Vol.2 Issue.1 March-2021	Global Media and Social Sciences Research Journal (Quarterly)	
Page-73-84		
Social Sciences Multidisciplinary	Website: http://www.gmssrj.com Email:editorgmssrj@gmail.com,editor@gmssrj.com	ISSN:2709-3433 (Online) ISSN:2709-3425 (Print)

A Study of Blockchain Technology, Bitcoin and other Cryptocurrencies as Means of Money Laundering, Frauds and Scams

Hassan Raza[1]
M.Riaz Raza[2]

[1]MS Scholar, Bahria Business School, Bahria University Islamabad,hassanrazamsf@gmail.com
[2]Assistant Professor, Media Sciences, Bahria University Islamabad,Mriaz.buic@bahria.edu.pk

Abstract

Blockchain[1] Technology, a whole new innovation in the financial technology industry used to transfer monetary value around the world. This growing Blockchain technology is just 10 years old, without regulations and monitoring, the sector is still known as the 'Wild West' of the financial industry. With the rise in market capitalization[2] of Cryptocurrencies[3], there has been increase in money laundering, thefts, hacks, frauds and scams. This innovation of transferring value has proven to be safe haven for criminals and fraudsters to in washing their illicit proceeds. This research is conducted to look into the fact that millions of dollars are lost to cryptocurrency each day just because of the naïve behavior of Investors in investing in cryptocurrency and believing in different scams. In the Covid-19 Pandemic, authorities all over the world have been reserved for the mitigation of health and economic crisis, it has been proposed that this unstable economic and health condition throughout the globe can cause people to suffer with more crypto crimes as people seek basic health necessities through web, avoiding personal contact. This article debates on the Bitcoin concept, Anonymity for transfer of money, challenges to Anti-Money Laundering Authorities and Recommendations of the FATF in response to the risk arise due to large scale adoption of this new innovation.

Keywords

- Block chain,
- Cryptocurrency,
- Money Laundering,
- Frauds,
- Scams,
- Covid-19,
- FATF

[1] Blockchain is a shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a business network (IBM, 2021).
[2]Market cap is known as the market value of shares outstanding of publicly traded company. Market capitalization is equal to the number of shares outstanding multiplied by the price per share (wikipedia, 2021).
[3] A cryptocurrency is digital currency, decentralized network, secured by cryptography and based on blockchain technology (frankenfield, 2020).

Introduction

Bitcoin Concept

Blockchain technology seek massive attention and financial industry is known as a primary user of the blockchain concept. Bitcoin, cryptocurrency is most well-known application of blockchain technology (Nofer, Gomber, & Hinz, 2017). In 2009, *Satoshi Nakamoto*, created the first crptocurrency, known as Bitcoin, it was introduced after the financial crisis of 2008, as an alternate and innovative medium of exchange, unpretentious from corporate and government regulations. This Cypherpunk[4] had an idea behind this innovation to provide a medium of exchange for pseudonymous[5] entities (Weidai, 2017). He wanted to transform financial system by presenting money with characteristics i.e. (i) not vulnerable to inflation[6]. (ii) Pseudonymous transactions and do not require physical interaction. (iii) Lacks government backing. Cryptocurrency is decentralized— so, it can bypass the banking system (Brenig, 2015). Cryptocurrencies are not backed by the central bank, the intrinsic value of cryptocurrencies is unknown and may fluctuates dramatically (Iwamura, 2014). Decentralization reflects the fact that cryptocurrencies do not have intrinsic value and the value is solely dependent on the demand and supply of the crypto-coin. Any medium that permits transmission of significant worth around the globe with no determination or record keeping is a magnet for lawbreakers, including terrorists, tax evaders, maverick states, and sanctions dodgers (Blanco, 2020).

Today, the cryptocurrencies market capitalization fluctuates around $1 Trillion. Total number of cryptocurrencies being traded in real time is around 8,265 which are being traded in more than 350 online trading exchanges[7]. The value of one Bitcoin was less than one USD in 2009 and in January 2020, it exceeded USD 40,000 (coinmarketcap, 2021). Individuals who want to transact or buy the cryptocurrencies either runs a program that supports Bitcoin protocol or make an account with the host website[8] which allows transaction through Bitcoin or different cryptocurrencies. Bitcoin is stored online by Bitcoins exchanges who provides a file called as Digital wallet[9].

