Advances in Economics, Business and Management Research, volume 123
1st International Conference on Accounting, Management and Entrepreneurship (ICAMER 2019)

Money Laundering:

Customer Due Diligence in the Era of Cryptocurrencies

Razana Juhaida Johari*, Norareena Binti Zul, Norli Talib
Faculty of Accountancy
UiTM Shah Alam, 40000 Shah Alam
Selangor, Malaysia
*razana@salam.uitm.edu.my

Sayed Alwee Hussnie Sayed Hussin
Jabatan Audit Negara
Putrajaya, Malaysia

***Abstract*—Money laundering is a global phenomenon and has been considered as major threat towards economic stability as it is associated with criminal's activity such as drug trafficking, terrorism funding and financial crimes including corruption and tax evasion. Advancement of technologies and emergence of cryptocurrencies such as Bitcoin and Monero are disruptive financial technology that present governments with new national security challenges and terrorist groups, criminals and rogue states with opportunities. Cryptocurrencies garnered attention and intense interest especially from businesses, consumers, central banks and other authorities as it promised to replace trust in commercial and central banks with a new decentralized system founded on block chain and related distributed ledger technology. Nevertheless, customer due diligence (CDD) which is the first line of defense of money laundering is vital in order to curb illicit money inflows and outflows from financial institution. In the era of cryptocurrencies, customer due diligence should be thoroughly conducted. The combination of information technology and CDD teams will create stronger defense in curbing the risks of money laundering in financial institution. This paper addressed the stages of money laundering, customer due diligence, emergence of cryptocurrencies and its nature as well as how it related to money laundering activities. Finally, the discussion on how CDD procedures could curb money laundering involving cryptocurrencies is also discussed.**

Keywords: money laundering, cryptocurrencies, financial institution, technologies

I. INTRODUCTION

Money laundering is a global phenomenon which can be considered as major threat towards economic stability as it is associated with criminal's activity such as drug trafficking, terrorism funding and financial crimes including corruption and tax evasion [1]. There are various definition of money laundering across the globe and according to Financial Action Task Force (FATF), money laundering as the processing of a large number of criminal acts to generate profit for an individual or group that carries out the act with the intention to disguise their illegal origin, in order to legitimize their ill-gotten gains of crime [2]. Furthermore, money launderers maximized their return and minimize their risk in non-financial term where such optimization is achieved by decreasing the possibilities of having their illicit money traceable to its origin [3].

In general, money launderers mainly focusing on finding ways to disguise their ill-gotten money and most of developing countries have the characteristics and attributes that is suitable for the money launderers to carry out their illegal activities [4]. A report by Global Financial Integrity (GFI), Malaysia's illicit outflows between 2005 and 2014 was estimated up to about US$431 billion (RM1.8 trillion). Moreover, as depicted in Figure 1, in 2014, illicit financial outflows from Malaysia was estimated around 6-10% of the value of Malaysia's trade of US$443.2 billion which put Malaysia in the fifth among all countries for illicit capital flight behind China, Russia, Mexico and India [5].

Estimated Ranges for Illicit Financial Flows, 2014 (cont)
(Percent of total country trade, unless noted)

Country	Illicit Financial Flows				Trade Misinvoicing				BOP Leakages		Total Trade (millions of US $)
	Outflows		Inflows		Outflows		Inflows				
	Low	High	Low	High	Low	High	Low	High	Outflows	Inflows	
Lesotho	3%	7%	1%	1%	3%	7%	0%	1%	0%	0%	3,133
Liberia	12%	25%	541%	693%	12%	25%	508%	660%	0%	33%	1,629
Libya	0%	0%	4%	5%	0%	0%	4%	5%	.	.	40,000
Macedonia, FYR	1%	1%	1%	2%	1%	1%	1%	2%	0%	0%	12,211
Madagascar	1%	1%	1%	2%	0%	0%	1%	2%	1%	0%	5,397
Malawi	7%	25%	4%	8%	5%	23%	4%	8%	2%	0%	4,116
Malaysia*	6%	10%	7%	13%	5%	9%	7%	13%	0%	0%	443,210
Maldives	15%	23%	0%	0%	6%	14%	0%	0%	8%	0%	2,137
Mali	7%	15%	9%	19%	4%	12%	9%	19%	3%	0%	6,056

Fig. 1. Estimated ranges for illicit financial flows [5].

