The current issue and full text archive of this journal is available on Emerald Insight at:
www.emeraldinsight.com/1368-5201.htm

The use of cryptocurrencies in the money laundering process

Chad Albrecht and Kristopher McKay Duffin
Huntsman School of Business, Utah State University, Logan, Utah, USA
Steven Hawkins
Southern Utah University, Cedar City, Utah, USA, and
Victor Manuel Morales Rocha
Autonomous University of Ciudad Juarez

Abstract

Purpose – This paper aims to analyze the money laundering process itself, how cryptocurrencies have been integrated into this process, and how regulatory and government bodies are responding to this new form of currency.

Design/methodology/approach – This paper is a theoretical paper that discusses cryptocurrencies and their role in the money laundering process.

Findings – Cryptocurrencies eliminate the need for intermediary financial institutions and allow direct peer-to-peer financial transactions. Because of the anonymity introduced through blockchain, cryptocurrencies have been favored by the darknet and other criminal networks.

Originality/value – Cryptocurrencies are a nascent form of money that first arose with the creation of bitcoin in 2009. This form of purely digital currency was meant as a direct competitor to government-backed fiat currency that are controlled by the central banking system. The paper adds to the recent discussions and debate on cryptocurrencies by suggesting additional regulation to prevent their use in money laundering and corruption schemes.

Keywords Cryptocurrency, Tax havens, Illegal transactions, Money laundering process, Regulatory bodies

Paper type Research paper

Introduction

Cryptocurrencies are a group of nascent electronic currencies that were invented in 2009. The first cryptocurrency, Bitcoin, was created by Satoshi Nakamoto, a *pseudonym* for an individual or group of individuals, whose identity is still unknown. Over the past decade, Bitcoin and other cryptocurrencies have revolutionized the financial world by creating a stable form of currency that is not backed by any government and allows encrypted, anonymous transactions (Swartz, 2014). By nature, cryptocurrencies allow direct peer-to-peer transactions and eliminate the need for a bank or other intermediary to facilitate financial transactions (Peters, 2015). Such anonymity has allowed the black market to flourish as cryptocurrencies have enabled individuals to make illegal financial transactions that are difficult, and in some cases impossible to track (Heilman, 2016):

> While Bitcoin and the blockchain were initially thought to be anonymous, recent tools by both the FBI and other government agencies has allowed individuals, governments, and others "to track" and "discover" many bitcoin users on the blockchain.

Journal of Money Laundering Control
Vol. 22 No. 2, 2019
pp. 210-216

1368-5201
DOI 10.1108/JMLC-12-2017-0074

For the most part, cryptocurrencies are viewed as a contender to traditional fiat currency backed by central banks. However, because cryptocurrencies are not backed by any government entity, the underlying value of cryptocurrencies is unknown and fluctuates dramatically (Iwamura, 2014). Furthermore, both the academic community and the financial markets are still unsure if cryptocurrencies are a currency (such as the US dollar), a store of value (such as gold) or a combination of both (Hayes, 2017).

The money laundering process

The money laundering process itself is complex and complicated. Money laundering by definition is the act of channeling illicit funds through outside financial channels to make the funds appeared legitimate (McDowell, 2001). In the past, money laundering was typically done through established, small businesses or even through the financial channels of a large corporation. However, with the advent of the internet, the money laundering process has moved into the digital realm.

Preventive money laundering legislation was not enacted in the USA until the 1970s. The most important piece of legislation was finally passed in 1986 when money laundering itself was criminalized (Sultzer, 1996). Before this law, banks were only required to report large financial transactions through the Bank Secrecy Act of 1970. Noncompliant banks, who did not report their transactions, were often fined by the US Government. This law, currently a core element of the USA financial system, requires that financial transactions of $10,000 or more must be reported.

Money laundering is considered a problem for the worldwide community because the actions of criminal individuals, as well as illicit businesses and organizations, receive their funds from illegal and unethical sources such as fraud, corruption, child and slave labor, prostitution, drugs, weapons and terrorist activities. As a result, money laundering undermines the well-being and performance of the global economy (Buchanan, 2004).