Risks Associated with Cryptocurrency

Bitcoin transactions are fast and have no restriction; nobody can block or freeze and neither irreversible nor traceable. Notwithstanding the source, size, nature and distance of the cybercrime funds, the Bitcoin gives unknown behavior or layering measure for cash out methodology, consequently the trail of money becomes ambiguous. By not involving any financial intermediary, the financial transactions by cryptocurrencies are never entered into the financial system and hence never recorded. Every crypto-exchange has given a limited access to the ledgers of entries for the authorities. Cryptocurrencies like Bitcoin (BTC), Litecoin (LTC) and Dash (DASH) are difficult, but can be traced besides mixing services[10]. Other currencies like Monero (XMR) and Zcash (ZEC) hide each transactions making impossible to

[4] Those who believe in achieving privacy, social and political change by use of cryptography (wikipedia, 2021).
[5] A Pseudonym is a fictitious name to hide their identity, or to impersonate other persons or entities in order to commit fraud.
[6] Inflation is defined as a decrease in purchasing power of currency (Fernando, 2020).
[7] Cryptocurrency exchanges are online based platform for trading in cryptocurrencies e.g. Coinbase, Binance, Bisq, cash app etc.
[8] LocalBitcoins is a peer to peer Bitcoin marketplace based in Helsinki, Finland. Its service facilitates over-the-counter trading of local currency for Bitcoins. Available at: https://localbitcoins.com
[9] A cryptocurrency wallet is also referred to as a digital Wallet, a trader need to have a digital wallet to trade and store cryptocurrencies.
[10] Mixing services are used to mix one's funds with other people's money to confuse the money trail and original source.

trace and identify (Deepika, 2017). In the Covid-19 Pandemic, authorities all over the world have been reserved for the mitigation of health and economic crisis, whereas the scammers and fraudsters have seen this as an opportunity of benefiting from the fear created by health crisis, — there were number of cases in Big Scale (Danske Bank 230 billion USD, Swedbank 10 billion USD) and Small scale 4 million USD (Smurfing case in Belgium) (Bloomberg 2019, Bloomberg 2019, EU Observer 2019). The official Twitter accounts of American Businessman Bill Gates, U.S Ex-President Barack Obama and Joe Biden a candidate for U.S Presidential Elections was hacked and demanded Twitter users to send Bitcoins to an unsubstantiated wallet, with the guarantee of a 2:1 profit for each transaction. The tweets were introduced by the message "I am giving back to the community" (Kyriakou, 2020). In January 2020, the official Twitter account of Elon Musk's was hacked, welcoming Twitter clients to a "Crypto party" (Dikbiyik, 2020). In October 2019, Polish police arrested Ivan Manuel Molina Lee, on international money laundering charges of cryptocurrencies including Binance, Kraken and BitMEX which is equivalent to 1.5 billion zlotys, about 350 million euros, obtained from illegal sources by money laundering for Colombian drug cartels using cryptocurrency exchange companies. In February 2020, the U.S. federal government has arrested Larry Harmon, CEO of the Coin Ninja and DropBit cryptocurrency wallet was arrested by U.S federal government for conducting money laundering activities which is equivalent to over 354,468 Bitcoin (BTC), approximately $ 311 million at the time of the transaction (Faccia, Cavaliere, Mosteanu, & Mataruna-Dos-Santos, 2020). According to Welle (2015) in November 2015, the three Greek banks were threatened to pay hundreds of thousands of euros in Bitcoin by a group of cybercriminals called as the Armada Collective. According to Kerbs (2015) the hackers demanded £80,000 from TalkTalk mobile telephone provider in BTC, in return for the hacked customer informations. Daily Telegraph (2016) reported that, the criminals who acquired control of Lincolnshire County Council's PCs with ransom ware also demanded $500 in BTC. These are just few examples of criminal activities in which BTC is considered as the preferred payment method. According to the UNODC[11] (2020) report on money laundering and globalization, it is assessed that $800bn - $2tn which is equivalent to the 2-5 percent of worlds GDP is laundered globally annually. That's between EUR 715 billion and 1.87 trillion each year. The lower figure represents even a bigger value than the total GDP of whole Russia. This underlines the magnitude of the money laundering problem around the world. Bryans (2014) stated that, the characteristic of Bitcoin that demonstrate helpful to its survival, and unsafe to viable Anti Money Laundering guideline, are the protocol obscurity and versatility through adaptability. Electronic money transfer makes it more difficult to detect money laundering process. The steps are modified in case of money laundering through cryptocurrencies, in the placement stage; the dirty money is floated into the Crypto Exchange working online to purchase Primary Coins (BTC). In the second stage, Layering, the firstly purchased coins (BTC) purchased are converted into other Altcoins to make money trail a bit complex, this is known as the 'chain hopping' process. Lastly, Integration, in this stage the Altcoins are again exchanged for the primary coins (BTC), which are later sold to convert them into cash which can be easily shifted to bank for cash withdrawal. Federal Bureau of Investigation (FBI) requested a budget allocation of 4.2$ Million for fiscal year 2020, for disrupt transnational organized crime financial and dark net networks (Wray, 2020). FBI spends about 75 percent of his total man hours capacity related to financial crimes on investigation of crimes related to Digital currency (Fruth, 2018). Criminals begin to hold onto Bitcoin as an accomplice in their cash out methodology and launder cash supported by Bitcoin (Moser, 2013). Gradually, Bitcoin