It is crucial to understand that money laundering activities may lead to volatility in exchange rates and interest rate owing to unexpected inflows and outflows of capital thus negatively affect the economic growth as a whole due to the availability of illicit funds in an economy [6]. Aluko and Bagheri [4] further stated that money laundering gives a significant impact on the economic, political and social facets of developing countries, hence, understanding all of these settings in developing countries is fundamental ingredient in the war against money laundering. Particularly in smaller and less developed countries, the rise of an illicit economy from injection of laundered money including from illicit drugs activities will resulted un reductions of annual economic growth rates because money laundering activities weaken the rule of laws, facilitates corruption and also reinforces the illicit drug sector [6].

The Managing Director of International Monetary Fund (IMF), Christine Lagarde, stated that there is no doubt that money laundering and terrorist financing can threaten a country's economic stability. Despite robust effort to curb illicit money inflows in legal financial system, sophisticated criminals is always one step ahead to exploit the vulnerabilities in financial systems for their proceeds of crime. The context of 'traditional money laundering' refer to the process took place to launder money which mainly focus on an act to conceal or disguise their proceeds of crime by exploiting the financial institutions as a vehicle which differ from the current complex structure of money laundering activities due to advancement of technologies which lead to emergence of disruptive technologies such as cryptocurrencies. Thus, anti-money laundering regime should be able to keep up with the fast pace of technologies advancement by combining a richer nexus of intertwined human and technology-generated decisions to identify suspicious transactions' red flags and money laundering behavior in order to curb inflows and outflows of illicit money into financial institution [7].

A. *Stages of Money Laundering*

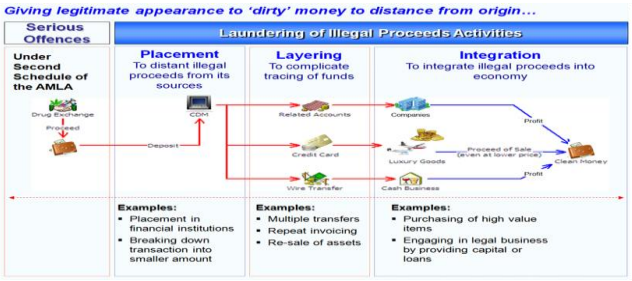

Fig. 2. Stages of money laundering.

Figure 2 presented three stages of money laundering process (i.e. placement, layering and integration) based on the Anti-Money Laundering (AML) & Counter Funding Terrorisms (CFT) [8].

1) Stage 1: Placement: Placement is the most vulnerable to detection risks due to suspicions that may arise after placing a huge amount into legitimate financial system. Sophisticated criminal planned their criminal activities with the main objective to evade controls and avoid detection. There are a lot of methods for the money launderer to separate their dirty money from illegal sources and placed into financial system. Common methods used by the criminal, are:

i. depositing the ill-gotten gains into financial institutions;
ii. structuring (smurfing) which the funds are of high value are broken into many small value transactions;
iii. use of financing facilities at a financial institution and making accelerated repayment before its tenure; and
iv. cashing unused chips at casinos for casino cheques, making them appear as "winning cheques".

2) Stage 2: Layering: The second stage of money laundering process is layering which is the most complex and often involves international movement of the funds with the primary focus to create multiple layers of transactions to ensure the illicit money are further distance from its origin. Layering are supposed to obscure or to make it even more difficult to trace and appeared as legal sources. Money launderer may electronically move the funds from one country to another and divide the funds into investments placed in legitimate financial institution by exploiting the loopholes or discrepancies in legislation. Examples of layering are:

i. multiple transfers and re-transfer of funds into the same or various accounts;
ii. repeat invoicing for the same transaction; and
iii. re-sale of assets originally purchased in cash by using the illicit funds

3) Stage 3: Integration: The final stage of money laundering process is Integration where laundered proceeds are successfully integrated into the economy as legitimate funds/money. This illicit money that have been 'clean' will the used to buy high value property or luxury items and engage in legal business. It would be difficult to detect illicit funds at this stage as it appeared to be from legitimate sources. Integration process are:

i. trading activities that include invoice manipulation to remit money abroad;
ii. engaging in legal business by providing capital or loans; and
iii. buying property or high value items

II. EMERGENCE OF CRYPTOCURRENCIES AND ITS NATURE

A. *Cryptocurrencies*

Digital/virtual currency which is known as cryptocurrencies is one of the famous types of electronic money. Cryptocurrencies is where the currency is being issued electronically and the transferability into fiat currency is not guaranteed by the state [9]. Besides that, cryptocurrencies are a digital currency in which block chain methods are used to secure the trades and control the generation of new units of currency and operating independently without a central authority [10]. In addition, Chiu and Koeppl [11] defined cryptocurrencies as a digital means of payment in a distributed system where a trusted third party is not involved. A moment ago, cryptocurrencies have become the main topics in the financial industry as it is immune to any central authority since it was not issued by them.

