of online money laundering as it possesses characteristics that criminals are fond of. Bitcoin and other cryptocurrencies are decentralised, anonymous/pseudonymous and irreversible. They provide the means to skirt the Anti-Money laundering safeguards that have been put in place.

This paper discusses the intersection between Anti-Money Laundering efforts and the challenges that are introduced by cryptocurrencies such as Bitcoin. It also looks at the case of Liberty Reserve to highlight these challenges.

I. Introduction

An old saying goes "for every level there's a new devil" and technology has taken society to a new level where it appears that cybercrime is the new devil that must be contended with. Cybercrime is not merely a virtual manifestation of terrestrial crime, it possesses new characteristics that present new challenges. However, as much as some cybercrimes can operate solely in the virtual environment, some embed themselves in the crevices of already existing crimes. Some terrestrial crimes adopt technological advances and use them to enhance their means. One such example is money laundering and the way that it adopts virtual currencies to ensure more success and even less detection.

Two of the law enforcement interests that were presented to the U.S. Department of Homeland Security and Governmental Affairs were firstly, efforts to deter and prosecute criminals who use virtual currency to move or hide money that has been used in criminal or terrorist financing activities i.e. for the purposes of money laundering; and secondly, to investigate the virtual currency services that themselves violate laws that are aimed at preventing illegal money schemes and money laundering [1].

The U.S Secret Service believes that virtual currencies are preferred by criminals because they offer:

1. The greatest degree of anonymity for both users and transactions.

 smabunda@uwc.ac.za

2. The ability to quickly and confidently move illicit proceeds from one country to another.
3. Low volatility, which results in lower exchange risk, increasing the digital currency's ability to be an efficient means to transmit and store wealth.
4. Widespread adoption in the criminal underground.
5. Trustworthiness [2].

This paper looks at the use of virtual currencies in money laundering. The first section will discuss money laundering, outlining what it is and what are the concerns surrounding it are. The second section will discuss virtual currencies with a focus on the cryptocurrency Bitcoin. That section will highlight one of the biggest challenges to Anti-Money Laundering (AML) efforts which is the anonymity that cryptocurrencies provide. The third section will discuss Liberty Reserve as an example of other virtual currencies (albeit not Bitcoin) in money laundering. That section will highlight the potential that virtual currencies have. Finally, some of the regulations that are in place to deal with money laundering will be discussed in the last section as a proposal for a way forward.

II. Money laundering

Money laundering is the process of concealing proceeds of illicit or illegal activities to obscure the link between the original criminal activity and the illicit funds. Money laundering is often only a secondary act which is preceded by the illegal act i.e. the predicate crime [3].

Money laundering is a serious global concern because it has devastating economic impacts and it is also closely linked to terrorist financing. It undermines the integrity and stability of financial institutions and the economic stability of countries in the way that is distorts international capital flows while also discouraging direct foreign investment [4].

The money laundering model is a three-stage process; *placement, layering* and *integration*. The *placement stage* is where the illicitly gained money is put into a legitimate enterprise like a small business or into real estate to create the initial distance between the money and the predicate offence. In the *layering stage* the money is used in many legal transactions to create more distance between it and the criminal act. This can be in the form of buying and selling equipment for the legitimate small business. The final stage is *integration* where the money is introduced back into the legitimate financial system. This can be done by depositing the proceeds from the sale of equipment or of real estate property into a bank [3]. There is often an overlap between these stages particularly placement and layering.

Traditionally banks and other financial institutions are the preferred vehicles for money laundering but with the growth of virtual currency, laundering money online is gaining popularity [4].

A. Financial Action Task Force (FATF)

There are several international bodies and agencies that are tasked with tackling money laundering. One of the most recognisable groups is the Financial Action Task Force on Money Laundering (FATF). The FATF is an inter-governmental body which was established in 1989 by the International Monetary Fund (IMF). The FATF is a 37-member body which has 35 member countries and 2 regional organisations [5]. It has developed a series of recommendations that are recognised as the international standards that states adhere to in their AML efforts. This also extend to the efforts against terrorist financing and the proliferation of weapons of mass destruction [5].