[11] The United Nations Office on Drugs and Crime that was established in 1997 as the Office for Drug Control and Crime Prevention. Available at: https://www.unodc.org

became a safe haven for criminals, of all the ransom ware classified in 2019, 97% of web assaults were demanded in BTC (Ciphertrace, 2020).

Literature Review

For literature review researchers have chosen to discuss arguments relating to (a) risks associated with Blockchain Technology and (b) disruptive changes in financial technology Industry. Criminals have mistreated cryptocurrencies for money laundering through many different ways, like contrabands on Silk Road and buying coins for illegal use (Forgang, 2019). Technology has become the biggest cause behind disruption, Or to be more accurate, the digital prospects to launder money provided by Financial Technology (Soudijn, 2019). Wegberg, Oerlemans, & Deventer (2018) examined money laundering and cash out strategy by considering VASPs (Bitcoin Mixing Services and Exchange Services). They concluded that Bitcoin money laundering is possible and has a high degree of likeness to be used in present and future money laundering schemes. Yaya J. Fanusie & Tom Robinson (2018) in their study regarding Illicit Bitcoin Transactions, found out that market places like Silk Road, AlphaBay were the main sources of illicit Bitcoin laundering through conversion services. Bitcoin exchanges received the greatest amount of identified illicit Bitcoins. Mixers and online gambling sites had the highest proportion for Bitcoin laundering. Mirzayi & Mehrzad (2017) stated that use of Bitcoin is money laundering and nonstop, modest, unregulated and illicit medium of transfers through financial boundaries. In accordance with the use of Bitcoins, India Mexico and china have restricted access to Bitcoins and countries like Ecuador Bolivia have banned trading of Bitcoins whereas European countries and US and Russia are taking measures to legalize and monitor Bitcoins.

United States of America in May 2017, officially recognized North Korea's cyber-related organization "WannaCry", which hacked more than 230,000 computers in 150 countries. In addition an analysis shows that North Korea earned $ 200 million in 2017 through the mining and hacking of cryptocurrencies including Bitcoin (Seo, Park, & Oh, 2018). According to Compin (2008) U.S. Authorities shut down a digital currency which was backed by gold, called E-gold, involved in money laundering, credit card and investment related frauds. The potential of these currencies to allow criminal proceeds to move faster and cheaper, making an allowance for people to use any currency they desire. On the argument on alternate medium of exchange for fiat currencies, Dwyer (2014), highlighted the fact that average monthly volatility of Bitcoin is higher than that for gold or a set of foreign currencies, and the lowest monthly volatilities for Bitcoin are less than the highest monthly volatility for gold and currencies. Cheah and Fry (2015) studied the volatile behavior and global adaption of cryptocurrency, they argued that volatility in price and market volume might not be expressed as bubbles and crashes, if Bitcoin is a true medium of exchange.

Additional typical fraud associated with cryptocurrencies would be fake ICO scheme. Concerns have been raised by Edwards, Hanley, Litan & Weil (2019) about initial coin offerings (ICOs) backed by cryptocurrencies[12]. The white paper document for issuance of Initial coins included confusing and insufficient disclosures for Investors. Investors are not able to distinguish between the legitimate issuers and those who are seeking profit by using fraudulent disclosures. Which results in floating of risky or bad crypto assets in the market. CoinDesk statistics, for 2018 indicated that an ICO could raise an average of $25 million, with estimates that 11% of the total amount would be scams (Mircea Constantin S, Crăciunescu, Brici, & Achim, 2020). According to the study towards sustainable cryptocurrency by (Limba, Stankevičius, & Andrulevičius, 2019), they concluded that Know Your Customer and Anti Money Laundering procedures is necessary step to mitigate risk carried by cryptocurrency.