Cryptocurrencies are a disruptive financial technology that present governments with new national security challenges and terrorist groups, criminals, and rogue states with opportunities. Cryptocurrencies garnered attention and intense interest especially from businesses, consumers, central banks and other authorities as it promised to replace trust in commercial and central banks with a new decentralized system founded on block chain and related distributed ledger technology. Cryptocurrencies is functioning by using the blockchain therefore, to maintain the trust, every transaction and the supply of the cryptocurrencies will be verified by the user while the other user have the same access to every transaction

that took place. Holding onto trust without a strong foundation also means that cryptocurrency can simply stop functioning, resulting in a complete loss of value.

Another feature of cryptocurrency is highly fluctuated in value, hence no matter how sophisticated decentralized technology of cryptocurrencies was built; it is actually a poor substitution of current available financial institution [12]. Since technology ahead rapidly, criminals had recognized the technology of cryptocurrencies as one of the system that can be used to commit their illegal profit and activities [13]. This is due to virtual banking allows them to do transaction such as sell, buy and exchange goods without interacting physically and this causes their illegal activities to be untraceable. Bitcoin which is one of thousand type cryptocurrencies clearly shown that it had been used by criminals to do their illegal activities such as they started to use bitcoin to cash-out their illegal money as it is undetectable and have no interference from the authority [14].

B. Cryptocurrencies as New Vehicle of Money Laundering

Phenomenal growth in the value of cryptocurrencies has attracted sophisticated criminal to manipulate the key feature of cryptocurrencies (i.e. the implementation of a set of rules that to align the incentives of all participants and also to create a reliable payment technology without central trusted agent) as their vehicle in money laundering activities. Another feature of cryptocurrencies that provide anonymity and irreversible transactions has complicated the money trails to avoid detection where it is further complicated as this digital currency does not have controls to protect against abuse [15]. Mabunda stated that money laundering activities has adopted cryptocurrencies to launder their illegally obtain funds to disguise their true identities and avoid arrest [16].

As crypto transactions do not require criminals to provide information such as their real name, personal identity, declaration of income and proof of source of income which usually needed for normal banking transaction, these criminals are able to evade the watchful eye of law enforcement. For example, as shown in Figure 3, instead of robbing a bank, criminals shifted their modus operandi by raiding cryptocurrency exchanges where first half of 2018 has seen nearly three times as much cryptocurrency stolen as in all of 2017 [17].

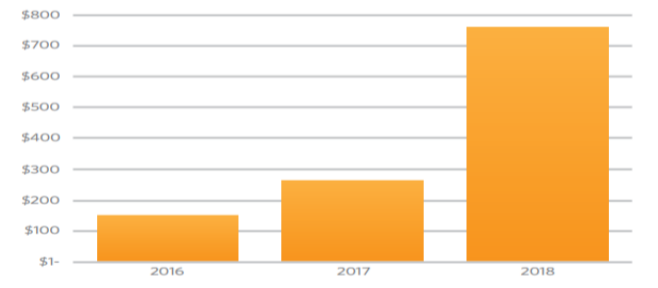

Fig. 3. 3x crypto stolen from exchanger [17].

Cryptocurrencies is proven to be the new vehicle for money laundering in Silk Road case which is well-known as the eBay for drugs activities. Silk Road is an online drug market that helped dealer to sell drugs with Bitcoin. Ross Ulbricht who was known as 'Dread Pirate Roberts' was arrested in the US and was charged with money laundering, computer hacking, narcotics trafficking and soliciting a murder [18]. Block chain underlying cryptocurrency does not store information such as IP addresses or private information that can be used to identify the account holder therefore it is impossible to determine whether an anonymous, numbered accounts is related to each other [19]. It is easy to associate money laundering activities and cryptocurrencies due to its key features that enhance difficulties of detection of suspicious activities, identify the users and obtaining the transaction records.

