Journal of Social and Development Sciences (ISSN 2221-1152)
Vol. 6, No. 3, pp. 35-42, September 2015

Why Does New Payment System and Products (NPSPs) Vulnerable to Money Laundering?

Go Lisanawati
University of Surabaya (UBAYA), East Java, Indonesia
lisanawatigo@gmail.com

Abstract: This paper will assess on the impact of the newest development on payment systems, which has been manifested in such kinds of payments products and threatening through money laundering. In order to increase the quality of people' lives in this technologically advanced era, many sophisticated products have been produced, such as virtual currencies, or other stored value cards. The anonymity characteristic of new payment systems and products is vulnerable to money laundering exploitation. The study of FATF, as reported by APG, shows that the AML/CFT risk has associated with the payment method (means as virtual currencies). There are some reason which may indicate the potentiality of AML/CFT. (APG, 2014). As a part of Scientific Research, this legal research will be using qualitative methods. It will assess on the implementation of virtual currencies in real world which is causing problem for anti money laundering. It is a doctrinal research and using conceptual approach to solve the problem. The result of this research shows that anti money laundering rules and regulation should be strictly implemented to virtual currencies's problem in order to anticipate its vulnerabililty to money laundering. The Due Diligence should be developed further.

Keywords: *New Payment System, Payment Products, Payment Services, Anti Money Laundering Approach*

1. Introduction

In its development nowadays, virtual currencies plays an important role to the payment system in the entire world. The problem of easiness and faster movement has been approved as the major reasons. The concept of virtual currencies is defined by the FATF as below:
A digital representation of value that can be digitally traded and functions as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but does not have legal tender status (i.e when tendered to a creditor, is a valid and legal offer of payment) in any jurisdiction. It is not issued nor guaranteed by any jurisdiction, and fulfills the above functions only by agreement within the community of users (underline by author) of the virtual currency. Virtual currency is distinghuised from flat currency (a.k.a "real currency", "real money", or "national currency"), which is the coin or paper money of a country that is designated as its legal tender; circulates; and is customarily used and accepted as a medium of exchange in the issuing country. It is distict from e-money, which is a digital representation of fiat currency used to electronically transfer value dominated in fiat currency. E-money is a digital transfer mechanism for fiat currency – i.e it electronically transfers value that has legal tender status. (FATF Reports, 2014)

The International standards on combating money laundering and the financing of terrorism and proliferation through the FATF Recommendation 14, mentioned:
Countries should take measures to ensure that natural or legal persons that provide money or value transfer services (MVTS) are licensed or registered, and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations. Countries should take action to identify natural or legal persons that carry out MVTS without license or registration, and to apply appropriate sanctions. Any natural or legal person working as an agent should also be licensed or registered by a competent authority, or the MVTS provider should maintain a current list of its agents accessible by competent authorities in the countries in which the MVTS provider and its agent operate. Countries should take measures to ensure that MVTS providers that use agents include them in their AML/CFT programmes and monitor them for compliance with these programmes.

The Recommendation 14 of FATF Recommendation (2012) above explain the system of money transfer in ordinary systems of a country as payment system. Countries should pay attention on the identification process. In the interpretative note Recommendation 14 then mention:
A country need not impose a separate licensing or registration system with respect to natural or legal persons already licensed or registered as financial institutions (as defined by the FATF Recommendations) within that country, which, under such license or registration, are permitted to perform money or value transfr services, and which are already subject to the full range of applicable obligations under the FATF Recommendations.

Recommendation 14 is still facing a difficulty to impose Hawala systems and other systems similar with Hawala, since it is not yet licensed or registrated. Inter alia with Recommendation 15 of the FATF Recommendation (2012), which explained:
Countries and financial institution should identify and assess the money laundering or terrorist financing risks that may arise in relation to (a) the development of new products and new business practices, including new delivery mechanism, and (b) the use of new or developing technologies for both new and pre-existing products. In the case of financial institutions, such a risk assessment should take place prior to the launch of the new products, business practices or the use of new or developing technologies. They should take appropriate measures to manage and mitigate those risks.