[12] ICO is an acronym for initial coin offering, which is a process of issuance of tokens in exchange for cash or cryptocurrencies.

Whereas banking case study for AML legislations, the research showed that there might be hindrances to implement KYC and AML procedures. The study shows that there is no possibility to stop Bitcoin transaction to its anonymity.

Contextual Analysis

Aim of the Study

The main task of the research is to analyze cryptocurrencies as an instrument for money laundering, frauds, thefts, hacks and scams. The past studies aimed at providing a qualitative research based on block chain technology, Bitcoin structure and functionality and future prospects. We are aimed at providing significant quantitative evidences on money laundering, frauds, thefts, hacks and scams through Bitcoins and other cryptocurrencies. Highlighting the events which will provide grounds for the Anti-Money Laundering authorities in control of money laundering, frauds and scams, political and terrorism funding. This study further explains the financial regulations by Anti-Money Laundering for better future of global financial system.

Problem Statement

Technology has brought huge changes to the society, where speciously cybercrime is a new battleground. Cybercrime is not just considered as a fundamental sign of global crimes but it has destructive potential for new difficulties (Mabunda, 2018). Block chain technology has shown destructive changes to the financial system working under unregulated environment. Faccia, Cavaliere, Mosteanu, & Mataruna-Dos-Santos (2020) stated that risks are increasing due to digital economy, such as theft and ransom ware attacks. Factors like anonymity made these markets attractive for the laundering of proceeds from traditional crimes for illegal use, such as terrorist financing and corruption.

Research Question

The main research questions identified for this paper:

1. To identify the global figures of cryptocurrency related Thefts, Hacks, Frauds and Money Laundering?
2. To identify County wise cryptocurrency Exchanges who received funds from Criminal sources?
3. What are the steps taken to improve Block chain technology adaption and to counter risk associated with Block chain Technology?

Methodology

The methodology in use for this research is Quantitative. The Content Analysis is carried out to review current challenges of Block chain Technology. Content Analysis is a type of method to collect Secondary data, critically evaluate research studies and extract data from different reliable sources. To identify global figures of Thefts, Hacks, Frauds and Money Laundered through cryptocurrency, we analyzed the transactions between 2017 and 2020 and represented in Million USD. We aggregated total volume of cryptocurrency Thefts, Hacks, Frauds and Money Laundered. Our study also examines transaction data to determine to what extent cryptocurrency exchanges are the direct recipients of proceeds of illicit activity. We ranked countries from 1-9 on the basis of volume of illicit money receiving from illicit sources. The data show the country wise amounts in percentages that a country cryptocurrency exchanges directly received from the unlawful sources. No private consumer data was accessed during this study. All information came through Bitcoin block chain, and other public information.

Data Analysis and Discussion

Cryptocurrency thefts and hacks, frauds and Money laundering

Table 1 below shows that, cryptocurrencies related thefts, hacks, and frauds marked at $1.36 billion during the first five months (January to May), a great threat that this year 2020 could see even highest total amount which is stolen in cryptocurrencies as compared to $4.5 billion of 2019, $1.7 billion of 2018 and 168 million of 2017. The Table 1 also shows the percentage of direct payments to cryptocurrency exchanges from criminal sources, which is highlighted in percentage of 0.42%, 0.32%, and 0.17% in 2017, 2018 and 2019 respectively. The data source is spring 2020 Cryptocurrency Crime and Anti-Money Laundering Report by Ciphertrace Cryptocurrency Intelligence. According to the Technology Review, Chain Analysis report on Blockchain, The money laundered through cryptocurrency exchanges stood at 266 million, 1000 million and 2800 million in 2017, 2018 and 2019 respectively as shown in Table 1.