III. Customer Due Diligence as Traditional Detection Mechanisms of Money Laundering

A. What is Customer Due Diligence?

Customer Due Diligence (CDD) is the most basic and fundamental development and compliance of an effective BSA/AML. Standard Guidelines on Anti-Money Laundering and Counter Financing of Terrorism issued by Bank Negara Malaysia requires every reporting institution such as banks and insurance companies to conduct customer due diligence and obtain satisfactory evidence and properly establish in its records, the identity and legal existence of any person applying to do business with it. CDD officer must ensure that evidence received is substantiated by reliable and independent source documents.

Furthermore, reporting institution is required to conduct CDD when establishing business relationship with any customers, transaction involving a sum amount that exceeds the amount specified by Bank Negara Malaysia, in the event where there is suspicion of money laundering or financing of terrorism or it has any doubt on information previously obtained information [20]. Money laundering is one of the immense risks in every financial institutions as failure to prevent inflows of illicit money into the financial institution will resulted in huge fines and suffer reputational damage [21]. For example, HSBC Bank has been fined by the United States regulator for almost USD$2 billion after it was revealed to be exploited by Mexican drug traffickers to launder money [22].

Mugarura [23] also supported that CDD is an important AML measure, which needs to be streamlined and implemented with care to apply across the board to properly safeguard the financial institution from being the vehicle of money laundering activities. Financial Action Task Force (FATF) 40 Recommendation, under Recommendation 5 stated that, financial institutions should verify the identity of the customer and beneficial owner before or during the course of establishing a business relationship or conducting transactions for occasional customers. This shows that despite banking institution are equipped with automated systems to identify the red flags of suspicious transaction and integrated customers' identification, human expertise is vital in assessing money laundering risk [21].

Therefore, it is crucial to have a competent frontline officer who are dealings with the customers and responsible to conduct customer due diligence before establishing business

relationship. Frontline officers are actually the first line defense against money laundering. Furthermore, FATF recommendation also stressed on the identification of the ultimate beneficial owner to avoid the misuse of corporate vehicles for any proceeds of crime [24].

Nevertheless, by taking into consideration the emergence of cryptocurrencies and their features that could be operated without the central trusted agent, has brought forward a question of whether the CDD is still considered relevant in detection of suspicious transactions of money laundering?

B. Customer Due Diligence and Cryptocurrencies

Cryptocurrencies' features are specially designed to avoid detection by the law enforcement, thus, current anti-money laundering (AML) regime is required to be comprehensive and effective to address this issue as the financial institution associated with money laundering activities will resulted in reputational damage and undermine the public trust. According to a survey, those involved in money laundering, knowingly or unknowingly, will face risk regulatory fines, reputational damage and even prosecution. This fear of regulatory breaches has unintended consequences as the financial institution deliberately avoiding their customers which they perceived as high risk and highly associated with financial crime. 72% of the respondents saying that they would choose to avoid rather than managing. The implications of financial crime conviction are as in the Figure 4 below [25].

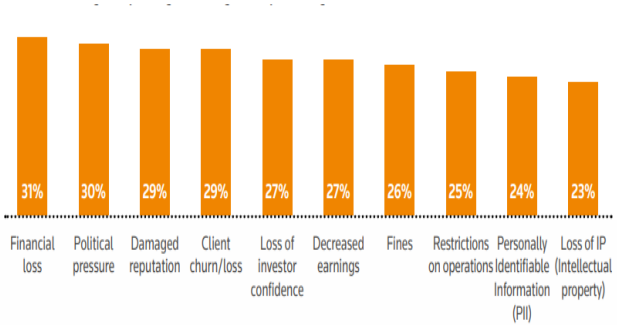

Fig. 4. Implication if convicted of financial crime [25].

This fear of financial and reputational damage due to regulatory breaches is having another, unintended consequence. Fearing that prevention alone may not be able to limit exposure to financial crime, organizations are deliberately avoiding customers, suppliers, regions or industries that they perceive as being most exposed to financial crime. The survey supports this view, with 72% saying they de-risk by avoiding, rather than managing, heightened risk customers. Rather than suppressing crypto adoption, regulators from all over the world has increased their focus on regulating a functional financial system. Customer due diligence in the era of cryptocurrencies is required to be vigorous as there is no way to verify the declaration of ownership information presented by the customers [26].