From the perspective of the money laundering organization, the main objective of the money laundering process is to assimilate the funds from illegitimate sources into the mainstream financial system and to make the funds appear "clean and usable" for investments and other business ventures that support and protect the criminal organizations (Levi, 2002). Furthermore, the money laundering process allows the criminals that generate the illicit revenue to increase their own personal lifestyle expenditures. The money laundering process itself has been broken down into three basic steps, namely, placement, layering and integration (Gilmour, 2016).

Placement involves the process of taking "dirty money" and putting the funds directly into the mainstream financial system. This can be done by depositing funds into one or multiple financial accounts and/or getting funds exchanged for money orders, debit cards and/or traveler's checks. In other situations, bank accounts that are created for money laundering purposes are often used as the vehicle to move the illicit funds into the mainstream financial system (Isa, 2015).

Layering is the act of taking the dirty money and using it in a host of legal financial transactions to obscure the trail as to where the funds have originated (Compin, 2008). This may also involve transferring funds into an offshore account, which further obscures the origin of the money.

Finally, integration is used to describe the act of taking funds and integrating those funds into a mainstream economic activity such as investments, bonds, letters of credit, etc.

The three steps described above allow illicit funds to enter the financial system, become "washed" and then be used for investments and other expenditures that benefit the criminals involved (Barbot, 1995). Some of these expenditures involve purchasing equipment to further support illegal activities.

There are several different strategies used to move the money in the "placement" phase of the money laundering process. For example, one type of strategy involves using mainstream banks, a second strategy involves the use of secondary financial institutions and a third strategy does not use any formal financial institution whatsoever.

Placement is the most important step of the money laundering process because, at this stage, money is exposed and can be tracked. The first route taken in the placement process is the use of various methods that involve primary financial institutions. For example, "smurfing" describes the process by which money is converted into a money order or check, and perpetrators typically ensure that all deposits to financial institutions are under $10,000 to avoid mandatory reporting by the Bank Secrecy Act (Quirk, 1997).

Tax havens and offshore bank accounts are the most often used methods for moving illegal funds. When funds are deposited into an offshore account, it is more difficult to trace and can be transferred through multiple banks to obscure the trail (Picard, 2011). Furthermore, if funds are moved from the jurisdiction they originated from, the funds become harder to track and monitor.

Secondary financial institutions are also frequently used as a way to efficiently "place" the money. The most traditional method used to launder money is to use cash-intensive businesses as a front to deposit the money, where the illegal money is counted toward the business's revenue. Prime examples of this activity include using restaurants and other businesses.

As discussed earlier, shell companies are also often used in conjunction with offshore accounts as a way to launder illegal funds. At times, shell companies may not even conduct any actual business in the country where the firm is registered. As such, the illicit money is deposited into these accounts and characterized as "earnings/profit" of the shell companies.

The last method used to move dirty money is through the use of an informal financial network. This type of network is most often seen in India and China. These networks operate by one person exchanging money for an encoded note or chip. Perpetrators will then move these funds into another country and exchange notes for the same amount of cash that was originally deposited. Any handling fees are subtracted from the total transaction and the informal networks eliminate any formal records or paper trails (Passas, 2009).

The money laundering process itself has spread throughout the entire world with billions of dollars being illegally transferred every year (Schneider, 2006). Efforts to curb money laundering are often costly and ineffective. If left unchecked, money laundering can lead to a lack of trust in the global financial system and even threaten government entities and financial institutions throughout the world.

Cryptocurrencies: what are they and where are they from?