Table 1

Global Figures of Cryptocurrency thefts and hacks, frauds and Money laundering

	Statement	2017	2018	2019	2020
1	Money lost by Hacks and Theft	167	1080	370.70	60
2	Money lost by Fraud and Misappropriation	1.58	654	4100	1300
3	Direct Payments from Criminals sources to Exchanges	0.42%	0.32%	0.17%	-
4	Money laundered through crypto Exchanges	266	1000	2800	-

Note: Amounts are expressed in USD Million. *Source:* Ciphertrace Cryptocurrency Intelligence

According to the report of MIT Technology Review, Mike Orcutt (2020) highlighted that $2.8 billion laundered through crypto exchanges in 2019. According to Fanusie (2018) Web based gambling and Mixers services receive a high amount of illicit Bitcoins and hence, are major fears for Bitcoin laundering. Cross border money laundering analysis highlighted that, in exchange to exchange transfer almost 74% of the Bitcoins transactions were cross border and 88% of funds were sent to offshore exchanges by US Bitcoin ATMs in 2019, that of all the ransom ware recorded in 2019, 97% of assaults demanded BTC (Ciphertrace, 2020).

Cryptocurrency Exchanges Receiving Funds Directly from Criminal Sources

Table 2

Country Wise Analysis of Funds Received Directly from Criminal Sources

Rank	Country	2017	2018	%Change	2019	%Change
0	Global	0.43	0.34	-20.9	0.17	-50
1	Finland	8.30	7.30	-12	12.10	+65.7
2	Russia	5.10	2.10	-51.8	5.23	+149
3	UK	0.80	0.10	-87.5	0.69	+590

4	China	0.10	1.70	+1600	0.31	-81.76
5	France	0.13	0.13	0	0.21	+61.5
6	South Korea	0.03	0.13	+333.3	0.19	+46.15%
7	US	1.38	0.05	-96.37	0.09	+80%
8	Germany	0.30	0.92	+206.7	0.06	-92.47
9	Japan	0.04	0.04	0	0.04	0

Source: Ciphertrace Cryptocurrency Intelligence

Table 2, shows the country wise amounts in percentages that a country cryptocurrency exchanges directly received from the unlawful sources. According to the data, Finnish exchanges ranked at 1st with a percentage of 12.10% of BTC received in 2019 were directly from the unlawful sources, which is 65.7% greater than the amount received in 2018, the amount received in 2018 was 7.3% which was 12% less than 8.3% received in 2017.Russian cryptocurrency exchanges ranked 2nd with a percentage of 5.23% in 2019 which is 149% greater than the amount received in 2018. The amount received from illegal sources in 2018 was 2.1% which was 51.8% less than the amount received in 2017 which was 5.1%. United Kingdom ranked at the 3rd position with a percentage of 0.69% in 2019, which is 590% greater than the amount received in 2018. The amount received from illegal sources in 2018 was 0.10% which was 87.5% less than the amount received in 2017 which was 0.80%. China ranked at the 4th position with a percentage of 0.31% in 2019, which was 81.76% greater than the amount received in 2018. The amount received from illegal sources in 2018 was 1.70% which was 1600% greater than the amount received in 2017 which was 0.10%. France ranked at the 5th position with a percentage of 0.21% in 2019, which was 61.5% greater than the amount received in 2018. The amount received from illegal sources in 2018 and 2017 remains the same, with no change. South Korea ranked at the 6th position with a percentage of 0.19% in 2019, which was 46.15% greater than the amount received in 2018. The amount received from illegal sources in 2018 was 0.13% which was 333.3% greater than the amount received in 2017 which was 0.03%. United States ranked at the 7th position with a percentage of 0.09% in 2019, which was 80% greater than the amount received in 2018. The amount received from illegal sources in 2018 was 0.05% which was 96.37% less than the amount received in 2017 which was 1.38%. Germany ranked at the 8th position with a percentage of 0.06% in 2019, which was 92.47% greater than the amount received in 2018. The amount received from illegal sources in 2018 was 206.7% greater than the amount received in 2017 which was 0.30%. Japan stood at the last position in the table with a percentage of 0.04% of BTC received in 2017, 2018 and 2019 were directly from the unlawful sources.

Preparing for the Better Future

Even though Bitcoin and other virtual are growing, users are concerned about the legal status and government crackdowns. Aggressive regulatory measures and implementing criminal sanctions would be an effective way against money laundering and Cybercrimes. Regulatory measures can stop illicit money from entering the financial system, whereas implementing fines and criminal sanctions will discourage possible money launderers. **Bank Secrecy Act (BSA)** introduced in 1970, Implementation to Bank secrecy act required every financial institution to have information about transacting parties transacting money more than $10,000. The Bank Secrecy Act was to develop an effective AML regulation. **The Money Laundering Control Act** (MLCA) of 1986 declared money laundering or assisting in money laundering a Federal Crime. This act is crucial for executing criminal sanctions. In 2000, Uniform Money Services Act was accumulated in National conference of Commissioners on Uniform State Laws (NCCUSL). Before the Act, Every state has its own laws for Bitcoin or virtual currency money

laundering. According to this Act, Money Services Businesses declared to non-banking entities, which require license for providing facilities of payment and money exchange.