This means that robust due diligence process to know you customer, in term of their background, source of income, nature of their business and other risks associated with is essential for high risk customers identification to mitigate the risks of association with sanctions, internal watch-list individuals, reported organized crime etc. Furthermore, FinCEN considers both virtual currency payment processors and virtual currency exchange platforms to be money transmitters which indicates that for established cryptocurrencies or Initial Coin Offerings (ICOs), customer due diligence procedure would be required to perform as when a customer open a new bank account, and they may be also have the obligation to monitor the transactions made with their cryptocurrency. Nevertheless, given the nature of cryptocurrency, it would be difficult from practical perspective.

Last but not least, it is believed that registered and highly supervised crypto money will lose its popularity as the sophisticated criminals focused on crypto money that able provide ultimate anonymity and low risk of detection and becoming one of reporting institution is definitely a hurdle for their proceeds of crime. Reporting crypto exchanger will face a huge challenge to monitor the transactions yet it may be preferable by investors to invest in the markets through a regulated venue to avoid the same incidence of cyber intrusion on South Korean cryptocurrency exchange Coinrail, resulted in loss for about 30 percent of the coins traded 40 billion won or $37.28 million [27].

IV. Customer Due Diligence Procedures to Curb Money Laundering Involving Cryptocurrencies

It is impossible for regulators to sit back and just let cryptocurrency proliferate without regulation and interference. Cryptocurrencies' key features are has attracted hackers, criminals and those who are looking to clean their illicit money anonymously. Various measures have been adopted to address the risks associated with cryptocurrency due to its rapid developments in its usage. Bank Negara Malaysia (BNM) in its press release dated 27th February 2018 wishes to reiterates that invocation of reporting obligations on digital currency exchange does not means authorization, licensing, endorsement or validation by the Bank of any entities involved in the provision of digital currency exchange services [28]. In addition, BNM also stressed that digital currencies are not a legal tender in Malaysia.

In 2014, Financial Action Task Force (FATF) released the report entitled "Virtual Currencies – Key Definitions and Potential AML/CFT Risks" and subsequently in June 2015, Guidance for a Risk-Based Approach for Virtual Currencies was issued to explain the application of the risk-based approach (RBA) to anti-money laundering/counter financing of terrorism (AML/CFT) measures in the digital currencies' context. FATF Risk-Based Approach for Virtual Currencies under Recommendation 10 requires that customer due diligence procedure should be conducted at the point of establishing new business relationship or during an occasional transaction greater than designated threshold by the convertible virtual currencies' exchanger [29].

Therefore, special due diligence will be applied once the customers decide to exchange fiat currencies to cryptocurrencies and vice versa. Recommendation by KPMG to combat money laundering involving cryptocurrencies by strengthening AML procedures at financial institution,

monitoring the transaction which as stated above would be difficult, improving the regulation, placing third-party providers under state supervision, regulating cryptocurrency exchanges and also by way of using blockchain as the solution.

A. Strengthening AML Procedures Focusing Mainly on Customer Due Diligence

Financial institution should focus on the process during the interchange of fiat currency to cryptocurrency and vice versa. In which, financial institution should be able to distinguish their normal customer behavior and high-risk customer related to financial crime activities. Strengthening AML procedures and adherence of recommendation by FATF will safeguard financial institution from becoming the vehicle of money laundering activities. Financial institutions are equipped with automated systems to identify the red flags of suspicious transaction [21]. The red flags of high-risk customers are when the predominant sources of income derived from cash or cash-equivalent transactions, recurring wire transfer to digital currency exchange, excessive inflows and outflows that does not match the customers source of income declared, transactions that was structured to evade record keeping and many more. As suggested by Isa, Sanusi, Haniff and Barnes [21], having competent personnel as CDD officer is crucial as they are the first line of defense against money laundering. Identification of such red flags would be the first step before conducting enhanced due diligence on high risk customers. Banking institution should assess their processes and system to avoid accepting flows from exchanges that do not require identification or CDD information and proceeds from privacy coins [19].