These Recommendation 15 mention about the exploration of new development technologies that may impact to the payment systems mechanism. More products will develop in order to fulfill the society's needed. As mentioned in the definition of virtual currency given by the FATF above, the existence of virtual currency in the world depends on the society. Bitcoin, in particular, as a major virtual currency form in society, has been attracting attention. Bitcoin is a payment based on internet. The problem of internet based crime is also an arising problem beside the problem of money laundering. Other is Liberty reserve payment system as a currency exchange. Both of Bitcoin and Liberty Reserve are actually arising problems of money laundering. In 2013, there was an indictment for an online currency exchange. Liberty Reserve was accused with laundering of $ 6 billion. Santora et al. (2013) mentioned: "The operator of a global currency exchange ran a $6 billion money laundering operation online, a central hub for criminals trafficking in everything from stolen identities to child pornography". In 2014, there was a charge for the Vice Chairman of the Bitcoin Foundation by U.S. Prosecutors in conspiring to commit money laundering. The founder was helping to funnel cash to illict online drugs bazaar Silk Road (Emily, 2014). Money laundering itself is understood as an organized crime applied in complicated process of hiding illict money that criminal gains in predicate crime. This process of crime is difficult to solve and enforce. Bitcoin and Liberty reserve has just shown that money laundering can be done in the process of exchange of virtual currency, with or without being realized by people. This working paper will assess on how the characteristic of new payment system through virtual currencies arouse problem in money laundering, one of the biggest crime in the world, and seek the solution in order to stop money laundering.

2. Methodology

As a part of Scientific research, legal research should fit to the scientific requirement on research methodology in order to seek the true answer of a problem. Since law was understood in the perspectives of epistemology as "norm" and "nomos", law is also multi interpretative. There is no single concept about what is law. But the existence of law as it is in society will be important to be noticed. Wignjosubroto (2009) in further explains that:
Kelak dalam kajian-kajian sains, canon of difference akan lebih sering atau lebih banyak dijadikan dasar penelitian eksperimental (dalam sains alam dan hayat) atau kuasi-eksperimental (dalam sains sosial) untuk menguji atau menemukan ada tidaknya hubungan kausal antara dua variabel.
Studi-studi tentang hubungan antara sebab (kausa) dan akibat (efek) memang merupakan bagian yang betul-betul penting dan mengambil porsi yang diperkenalkan John Stuart Mill, Jr ini memang dimaksudkan untuk mengefektifkan silogisma induksi untuk kepentingan sains yang lebih praktis...
(Free translation: In the future of science study, canon of difference will be more considered as basis of experimental research (in natural science) or quasi-experimental (in social science) to examine or to find whether there is causal relationship between two variables or not.

The study of cause and effect relationship is the important part and took an important portion as introduced by John Stuart Mill, Jr is purposed to make inductive silogism to practical science effectively...) In this context, the legal research will use conceptual approach to find the answer. Even though using empirical research method, but the existences of legal research as normative research method should has its identity. Further P. Casws, as quoted by Ibrahim (2006), mention: "The difference between the various sciences, then, are not essentially differences; there is a genuine logical and methodological unity underlying their apparent diversity". Thus a normative legal research remain able to continue with empirical research supplement without changing its identity of normative science into empirical science but should keep its genuine logical and methodological.

3. The Threat and Strength of Virtual Currencies as a Modality to Exist

Virtual currencies got technological support in its operation. It means that high technology will be supporting the activity of value exchanges. Bryan (2014) explained:
Technology forges ahead at a rapid pace, whether we like it or not. Criminals recognize the inevitability and use technological improvements to advance their craft, committing crimes from half a world way in real time. Meticolous criminals also use technological advancements to distance themselves from their illegal activities and profits through use of virtual banking and electronic money transfer systems, which allow criminals to buy, sell, and exchange goods without any physical interaction. Through such services use digital logs that serve to identify a sender and a receiver's digital identies, criminals possess the means to obfuscate their digital identity by simply spoofing their Internet Protocol address or by using another individual's account, essentially making their activities untraceable.

Bryan's explanation above shows that sophisticated technology is the perfect support for criminals to explore their criminal activity "safely" and "productively". It means the technological advancement will arise perfect crime in this globalization era. As it's understood, in globalization era technological advancement plays an important role. Thus every people will say that techology is their friend. Internet is living closely to them. Hence, Rothe & Friedrichs (2015) warns that there is a challenge to defining what is crime, as below:
For some criminologist, the term "crime" itself is inevitably so limiting and so constrained by its historical meaning that it should be abandoned in favor of "social harm" as the focus of our concern, with criminology itself being replaced by "zemiology" or the study of harm. The social harm initiative usefully calls for reconsideration of how we think about crime, but has some limitation as well if it abandons the concept of crime itself.

Smith et al. (2004) then explain about 4 (four) formidable challenges of crime in the context of cyber crime, as:

This transnational dimension of cyber crime poses four formidable challenges for prosecutors, especially those who may be involved from an early stage of investigations. The first is simply to determine whether the conduct in question is criminal in their own jurisdiction.... The second challenge is to assemble sufficient evidence to mobilise the law, that is, to obtain appropriate judicial authority for a physical search.... The third challenge is to identify the perpetrator, and to determine where he or she is physically located... Finally, there remains the decision of whether to leave the matter to authorities in the country where the suspect is physically situated...
Once again technology shows its strength to be a perfect friend to people in its development. But technology has also arise as a perfect enemy to people through the exploration of its advancement by criminals. Technology is also arising as a perfect enemy in the future.