B. Digital Economy Task Force

The second stakeholder is the Digital Economy Task Force which was created at a conference that was held at the World Bank in 2013. Officials from the European Central Bank, ICMEC, International Monetary Fund, Thomson Reuters, the U.S Federal Reserve, the U.S Department of the Treasury's Office on Terrorism Financing and Financial Crimes were present when this body was created. The purpose of the Task Force is to explore solutions that would be constructive and reasonable which include ways in which to tackle the challenge of anonymity [6]. Anonymity is an important concern when dealing with money laundering through virtual currency because it goes against many of the safeguards in place to prevent cyber laundering.

C. Financial Crimes Enforcement Network (FinCEN)

The third important stakeholder in AML is the U.S. Department of Treasury's Financial Crimes Enforcement Network (FinCEN). FinCEN reports directly to the Office of Terrorism and Financial Intelligence which issues directives, guidelines and regulations that are aimed at combatting money laundering.

FinCEN's mission is three-fold. Firstly, it is to safeguard the financial system from illicit use; secondly, it is to combat money laundering; and lastly it aims to promote national security through the collection, analysis, and dissemination of financial intelligence and strategic use of financial authorities [7]. Additionally, FinCEN administers the Bank Secrecy Act (BSA) which requires that financial institutions have effective AML programs. The BSA was passed in 1970 and it required that money services businesses report all financial transactions of more than $10, 000. This Act has been amended several times since its enactment because of the changing landscape and proliferation of money laundering [3]. The types of financial institutions referred to include banks, insurance companies, securities and futures brokers/dealers, casinos and so forth. Interpretive guidelines were also provided to those individuals and companies that deal with virtual currencies [8]. It is important to note that although there are measures presented to regulate virtual currencies and that the risks associated with them is acknowledged, their risk is mitigated by the fact that virtual currencies are useful and can play an important role in society [6].

FinCEN outlines the responsibilities that financial institutions have such as reporting and record keeping but they also outline that these requirements are reserved for 'money

transmitters' such as virtual currency exchangers but they will not apply to individuals who use virtual currencies for common personal transactions such as buying and selling goods and services online. Whereas, those that operate as intermediaries in the transfer of virtual currency are required to register to FinCEN as money service business [7].

It is without doubt that virtual currencies play a significant role in the advancement of money laundering therefore, it is important to understand them so that suitable responses and safeguards can be explored.

III. Virtual currencies

Recent years have displayed significant increases in the volume of internet transactions which has made providing secure online payments important for global business [6]. This has spurred the growth and rapid adoption of virtual currencies. Virtual currencies first entered the marketplace in the 1990's and they have been the subject of discussion since. The conversations have been accelerated by the growth in popularity of cryptocurrencies that emerged around 2013 [9].

While the U.S Government Accountability Office (GAO) has observed that there is no single and widely accepted legal definition for virtual currency, they describe it as "… a digital unit of exchange that is not backed by a government-issued legal tender. Virtual currencies can be used entirely within a virtual economy, or can be used in lieu of a government-issued currency to purchase goods and services in the real economy" [10]. Furthermore, it is important to note that virtual currency transactions do not merely denote the transferring of fiat currency through digital means such as one does when using a credit card to buy a product online [11].

Bitcoin represent a type of virtual currency called cryptocurrency (cryptographical currency). It is not the only cryptocurrency that is in circulation today, but it is one of the most recognisable. At the time of writing, the second and third best trading cryptocurrencies are Etherium and Ripple respectively where are over 1400 different types of cryptocurrency trading (although not all of them are mineable) [12].

In this paper, Bitcoin will be used as a representative of all cryptocurrency whilst acknowledging that not all cryptocurrencies are created equal. It is also acknowledged that at the time of writing, Bitcoin is facing tumultuous trading numbers and its future is not guaranteed, but the foundations that Bitcoin have been built on are strong enough to assert that if Bitcoin does not survive long term, there will be bigger and better cryptocurrencies that will pick up where it left off. It is therefore important to not discount the role that it and other cryptocurrency play in the money laundering because this is a problem that will not disappear quietly into the night.