As discussed earlier, cryptocurrencies are a nascent form of "digital" money that was first created with Satoshi Nakamoto's invention of the Bitcoin in 2009. In more simple terms, cryptocurrency is a string of code that is recorded on an open public ledger to allow direct peer-to-peer exchange without any middle entity. The code used for cryptocurrencies is encrypted and verified on the "blockchain" – a large network of computers that verify every transaction of the ledger (Litchfield, 2015). While the blockchain is public, identifying an individual person or company to a specific transaction on the blockchain is extremely difficult. While certain cryptocurrency transactions, such as those recorded by Bitcoin, Litecoin and Dash are difficult, but possible to trace, other cryptocurrencies, such as Monero and Zcash hide each individual entry making financial transactions impossible to trace and identify (Deepika, 2017). As most cryptocurrencies are difficult to track, many criminals on the black market have begun to use cryptocurrencies throughout the money laundering process to engage in illegal financial transactions.

To avoid regulators over the past few years, criminals have revolutionized the money laundering process through cryptocurrencies. Before this new system of economic exchange, criminals were forced to transfer and hide their illegal funds through the central banking system. As a result, various governments were able to indirectly control money laundering by slapping heavier regulations and fines on banks and financial institutions, which made moving illegal funds increasingly difficult (Gao, 2009).

On the other hand, because cryptocurrencies do not involve central banks, cryptocurrencies bypass the banking system altogether (Brenig *et al.*, 2015). When each transaction is entered into the blockchain, it is anonymously recorded. For example, in the traditional banking system, accounts are used when money is deposited or withdrawn on behalf of the account holder by the central authority or through the actions of its members with the approval of the central authority. The amount of money within each account is confidential and the validity of all transactions are verified through the central bank or authority within the system.

However, with cryptocurrencies, users do not hold accounts in the traditional sense. With cryptocurrencies, each unit (or coin) of each cryptocurrency is tracked with a set of access keys that identify each individual coin. The owner of the coin receives a private key, which then identifies the individual as the legitimate owner of the funds (Reid, 2011). A transaction involving any number of units cannot take place unless both the private and public keys are used and encrypted. The public set of keys allow the community to track the movement and expenditure of all units as an additional measure to prevent double spending. As such, in the cryptocurrency system, users are not required to disclose personal information to engage in financial transactions.

Cryptocurrencies provide additional economic incentives for criminals to use this system. One growing benefit for criminals is the fact that cryptocurrencies as a whole are becoming more widely accepted as a form of payment amongst retailers. Currently, this acceptance is limited as cryptocurrencies often have to be exchanged for fiat currencies. However, this process becomes less burdensome as more and more retailers accept Bitcoin.

Another more prominent benefit of using cryptocurrencies is the ease in which funds can be moved from one country to another. In the layering step of the money laundering process, illicit funds are not only used to facilitate a *myriad* of financial transactions but also transferred to other financial jurisdictions where illegal organizations can access their funds from their base of operations, protecting their funds from seizure (Gruber, 2015).

With cryptocurrency, all that is required to move and transfer funds from one country to another is an internet connection. As there is no central authority regulating the transactions, funds can easily be moved between countries within the network established by the cryptocurrency. As the blockchain is compiled by peers, every node would have to be disconnected to cause a system collapse. This design allows the network to be resilient from outside disturbances, which facilitates a greater portability when transferring illicit funds (Levi, 2015).

One pattern of behavior that aids in the process of money laundering is the act of tax evasion. The act of tax evasion is defined as producing earnings outside an organization's tax jurisdiction or transferring funds to a "tax haven" where the earnings are not taxed or taxed very little (Marian, 2013). This evasion undermines the revenues that countries receive, with billions of dollars in losses of unreported revenue. The emergence of cryptocurrency has presented itself as the ultimate tax haven.

In recent years, governments from around the world have begun to cooperate with each other in an effort to target these tax havens. As international laws prevent governments from directly targeting the funds within those tax havens, governments have placed increasing pressure on the financial institutions used to transfer funds from one jurisdiction to another (Alldridge, 2008).

With the use of cryptocurrencies as a tax haven, there is no financial institution for governments to target. As a result, corrupt firms and criminal organizations can convert their earnings into cryptocurrencies and then transfer these funds anywhere in the world to evade tax authorities. This increased protection aids the money laundering process because it allows criminal organizations to gain full access and control to all the revenue they produce.