Financial Action Task Force (FATF) was established by the International Monetary Fund (IMF) in 1989. FATF has been strictly monitoring the money laundering through the exchange of virtual currencies, and we have seen developments have been made by countries implementing regulations for virtual asset sector, whereas still majority of the countries don't have any measures against the virtual currencies which has provided criminals a safe haven for illicit proceeds to launder. With support from the G20, the FATF has issued global, binding standards to guarantee that the virtual assets are treated equally, Implementation of regulations as same as the financial sectors to prevent the fraud of virtual assets for money laundering. The mass adoption and person-to-person transaction (Direct Transaction) are considered as the main challenges for regulatory bodies. These challenges can bring serious changes to the financial system and threat our ability to prevent and detect money laundering.

Digital Economy Task Force was established in 2013, at a conference that was held at the World Bank in 2013. The purpose of Digital Economy Task Force was to counterattack the property of anonymity of Virtual currencies. This property of virtual currencies is against every preventive measures to prevent cyber money laundering. Coinbase, the largest cryptocurrency exchange and other exchanges has implemented know-your-customer (KYC) program to address the increase in illegal activities through exchanges. While opening an account with Coinbase Exchange, user is required to provide information i.e. Passport, National ID, Driving License etc. which is later passed through authenticating process. Through this program, information about transactions will be possible to some extent.

In June 2019, Travel Rule was introduced by the Financial Action Task Force (FATF). According to this Rule, all Virtual Asset Service Provider (VASP) must ensure that they have enough verifiable information about the transacting parties which can be identified when needed. This rule is introduced to counter the anonymity of users. There are numerous tools available to allow VASPs to obey with aspects of the travel rule requests. In May 2020, The FATF through annual Private Sector Consultative Forum envisioned to involve the VASP sector, which was overdue due to the COVID-19 pandemic. European Financial and Economic Crime Centre (EFECC) has been established in June 2020 under the Europol, EFECC has the motive to enhance the support to EU States and EU bodies in countering financial and economic crimes. EFECC consists of 65 international financial experts and analysts. European Cybercrime Centre (EC3), European Counter Terrorism Centre (ECTC), European Migrant Smuggling Centre (EMSC) and the European Serious Organised Crime Centre (ESOCC) also have the similar purpose of EFECC.

So-called Stablecoins are the proposed coins in key development in the FATF Standards. Proposals show huge potential for mass-adoption which is not seen in existing virtual assets. So-called Stablecoins are designed to comply with the Federal laws and would be considered as VA or financial asset and their providers will be considered as either financial institutions or VASPs. FATF is also considering the risk lies within the adoption of so called stable coin on peer to peer transactions without the hosted financial institution's or VASPs. Initial Exchange Offering technique instead Initial coin offering will help in reducing the risk of frauds and scams and establishes a trust between investors and token issuers. Traditionally ICO, token issuers approach investors directly before the listing of the token in the exchange, this process often lead to scam and frauds resulting in huge loss of investors' money. In IEOs, a third-party in the form of a crypto exchange is involved before token sale; cryptocurrency exchanges thoroughly authenticate the credibility of token issuers. This gives security to the investors. Token issuers and investors details are verified according to KYC and AML protocols, screened against various global criminal databases. It helps in eliminating the

fraudsters, scammers, money launderers, terrorist financiers and other criminal entities from misusing the IEOs.

Conclusion

Financial institutions must identify the risks arise with the use of digital currency and new businesses with the technological advancements. Regulations and recommendations by the AML and FATF such as know your customers and adoption of so-called stable coins to cope and alleviate the risks emergent from VA. Looking at the brighter side of the technological advancement, this digital currency has the potential to become an alternate payment method for economies using fiat currencies. If we consider the Iraqi Swiss dinar and Bitcoin, we might be convinced that Bitcoins may succeed. Government actions to shut down the use of Bitcoins and other currencies will eventually create hatred for governments. Anonymous trait of Bitcoins make impossible to shut down, the explanation to the legit use of digital currencies lie in regulations and investigation of money launderers, scammers, fraudsters and other criminals. It would be eventually better to recognize the technology and then make strict regulations for the constructive use of digital currencies.