IV. Bitcoin

Much has been said Bitcoin, the new cryptocurrency sweeping across nations. It is a cryptocurrency which is based on ideas from B-Money as proposed by Wei Dai in 1998 [13].

Basically, Bitcoin is not a physical coin but rather it is a decentralised cryptographic currency which consists of a chain of signatures that record and provide the transactional history of the bitcoin. It makes use of many individuals called 'miners' who crack complex mathematical algorithms that verify the transactions that each Bitcoin has engaged in. Over time, there is an expansion of the number of Bitcoins in circulation and they have a preannounced limit of twenty-one million which, it is estimated, will be reached in 2040 [9].

Bitcoin uses peer-to-peer networks to distribute a master copy of the public ledger which will have all Bitcoin transactions recorded and verified. This public ledger is referred to as a blockchain and it ensures that transactions are not duplicated nor are they counterfeited. The use of the blockchain means that all transactions are recorded publicly thereby verifying that identical Bitcoins are not used or 'double-spent' [6].

Bitcoin was introduced to the world in 2008 and it has been met with both suspicion and admiration since its introduction in the seminal paper by a person or group called "Satoshi Nakamoto" [14]. In the paper, he, she or they begin by describing the deficiencies of commerce on the internet, noting that commerce has come to rely almost entirely on the participation of financial institutions which play the role of trusted third parties in financial transactions. Nakamoto notes that one of the inherent weaknesses of this system is that it is not possible for there to be completely non-reversible transactions because the costs associated with it are undesirable [14]. The possibility of reversible transactions means that the fraud is ultimately accepted as being unavoidable. The costs that are associated could be mitigated by requiring that payments be made by using physical currency but unfortunately, there are no mechanisms that exist that would allow transactions without the participation of the trusted third parties [14].

Nakamoto proposes that to do away with the need for a third party, an electronic payment system is needed that will be based on cryptographic proof rather than on trust. It would allow any willing parties to transact directly with each other without the involvement of the trusted third party. These transactions would be computationally impossible to reverse, therefore protecting the sellers from fraud. There would also be routine escrow mechanisms that could be implemented to protect buyers as well [14].

These introductory remarks in Nakamoto's paper clearly outlines the intentions with which Bitcoin was created. The primary concern was attaining security for online financial transactions by creating inexpensive non-reversible payments that would reduce or even eliminate the instances of fraud. However, even with the best of intentions, even good inventions can be corrupted to advance more unscrupulous ends.

Dai's intentions when he created B-Money were somewhat different. He envisioned a system that would provide untraceable and pseudonymous entities the ability to exchange and enforce contracts. He wanted a medium which would not need intermediaries in electronic transactions, which would result in government involvement not only being "temporarily destroyed, but permanently forbidden and permanently unnecessary" [13]. The

underground world of cybercrime and online organised crime have brought his vision to life. Cryptocurrencies are used in dark web drug trafficking, sex trafficking, child pornography and a host of other cybercrimes. Bitcoin has been criticised for the active role it has played in online drug markets such as Silk Road.

V. The trouble with anonymity

Since its introduction, Bitcoin has been met with suspicion because it is supposedly anonymous and irreversible. It is also worrying to financial regulators and governments because it is not controlled by any central entity such as a national reserve bank and therefore, its core system is not subject to regulations and enforcement efforts [15].

As stated, Bitcoin is largely thought to be anonymous. Möser et al., argue that it is better to describe Bitcoin as pseudonymous rather than anonymous. They show that obtaining the identities of the transacting parties may not be as easy as when dealing with ordinary financial transactions, it is not impossible [15]. They propose that one of the ways to keep a record of who is transacting with Bitcoin would be requiring them to provide the identity document for example at the terminals where fiat currency is exchanged for Bitcoin and vice versa [15]. This would ensure there is some margin of record keeping and collection of identifying information.