B. Robust Transaction Monitoring

Robust transaction monitoring can only be done during exchange however, the anonymity of cryptocurrency prevents financial institution to follow the money trail. Therefore, it is impossible to identify the beneficiary of the transaction. However, patterns and behavior of money laundering scheme can be identified via algorithm developed for fiat currency. As the public ledger is made available for every user, relationship of one account with criminal activities can be identified where the flow of money will then be compiled to formulate powerful intelligence for law enforcement [19]. However, there is no guarantee that the criminal will use crypto money that has registered as reporting institution resulted in no impact in reducing the rate of money laundering activities. Besides, issuance of e-wallet should not be taken lightly and rigorous CDD is needed at the point of creation to avoid issuance of anonymous trading accounts. Global standard should be developed where e-wallet is required to be developed to an existing person.

C. Blockchain as a Solution

Blockchain is a perfect system as a solution for the abuse use of cryptocurrencies for illegal activities such as drugs trafficking and money laundering. As mentioned above, blockchain is maintained on an online public ledger, which enables the supervision, validation and recording of the complete history of each transaction [19]. Hence, by integrating anti-money laundering risk analysis as well as alert and reporting mechanisms into blockchain technology, a greater supervision will be allowed. This because, blockchain technology has its unique features which verifies each of its phase of transactions where transactions without verification of all transaction phases will be blocked immediately. This inherent characteristic would reduce the challenges face by anti-money laundering team, nevertheless, such technology will definitely come at higher cost and jeopardize the main unique feature of cryptocurrency which is anonymity.

V. CONCLUSIONS

Cryptocurrencies is a disruptive financial technology that is vastly on the rise due to the advantages that cryptocurrencies pose, including speed of transaction, traceability and transparency. However, the law enforcements agencies and cyber security has difficulty to keep up with this complex and ever changing nature money laundering activities. Cryptocurrencies mass adoption is a huge challenge for regulatory body to strengthen their AML/CFT regulation in combating money laundering. Thus, enhancing the procedure of customer due diligence that suits the nature of cryptocurrencies can be the key to combat money laundering. Integrating anti-money laundering risk analysis as well as alert and reporting mechanisms into blockchain technology will allow a greater supervision of cryptocurrencies however, this will come with a huge cost and affect the anonymity features of cryptocurrencies.

The rise of the usage of crypto money is due to technology advancements however, as a law-abiding citizen, such technology enhanced payments system while at the same time evade the controls from enforcements bodies will facilitates financial crime at a greater scale of law enforcement agencies foes not address this issue in timely manner. Customer due diligence process may be insignificant procedures that took place to collect the customers' information at the first point of sales however, by having competent personnel as CDD officer will definitely reduce the risk of financial institution from becoming the vehicles of money laundering activities.

Moreover, CDD in the era of cryptocurrency should be comprehensive and identification of the red flags should be at the tips of their fingers and in order to achieve this, financial institution should provide their staff with continuous training to ensure they are updated with the latest requirements, rules and regulations governing cryptocurrency exchanger. In the nutshell, despite the challenges face by anti-money laundering enforcement bodies to address this matter, focusing on the basic of detection processes which is customer due diligence processes is vital in order to safeguard the organization from being exploited by the sophisticated criminals for their illegal proceeds of crime.

REFERENCES

[1] Z. Hamin, N. Omar and M.A. Hakim, "Implications of forfeiting property in money laundering cases in Malaysia," Journal Of Money Laundering Control, vol. 20, no. 4, pp. 334-344, 2017.

[2] Anti-Money Laundering, AntiTerrorism Financing and Proceeds of Unlawful Activities Act 2001.

[3] M. Salvo, Corruption and Money Laundering as a Threat to Financial Stability: 'Lava Jato' Case Study [Online] Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2788735, 2016.

[4] A. Aluko and M. Bagheri, "The impact of money laundering on economic and financial stability and on political development in developing countries," Journal Of Money Laundering Control, vol. 15, no. 4, pp. 442-457, 2012.

[5] M. Salomon and J. Spanjers, Illicit Financial Flows to and from Developing Countries: 2005-2014 [Ebook] (7th ed.). Creative Commons Attribution License [Online] Retrieved from https://www.gfintegrity.org/wp-content/uploads/2017/05/GFI-IFF-Report-2017_final.pdf, 2017.

[6] UNODC, The Drug Problem And Organized Crime, Illicit Financial Flows, Corruption And Terrorism [Online] retrieved from: htps://www.unodc.org/wdr2017/field/Booklet_5_NEXUS.pdf, 2017.

[7] D. Demetis, "Fighting money laundering with technology: A case study of Bank X in the UK," Decision Support Systems, vol. 105, pp. 96-107, 2017.