Authority and regulatory perspectives

Cryptocurrency itself is a specific form of virtual currency. Virtual currencies originated when the internet was born to facilitate transactions on the Web. Virtual currencies closely mirror the currencies issued by central banks in the sense that they have third parties that verify the transactions and supply of each virtual currency.

The first major efforts that were made by the USA Government to regulate virtual currencies was the prosecution of e-gold in 2007. E-gold was backed by gold and other precious metals to facilitate transactions through the trade of precious metals. However, it was discovered that the company that backed e-gold had approved transactions that clearly supported illegal activity and other money laundering activities.

As e-gold required a central authority that approved all transactions, the government could easily source records and track payments. The company first objected to the US Government's accusations by stating that it could not be targeted as it was not a money-producing business. However, the government was able to prove that e-gold had failed to obtain a license from the federal government to transmit money. The government interpreted the law as any organization or entity that transmitted money, whether it was fiat back currency or not, was subject to the rules and regulations surrounding the transfer of funds. This case was important as it set the standard that allowed the government to, for the first time, target businesses that dealt in virtual currencies, including cryptocurrencies.

However, unlike e-gold, cryptocurrencies cannot be easily investigated or prosecuted because cryptocurrencies are decentralized. In theory, cryptocurrencies have the potential to destabilized fiat currency and induce a state where the economy is not directly controlled or regulated by the government. Because of this risk, certain countries including India and China have strict laws against cryptocurrencies (Filippi, 2014). On the other hand, countries such as Japan have enacted laws and regulations specifically accepting cryptocurrencies as a legitimate form of currency (Chohan, 2017). Even so, most governments are now just beginning to discuss legislation and other routes that could potentially influence and even regulate the use of Bitcoin.

Conclusion

The use of cryptocurrencies in the money laundering process has the potential for widespread implications for economies around the world. Throughout history, money laundering has always been a significant challenge for governments. As the creation of the central banking system, money laundering has bypassed formal financial controls through placement, layering and integration. Cryptocurrency is closely tied with money laundering because of the anonymity it provides. With the use of cryptocurrencies in the money laundering process, criminal organizations are able to channel funds with increasing ease and evade investigation by authorities.

Although the price of Bitcoin and other cryptocurrencies fluctuate widely, they have proven to become more stable and accepted over time. If the use of cryptocurrency in the money laundering process is not addressed further, the unethical use of cryptocurrencies could be used to ultimately undermine the stability of the global economy. The solution to the illegal use of cryptocurrencies lies in the regulation and prosecution of money laundering wherever it is discovered, and the close regulation of cryptocurrency itself, including common anti-money laundering controls such as know your customer and other preventive measures, which would aid in preventing this new type of currency from being used for unethical and often illegal purposes.

References

Alldridge, P. (2008), "Money laundering and globalization", *Journal of Law and Society*, Vol. 35 No. 4, pp. 437-463.

Barbot, L.A. (1995), "Money laundering: an international challenge", *Tulane Journal International and Comparative Law*, Vol. 3, pp. 161-200.

Brenig, C., Accorsi, R. and Müller, G. (2015), "Economic analysis of cryptocurrency backed money laundering", ECIS 2015 Completed Research Papers. Paper 20.

Buchanan, B. (2004), "Money laundering–a global obstacle", *Research in International Business and Finance*, Vol. 8 No. 1, pp. 115-127.

Chohan, U. (2017), *Assessing the Differences in Bitcoin and Other Cryptocurrency Legality across National Jurisdictions*, University of New South Wales Business School, Sydney.

Compin, F. (2008), "The role of accounting in money laundering and money dirtying", *Critical Perspectives on Accounting*, Vol. 19 No. 5, pp. 591-602.

Deepika, P. (2017), "Cryptocurrency: trends, perspectives, and challenges", *International Journal of Trends in Research and Development*, Vol. 4, pp. 4-6.