Straightforward Bitcoin transactions may be easier to trace via the endpoint identification but for those that require additional levels of protection from being identified, they can increase their anonymity through Bitcoin mixes. Bitcoin mixes occur at the middle of the transactions so that when one tries to trace the pathways of the Bitcoin transactions, they are obfuscated. An example of an intermediary which provides such a service is "Bitlaundry". Möser et al., find that while some Bitcoin mix intermediaries such as BitLaundry, do not guarantee anonymity, others such as "BitFog" and "Blockchain.info" made it impossible for them to find any direct connections in the transaction graphs [15]. This indicates that some Bitcoin mix intermediaries may be more effective than others, however, whether Bitcoin is regarded as anonymous or pseudonymous, it is important to note that it still poses a greater threat to anti-money laundering efforts than fiat currency or physical property because it provides a greater level of anonymity.

The Liberty Reserve is a brilliant real life example of the difficulties that present with virtual currencies. Although Bitcoin was not the currency used in the money laundering schemes of Liberty Reserve, it is a testament to the fact that even if Bitcoin itself were to lose value and be discontinued today, its capabilities have been broached and the technology can be enhanced to achieve even greater feats.

VI. Liberty reserve

In 2013, a sealed indictment from a grand jury was brought against defendants Liberty Reserve S.A., Arthur Budovsky, Vladimir Kats, Ahmed Yassine Abdelghani, Allan Esteban Hidalgo Jimenez, Azzeddine El Amine, Mark Marmilev, and Maxim Chukharev. The charges against them were (1) conspiracy to commit money laundering conspiracy to

operate (and operating) an unlicensed money transmitting business [16]. The indictment was seeking the forfeiture of the property that was involved in the money laundering conspiracy or the operation of the unlicensed money transmitting business offences.

It has been reported that Liberty Reserve had more than one million users worldwide. It was alleged that approximately $6 billion in funds was laundered in suspected proceeds of crime which include the trafficking of narcotics [17].

Liberty Reserve performed money services in the same way that banks and other financial institutions do but it did not have any of the safeguards that are required of banks and financial institutions. When a customer used the Liberty Reserve services, she would only be required to provide basic identifying information such as her name, address and date of birth. However, unlike traditional banks, Liberty Reserve did not require any supporting documents to verify the legitimacy of the identifying information, such as an official identification document. This meant that accounts could be easily created with fictitious or anonymous identities [17].

Once the user opened an account, she could transact with other Liberty Reserve customers. Liberty Reserve used a digital currency known as LR that the customers could transfer to each other and make purchases to merchants who accepted LR as a currency. Each of these transactions were charged at a one percent fee to Liberty Reserve. Additionally, a user could choose to pay a 75 cent 'privacy fee' on each transaction. This privacy fee would allow the user to hide her own Liberty Reserve account number to make the transaction completely untraceable even within Liberty Reserve's own system [1].

As if that was not enough, Liberty Reserve added an additional level of anonymity by not allowing the users to fund their Liberty Reserves account directly. This means that users were not allowed to make transfers from their credit cards or through a wire transfer and by the same token they were not allowed to withdraw money through an ATM. Liberty Reserve required them to make any deposits or withdrawals through third party 'exchangers'. This allowed Liberty Reserve to avoid collecting any information about their users through banking transactions which meant that there was no centralised paper trail [17]. Liberty Reserve was the antithesis of traditional banking system.

The relationship between Liberty Reserve and its third- party exchangers was the major component to the money laundering scheme. The third-party exchangers were the only ones that maintained a direct relationship with Liberty Reserve and their role in the scheme was to buy and sell LR in bulk and then exchange it for fiat currency. Then the exchangers would buy and sell the LR to the end users in smaller transaction in exchange for the fiat currency. Therefore, for the user to transact with Liberty Reserve she would have to make the payment to the exchanger. The exchanger would then credit her Liberty Reserve account with the corresponding LR amount by transferring LR from the exchanger's Liberty Reserve account into her account [17]. When the user wished to withdraw money, the reverse process would occur.