Limitations

There have been numerous cases in the world in which money laundering and fraud events have been found within the Financial Technology industry, but, in the absence of reliable sources, it was chosen not to include them in the list. Another limitation is the lack of possibility to carry out qualitative analysis, interview of victim of fraud or scam, which could have better supported the findings and conclusions. Our study is also limited by the lack of consolidated and verifiable data in the field of cryptocurrencies and especially in terms of the influence of cryptocurrencies in Political engineering, Terrorism funding and Human trafficking. We intend to identify suitable methods in the future to substantiate our finding both in the study of the impact of cybercrime in the evolution of cryptocurrencies, and of the influence of cryptocurrencies in cybercrime.

References

Blanco, K.A., (2020). Consensus Blockchain Conference (Virtual). *Financial Crimes enforcement network*. Available at: https://www.fincen.gov/news/speeches/prepared-remarks-fincen-director-kenneth-blanco-delivered-consensus-blockchain

Bloomberg Businessweek. (2018). *How's That ICO Working Out? Breaking down the biggest ICOs from the past few years*, available at: https://www.bloomberg.com/news/articles/2018-12-14/crypto-s-15- biggest-icos-by-the- numbers

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

Bryans, D. (2014). Bitcoin and money laundering: mining for an effective solution. *Ind.* LJ, 89, 441.

Cheah, E. and Fry, J. (2015) Speculative bubbles in Bitcoin markets? An empirical investigation into the fundamental value of Bitcoin. *Economics Letters*, 130. pp. 32-36. ISSN 1873-7374 Available at: https://doi.org/10.1016/j.econlet.2015.02.029

Ciphertrace. (2020). *Spring 2020 cryptocurrency crime and anti-money laundering report.* Retrieved from Ciphertrace:https://ciphertrace.com/spring-2020-cryptocurrency-anti- money-laundering-report/

Coinmarketcap. (2021). *Top 100 Cryptocurrencies by Market Capitalization*. Retrieved from coinmarketcap: https://coinmarketcap.com

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

Crypto.com the Syndicate, (2020). *Top 100 Cryptocurrencies by Market Capitalization*. Available at: https://coinmarketcap.com/

Daily Telegraph. (2016), *Council falls victim to cybercrime attack demanding ransom*. 1 February. Available at: http://tinyurl.com/zwcxl5t (accessed 1 February 2016).

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

Dikbiyik, F. (2020, April 11). *Who is behind the latest Elon Musk scam?* Retrieved from Medium: https://medium.com/@fdikbiyik

Dwyer, GP. (2014). The Economics of Bitcoin and Similar Private Digital Currencies. *Clemson University and the University of Carlos III*, Madrid.

Edwards, F. R., Hanley, K., Litan, R., & Weil, R. L. (2019). Crypto Assets Require Better Regulation: Statement of the Financial Economists Roundtable on Crypto Assets. *Financial Analysts Journal* , 75:2, 14-19, DOI: 10.1080/0015198X.2019.1593766 .

Faccia, A., Cavaliere, L. P., Mosteanu, N. R., & Mataruna-Dos-Santos, L. J. (2020). Electronic Money Laundering, The Dark Side of Fintech. An Overview of the Most Recent Cases . *12th International Conference on Information Management and Engineering*, (p. DOI: 10.1145/3430279.3430284).

Fanusie, Y., & Robinson, T. (2018). Bitcoin laundering: an analysis of illicit flows into digital currency services. *Center on Sanctions and Illicit Finance memorandum*, January.

Fernando, J. (2020, Nov 18). *Inflation.* Retrieved from Investopedia: https://www.investopedia.com/terms/i/inflation.asp

Frankenfield, J. (2020, May 05). *Cryptocurrency.* Retrieved from Investopedia: https://www.investopedia.com/terms/c/cryptocurrency.asp

Forgang, George. (2019). "Money Laundering Through Cryptocurrencies". *Economic Crime Forensics Capstones*. Available at: https://digitalcommons.lasalle.edu/ecf_capstones/40

Fruth, J. (2018, February 14). 'Crypto-cleansing:' strategies to fight digital currency money laundering and sanctions evasion. Retrieved from Reuters: Available at: https://www.reuters.com/article/bc-finreg-aml-cryptocurrency/crypto-

cleansingstrategies-to-fight-digital-currency-money-laundering-and-sanctions-evasionidUSKCN1FX29I

Fanusie, Y., & Robinson, T. (2018). Bitcoin laundering: an analysis of illicit flows into digital currency services. *Center on Sanctions and Illicit Finance memorandum*, January.