Filippi, P. (2014), "Bitcoin: a regulatory nightmare to a libertarian dream", *Internet Policy Review*, Vol. 3 No. 2.

Gao, S. (2009), "Conceptual modeling and development of an intelligent Agent-Assisted decision support system for anti-Money laundering", *Expert Systems with Applications*, Vol. 36 No. 2, pp. 1493-1504.

Gilmour, N. (2016), "Understanding the practices behind money laundering–a rational choice interpretation", *International Journal of Law, Crime, and Justice*, Vol. 44, pp. 1-13.

Gruber, S. (2015), "Trust, identity, and disclosure: are bitcoin exchanges the next virtual havens for money laundering and tax evasion?", *Quinnipiac Law Review*, Vol. 32, pp. 135-208.

Hayes, A.S. (2017), "Cryptocurrency value formation: an empirical study leading to a cost of production model for valuing bitcoin." *Telematics and Informatics*, Vol. 34 No. 7, pp. 1308-1321.

Heilman, E. (2016), "Blindly Signed Contracts: anonymous On-blockchain and Off-blockchain bitcoin transactions", *Financial Cryptography and Data Security*, Springer, Berlin, Heidelberg, pp. 43-60.

Isa, Y. (2015), "Money laundering risk: from the bankers and regulators perspectives", *Procedia Economic and Finance*, Vol. 28, pp. 7-13.

Iwamura, M. (2014), "Can We stabilize the price of a cryptocurrency? understanding the design of bitcoin and its potential to compete with Central bank money", *International Finance Journal.*

Levi, M. (2002), "Money laundering and its regulation", *The ANNALS of the American Academy of Political and Social Science*, Vol. 582 No. 1, pp. 181-194.

Levi, M. (2015), "Money for crime and money from crime: financing crime and laundering crime proceeds", *European Journal on Criminal Policy and Research*, Vol. 21 No. 2, pp. 275-297.

Litchfield, H. (2015), "A novel method for decentralised peer-to-peer software license validation using cryptocurrency blockchain technology", *Australian Computer Society*.

McDowell, J. (2001), "Consequences of money laundering and financial crime", *Economic Perspectives*, Vol. 6 No. 2, pp. 6-8.

Marian, O. (2013), "Are cryptocurrencies 'super' tax havens?", *Michigan Law Review*, Vol. 112, p. 38.

Passas, N. (2009), *Informal Value Transfer Systems, Terrorism, and Money Laundering*, *Northeastern University*, Boston.

Peters, G.W. (2015), "Trends in cryptocurrencies and blockchain technologies: a monetary theory and regulation perspective".

Picard, P. (2011), "Bank secrecy, illicit money, and offshore financial centers", *Journal of Public Economics*, Vol. 95 Nos 7/8, pp. 942-955.

Quirk, P.J. (1997), "Macroeconomic implications of money laundering", *Trends in Organized Crime*, Vol. 2 No. 3, pp. 10-14.

Reid, F. (2011), "An analysis of anonymity in the bitcoin system", *Privacy, Security, Risk and Trust*, Springer, New York, NY.

Schneider, F. (2006), "Money laundering and financial means of organised crime: some preliminary empirical findings", *Global Business and Economics Review*.

Sultzer, S. (1996), "Money laundering: the scope of the problem and the attempts to combat it", *TN Law Review*, Vol. 63, pp. 135-234.

Swartz, N.D. (2014), "Bursting the bitcoin bubble: the case to regulate digital currency as a security or commodity", *Tulane Journal of Technology and Intellectual Property*, Vol. 17, pp 320-335.

Further reading

Chan, J. (2017), *The Digital Shadow Economy: Money Launderers, Firms, and Governance*, *National University of Singapore*, Singapore.

Hughes, S. (2014), "Regulating cryptocurrencies in the United States: current issues and future directions", *William Mitchell Law Review*, Vol. 40.

Corresponding author

Chad Albrecht can be contacted at: chad.albrecht@usu.edu