Furthermore, Liberty Reserve had a list of 'pre-approved' exchangers who were typically unlicensed money transmitting businesses which operated without significant government oversight and were therefore not held to any AML regulatory standards. Most of these exchangers were based in Malaysia, Russia, Nigeria and Vietnam. Given the nature of their services, they charged transaction fees that were higher than conventional banks, typically the fees amounted to five per cent or more of the transactions they facilitated [17].

Anonymity was the cornerstone of Liberty Reserve's business practices. It was designed in such a way that the identities of the users would be hidden under multiple layers of anonymity which would ensure that they are not apprehended by law enforcement agencies. Furthermore, this anonymity meant that the users preferred Liberty Reserve as their primary vehicles for illegal activities where they could routinely activate multiple accounts under false identities, some as brazen as "Russian Hacker" [17].

Liberty Reserve's services were not only limited to providing the platform for criminals to complete financial transactions, it also provided a means for 'merchants' to display a Liberty Reserve 'shopping cart interface' on their website which would enable customers to use Liberty Reserve as a means of payment. This would be like the VISA or MasterCard icons appearing on websites for easy credit card payments. Some of these merchants sold stolen credit cards, some peddled Ponzi schemes and get-rich-quick schemes, computer hackers for hire, underground drug dealing enterprises and so forth [17].

Eventually, the United State Department of Justice apprehended some of the people responsible for running the site and shut it down. One of the defendants entered a guilty plea [6].

VII. Safeguards against money laundering

The first line of defence against money laundering is customer due diligence. Where AML regulations are in place, banks and other financial institutions are required to perform due diligence. This ensures that banks are proactive in the fight against money laundering by monitoring and preventing customers from performing transactions that may be involved in money laundering. This creates accountability for financial institutions and places an additional burden on them because they are liable for prosecution if they do not conform to the regulatory requirements.

Due diligence entails verifying that the customers are legitimate in instances where their transactions involve: (1) transfers from foreign institutions; (2) any transactions that involves currency in an amount that would be greater than an internationally established threshold; (3) any transactions that involves a bank or financial institution that is from a an FATF non-cooperative state; or (4) where there are suspicions about whether or not previous customer information and data is accurate [18].

The first challenge with cryptocurrency relates to not being able to easily tie an identifiable user to a single bitcoin or bitcoin address which would allow enforcers to track the placement, layering and integration of laundered funds. [11]. This was the part that Liberty Reserve understood well. There were broken links between the user's already tenuous identities and Liberty Reserve using their network of exchangers.

The second challenge is that interrupting laundering transactions that occur via Bitcoin is nearly impossible. This is because peer-to-peer transactions and verification through 'miners' means that disabling one bitcoin node will not be sufficient, instead one would have to get rid of every single miner on the network [11]. This would be a hard thing to achieve as miners are incentivised to mine for Bitcoin. For this reason, Liberty Reserve used a network of exchangers so that if one is taken offline, the others could easily take the place of the others. This was also helpful so that the user's transactions and identities are decentralised.

The third big concern with cryptocurrency is the presence of sophisticated encryption which enhances the degree of anonymity. Strong encryption algorithms are important because cryptocurrency does not have central regulatory authorities therefore they are needed to ensure secure transactions. For AML purposes, encrypted cryptocurrency wallets pose serious difficulties when investigating, seizing evidence and forfeiting criminal proceeds [1]. It should be noted that encryption is not synonymous with anonymity. In cases where there are appropriate AML safeguards and adequate know-your-customer (KYC) controls, encryption on its own should not be troublesome.

VIII. Conclusion

Laundering money with cryptocurrency shares a lot of common characteristics with the archetypal money laundering. The process in laundering money is the same and so is the consequences of thereof. It is the properties inherent to the cryptocurrency -the money laundering vehicle - that poses the biggest challenge to regulators [3].