[8] AML/CFT, [Online] Retrieved from http://amlcft.bnm.gov.my/, 2018.

[9] European Central Bank, [Ebook] (pp. 13-18). Frankfurt am Main, Germany [Online] Retrieved from https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf, 2012.

[10] J. Liang, L. Li, and D. Zeng, "Evolutionary dynamics of cryptocurrency transaction networks: An empirical study," PLOS ONE, vol. 13, no. 8, 2018.

[11] J. Chiu and T. Koeppl, "The Economics of Cryptocurrencies Bitcoin and Beyond," SSRN Electronic Journal, pp. 1-10, 2017.

[12] Bank of International Settlements, Annual Economic Report 2018 [Ebook] [Online] Retrieved from https://www.bis.org/publ/arpdf/ar2018e.pdf, 2018.

[13] D. ryans, "Bitcoin and Money Laundering: Mining for an Effective Solution," Indiana Law Journal, vol. 89, no. 1, pp. 1-10. 2017.

[14] R.V. Wegberg, J. Oerlemans and O. van Deventer, "Bitcoin money laundering: mixed results? An explorative study on money laundering of cybercrime proceeds using bitcoin," Journal of Financial Crime, vol. 25, no. 2, pp. 419-432, 2018.

[15] A. Viswanatha, U.S. officials: virtual currencies vulnerable to money laundering [Online] Retrieved from https://www.reuters.com/article/us-senate-virtualcurrency/virtual-currencies-vulnerable-to-money-laundering-u-s-justice-idUSBRE9AH0P120131118, 2018.

[16] S. Mabunda, "Cryptocurrency: The New Face of Cyber Money Laundering," 2018 International Conference On Advances In Big Data, Computing And Data Communication Systems (Icabcd), 2018.

[17] CipherTrace, Cryptocurrency Anti-Money Laundering Report. CipherTrace [Online] Retrieved from https://info.ciphertrace.com/crypto-aml-report-q218, 2018.

[18] Network Security, "Silk Road online drug market taken down," Network Security, 2013(10), pp. 1-2, 2013.

[19] P. Sprenger and F. Balsiger, Anti-Money Laundering in times of Cryptocurrencies. [Online] Retrieved from https://assets.kpmg.com/content/dam/kpmg/ch/pdf/anti-money-laundering-in-times-of-cryptocurrency.pdf, 2018.

[20] Standard Guidelines on Anti-Money Laundering and Counter Financing of Terrorism. (2013). [Ebook]

[21] Y. Isa, Z. Sanusi, M. Haniff and P. Barnes, "Money Laundering Risk: From the Bankers' and Regulators Perspectives," Procedia Economics And Finance, vol. 28, pp. 7-13, 2015.

[22] A. Viswanatha and B. Wolf, HSBC to pay $1.9 billion U.S. fine in money-laundering case [Online] Retrieved from https://www.reuters.com/article/us-hsbc-probe/hsbc-to-pay-1-9-billion-u-s-fine-in-money-laundering-case-idUSBRE8BA05M20121211, 2012.

[23] N. Mugarura, "Customer due diligence (CDD) mandate and the propensity of its application as a global AML paradigm," Journal Of Money Laundering Control, vol. 17, no. 1, pp. 76-95, 2012.

[24] FATF, Transparency And Beneficial Ownership [Online] Retrieved from http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-transparency-beneficial-ownership.pdf, 2014.

[25] Revealing the True Cost of Financial Crime, Thomson Reuters Risk. Management Solutions, 2018.

[26] G. Jurva, KYC in the Digital Age: Cryptocurrencies, PEPs and Due Diligence [Online] Retrieved from http://www.legalexecutiveinstitute.com/kyc-in-the-digital-age-q-a-2/, 2018.

[27] C. Kim and C. Yoo, Bitcoin tumbles as hackers hit South Korean exchange Coinrail [Online] Retrieved from https://www.reuters.com/article/us-markets-bitcoin-korea/bitcoin-tumbles-as-hackers-hit-south-korean-exchange-coinrail-idUSKBN1J703I, 2018.

[28] Bank Negara Malaysia, Bank Negara Malaysia issues policy document for digital currencies [Online] Retrieved from http://www.bnm.gov.my/index.php?ch=en_press&pg=en_press&ac=4628&lang=en, 2018.

[29] FATF, Guidance For A Risk-Based Approach. Retrieved from https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf, 2018.