IBM. (2021). *Overview of Blockchain technology.* Retrieved from IBM: https://www.ibm.com/ae-en/blockchain/what-is-blockchain?

Iwamura, Mitsuru and Kitamura, Yukinobu and Matsumoto, Tsutomu, Is Bitcoin the Only Cryptocurrency in the Town? Economics of Cryptocurrency and Friedrich A.

Hayek (February 28, 2014). Available at https://ssrn.com/abstract=2405790 or http://dx.doi.org/10.2139/ssrn.2405790

Krebs, B. (2015). TalkTalk hackers demanded £80K in Bitcoin Oct 2015. In: Krebs on Security. Available at: http://tinyurl.com/q3adtrt (accessed 28 January 2016).

Kyriakou, P. (2020, July 24). *Cryptocurrency theft, scam and other misadventures: what prospects for international governance?* Retrieved from Blog of the European Journal of International Law: https://www.ejiltalk.org/cryptocurrency-theft-scam-and-other-misadventures-what-prospects-for- international-governance/

Limba, T., Stankevičius, A., & Andrulevičius, A. (2019). Towards sustainable cryptocurrency: Risk mitigations from a perspective of national security. *Journal of security and sustainability issues ISSN 2029- 7017*, Volume 9 Number 2. Available at: http://doi.org/10.9770/jssi.2019.9.2(2).

Mabunda, S. (2018). Cryptocurrency: The new face of cyber money laundering. *2018 International Conference on Advances in Big Data, Computing and Data Communication.* Durban, South Africa. (pp. 1-6).

Mike Orcutt. (2020). *Blockchain.* Cambridge: MIT Technology Review. Available at: https://www.technologyreview.com/2020/01/16/130843/cryptocurrency-money- laundering-exchanges/

Mircea Constantin S, c., Crăciunescu, S. L., Brici, I., & Achim, M. V. (2020). A Cryptocurrency Spectrum Short Analysis. *Journal of Risk and Financial Management*, Vol 13, 184; doi:10.3390/jrfm13080184.

Mirzayi, S., & Mehrzad, M. (2017). Bitcoin, an SWOT Analysis. *7th International Conference on Computer and Knowledge Engineering (ICCKE 2017)*. Mashhad.

Möser, M., Böhme, R., & Breuker, D. (2013). An inquiry into money laundering tools in the Bitcoin ecosystem. *In 2013 APWG eCrime researchers summit*. (pp. 1-14).

Nofer, M., Gomber, P., & Hinz, O. (2017). Blockchain. *Bus Inf Syst Eng*, 59(3):183–187

Seo, J., Park, M., & Oh, H. (2018). Money Laundering in the Bitcoin Network: Perspective of Mixing Services. *2018 International Conference on Information and Communication Technology Convergence (ICTC*). jeju, south Korea.

Soudijn, M. (2019). Using police reports to monitor money laundering developments. Continuity and change in 12 years of Dutch Money Laundering Crime Pattern Analyses. *European Journal of Criminal Policy and Research*. Available at: https://doi.org/10.1007/s10610-018-9379-0.

UNODC. (2020). *Money laundering and Globalization*. Retrieved from UNODC: https://www.unodc.org/unodc/en/money-laundering/globalization.html

Weidai. (2017). *Bmoney*. Retrieved from Weidai: http://www.weidai.com/bmomey.txt

Welle, Deutsche. (2015). *Greece says hackers hit banks with Bitcoin ransom demand*. November. Available at: http://tinyurl.com/hvce48v (accessed 28 January 2016).

Wegberg, R. v., Oerlemans, J.-J., & Deventer, O. v. (2018). Bitcoin money laundering: mixed results? *Journal of Financial Crime*, Vol. 25 No. 2.

Wray, C, (2019). *FBI Budget Request for Fiscal Year 2020. FBI news*. Available at: https://www.fbi.gov/news/testimony/fbi-budget-request-for-fiscal-year-2020

wikipedia. (2021). *cypherpunk.* Retrieved from wikipedia: https://en.wikipedia.org/wiki/Cypherpunk

Wikipedia. (2021, january). *Definition of market capitalization*. Retrieved from wikipedia:https://en.wikipedia.org/wiki/Market_capitalization

Yaya J. Fanusie., Tom Robinson. (2018). Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services. *Foundation for Defense of democracies Center on sanctions & Illicit Finance*.