Virtual currencies in its existence shows the need of high techological support to do every kind of activities. The FATF has mentioned also that:
While the NPPS Guidance broadly addressed internet-based payment system, it did not define "digital currency", "virtual currency" or "electronic money". Nor did it focus on virtual currencies, as distinct from internet-based payment systems that facilitate transactions denominated in real money (fiat or national currency) (e.g. Pay-pal, Alipay, or Google Checkout). It also did not addressed decentralised convertible virtual currencies, such as Bitcoin...

A common set of terms reflecting how virtual currencies operate is a crucial first step to enable government officials, law enforcement, and private sector entities to analyse the potential AML/CFT risks of virtual currencies as a new payment method...

Since the internet will be the best supporter, it should has strong regulation in technology operation. Bryans (2014) further has warned also that virtual currency has been accepted and get respected by society, even though it is different from the ordinary payment transfer using fiat currency. The FATF (2014) shows:
In a short period of time, virtual currencies, such as Bitcoin, have developed into a powerful payment method with ever growing global acceptance. Virtual currencies offer an innovative, cheap and flexible method of payment. At the same time, the unique and often unfamiliar business model of virtual currencies poses a challenge to regulators around the world who are unsure how to deal with this payment method. The policy responses vary considerably, with some countries embracing this new technology and others severely or totally limiting its legitimate use. The FATF conducted research into the characteristics of virtual currencies to make a preliminary assessment of the ML/TF risk associated with this payment method. An important step in assessing the risks and developing an appropriate response is to have a clear understanding of the various types of virtual currencies and how they are controlled and used.

Virtual currencies have been developed well globally through its innovation, flexibility, and cheap costs. APG (2014) in its yearly typologies report about methods and trends of money laundering and terrorism financing explain: "the legitimate use of virtual currencies offers many benefits such as increased payment efficiency and lower transaction costs. Virtual currencies facilitate international payments and have the potential to provide payment services to populations that do not have access or limited access to regular banking services". Hence, the benefit of virtual currencies will attracted society to keep this virtual currencies method as a new payment system as center of payment system nowadays. As a payment system, Virtual currencies will give benefit to people who want easiness in their transaction. Virtual currencies are also anonym. Since it is internet based, most of the transaction in internet are anonym because everyone can have their identity in internet. It is pseudonymous and mostly peer-to peer transaction between networking.

There are two types of virtual currencies as defined by the FATF (2014), as convertible virtual currency and non-convertible virtual currencies. The convertible virtual currencies is an open virtual currencies which has equivalent value in real currency. It can be changed back and forth for real currency, that needs the participatory of private people to offers and accepts the exchange offering. The convertible virtual currencies here is including Bitcoin, e-Gold, Liberty Reserve, Second Life Linden Dollars, and WebMoney. While non-convertible virtual currencies can be understood as a closed virtual currencies which is intended to be specific to a particular virtual domain or world. It can not be used as fiat currency exchange. The example here is including Q coins, Project of Entropia Dollars, or World of Warcraft Gold. This paper will be underlining the virtual currencies only in the context as open virtual currencies. Other is virtual currencies dividing into centralised virtual currencies and decentralised virtual currencies. The term of centralised means the system will have one single administrating authority, such as the participatory of third party to control the system, and also controlling the exchange rate, etc. while decentralised virtual currencies is uncentralised control and monitoring of administration. It is using cryptography to protect the system. In a diagram, virtual currencies can be classified in its taxonomy as described by the FATF (2014):

Figure 1: Taxonomy of Virtual Currencies

	Centralised	**Decentralised**
Convertible	Administrator, exchangers, users, third-party ledger, can be exchanged for fiat currency. Example WebMoney	Exchangers, users (no administrator); no Trusted Third-Party ledger, can be exchanged for fiat currency. Example Bitcoin
Non-convertible	Administrator, exchangers, users; third-party ledger, cannot be exchanged for fiat currency. Example: World of Warcraft Gold	Does not exist

The characteristic of Virtual Currencies as researched by the FATF that endanger AML/CFT regimes, are:

- The anonymity provided by the trade in virtual currencies on the internet

- The limited identification and verification of participants
- The lack of clarity regarding the responsibility for AML/CFT compliance, supervision and enforcement for these transactions that are segmented across several countries
- The lack of a central oversight body