Money Laundering is a deleterious crime that perpetuates the predicate crimes where the laundered money is derived. It creates a vicious cycle where criminals and criminal entities have a constant stream of funds. The invention of virtual currencies has been a double-edged sword. On one hand, it has made it easier to securely transact over the internet but on the other hand it has been exploited to facilitate myriad cybercrimes and assist the criminals to safely launder the proceeds. Bitcoin is an example of a cryptocurrency that has been exploited because of its anonymity, security, irreversibility and decentralisation.

Although Bitcoin is the most recognisable cryptocurrency presently, it is not immune to market volatility. However, this does not mean that if it collapses, the use of cryptocurrency will cease to be used in laundering money. Bitcoin has just shown the opportunities available to criminals and as Liberty Reserve has shown, the possibilities are endless.

[1] M. Raman, Department of Justice, Press Release (Nov. 18, 2013), available at http://www.justice.gov/criminal/pr/speeches/2013/crm- speech-131118.html (accessed 15 January 2018).
[2] Statement of E. W. Lowery III, "Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies: Hearing Before the S. Comm. on Homeland Security & Governmental Affairs" 113th Cong. (Nov. 18, 2013 (citing DEPARTMENT OF FinCEN, guidance fin-2013- g0001, application of fincens's regulations to persons administering, exchanging, or using virtual currencies (Mar. 18, 2013).
[3] N. J. Ajello "Fitting a square peg in a round hole: bitcoin, money laundering, and the fifth amendment privilege against self- incrimination," Brook. L. Rev. 80 15, 2015.
[4] National Drug Intelligence Center, "Money laundering in digital currencies," U.S. Department of Justice, No. 2008-R0709-003, June 2008.
[5] FAFT-GAFI http://www.fatf-gafi.org/ (accessed 20 January 2018). [6] L. Trautman, "Virtual currencies bitcoin and what now after Liberty Reserve, Silk Road and Mt. Gox?" RICH. J.L. & TECH. 20 13, 2014 available at http://jolt.richmond.edu/v20i4/article13.pdf (accessed 15 Jan 2018) p 33.
[7] Statement of J. Shasky Calvery, "Beyond Silk Road: potential risks, threats and promises of virtual currencies," Hearings Before the S. Comm. on Homeland Sec. & Gov't Affairs, 113th Cong. 2013.
[8] FinCEN, "Application of FinCEN's regulations to persons administering, exchanging, or using virtual currencies" Fin-2013-G001, 2013, available at http://www.fincen.gov/statutes_regs/guidance/html/FIN-2013- G001.html (accessed 25 Jan 2018) unpublished.
[9] S.J. Hughes, and S.T. Middlebrook, "Regulating cryptocurrencies in the United States: current issues and future directions," WM. MITCHELL L. REV. 282 40, 2014, p 814.
[10] Department of Justice press release, "Co-Founder of Liberty Reserve Pleads Guilty to Money Laundering in Manhattan Federal Court" GAO- 13-516, Oct. 31, 2013, available at http://www.justice.gov/opa/pr/2013/October/13-crm-1163.html (accessed 12 January 2018).
[11] D. Bryans. "Bitcoin and money laundering: mining for an effective solution," Indiana Law Journal: Vol. 89: Issue 1, Article 13, 2014, p443.
[12] "Cryptocurrency market capitalization" https://coinmarketcap.com/all/views/all/ (accessed 23 January 2018).
[13] W. Dai, "Bmoney" http://www.weidai.com/bmoney.txt (accessed 18 January 2018).
[14] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2009, available at https://bitcoin.org/bitcoin.pdf (accessed 14 January 2018).
[15] M. Möser, R. Böhme, and D. Breuker, "An inquiry into money laundering tools in the bitcoin ecosystem," eCrime Researchers Summit, IEEE, 2013.
[16] 18 U.S.C. §1956(h) (2012).
[17] United States v. Liberty Reserve, 13 Crim. 368 (S.D.N.Y. May 20,
2013) (available at https://archive.org/stream/704540-liberty-reserve- indictment/704540-liberty-reserve-indictment_djvu.txt) 2013.
[18] M. Anderson, "International money laundering: the need for ICC tive Jurisdiction" Virginia Journal of International Law, Vol. 53, pp 764-786.