According to the characteristic above it can be understood that the strength of virtual currencies for criminals has become risks for law enforcement officer and people who are indirectly involved in the money laundering processess. Since virtual currencies can be traded on the internet, it is emerging a characteristic of non face to face customer type. There is no relationship between the trader. The FATF (2014) also mentioned that they "may permit anonymous funding (cask funding or third party funding through exchangers that do not properly identify the funding source). They may also permit anonymous transfers, if sender and recipient are not adequately identified". Other vulnerability came from the accessibility of Virtual Reserve that easily accessed through internet including mobile phones accesses. It is easy to move out the funds or value cross border and make it as payments and transfers. the holder of transaction records can be held by different entities. So, it is arising difficulties to implement AML/CFT compliance which is depending to the jurisdiction.
Liberty Reserve as one of the open virtual currencies is a centralised virtual currency service. Wikipedia (2015) explains:

Based in San Jose Costa Rica, Liberty Reserve was a centralised digital currency service that allowed users to register and transfer money to other users with only a name, e-mail, address, and birth date. No efforts were made by the site to verify identities of its users, making it an attractive payment processor to scam artists. Deposits could be made through third parties using a credit card or bankwire, among other deposit options. Liberty Reserve did not directly process deposits or withdrawals. Deposits funds were tied to the value of the US Dollar and the euro respectively, or to ounces of gold. No limits were placed on transaction sizes. The service made money by charging a small fee, about 1%, on each transfer. Transactions were "100% irrevocable" . Liberty Reserves also offered shopping cart functionality and other merchant services.

According to the description given by wikipedia above show that the use of Liberty Reserves is very easy, cheap, and without control. There is no limitation of transaction also. Liberty Reserve in its jargon mentioned that it is "the oldest, safest and most payment processor which is serving millions all around the world". Since it does not has control in the person who use the service, Liberty Reserves does not have control to request the sources of money people transfer too, whether it is an illegal or a legal source. In 2006, there was an indictement for U.S Businessman named Arthur Budovsky and Vladimir Kats with charges of operating an illegal financial business. Liberty Reserve is identified also as a virtual currency payment system which does not has good of transperancy mechanism. Wikipedia (2015) is explaining also that "in 2011, Liberty Reserve was linked to (unrelated) attempts to sell thousands of stolen Australian bank account numbers and British bank cards. In 2012, a group of hackers attempts to blackmail anto-virus software company symantec into transferring $50,000 into Liberty Reserve account". In 2014, Liberty Reserve once again was charged with criminal trafficking, and stolen identities to child pornography. Liberty Reserves can be a medium to do money laundering. It is difficult to identify the identity of the sender and/or the receiver, and also the source of the funds that has been transferred by both parties. Even though Liberty Reserve is centralised system, but it is still lacking in security and undetected criminal and illicit fund's gained.

Bitcoin, as one of the biggest and wellknown new payment system method nowadays has been arising a new threat for law enforcement schemes. As defined from CoinDesk (2015), Bitcoin is "a form of digital currency, created and held electronically. No one controls it. Bitcoin aren't printed, like dollars or euros – they've produced by people, and increasingly business, running computers all around the world, using software...". as its characteristic as decentralized system, it might caused difficulties to regulate. There is no single organisation or institution which can controls the network of Bitcoin itself, even banks can not control it either. Other is that the holder of Bitcoin can buy things electronically. There are some charactersitic of Bitcoin that explained in CoinDesk (2015), such as: Decentralised, easy to set up, anonymous, completely transparent, cheap fees, fast transaction, non repudiable transaction. Bryans (2014) then describe Bitcoin as:
Bitcoin is a decentralized, virtually anonymous (commonly called pseudonymous), peer to peer (transactions occur directly between users) network. Bitcoin's decentralization and peer to peer infrastructure allows it to be virtually immune to the risks of server raids or the loss of a central database to hackers. Due to possibility

of its use for nefarious activities such as money laundering, Bitcoin's pseudonymous network negatively impacted the image of emerging virtual currency systems, and some authorities view Bitcoin solely as a platform for criminals. Whatever the perceived or potential economic role may be for Bitcoin...
Bitcoin transactions begins when a buyer transmits a quantity of bitcoins from his or her personal digital wallet through a Bitcoin client to the coded Bitcoin address representing the seller's digital wallet. The Bitcoin network processess the transaction and adds the value and each node (called a miner). Miners then encode this "block" of recently broadcast transmissions onto the end of all the previous completed blocks. The explanation above has implicitly mention that law enforcement of money laundering will face difficulties to handle it due to the characteristic of technological support, and may hiding illicit gain through personal device as digital wallet. It is simply easy to be handed by the criminals to hide it. No control of financial institutions nor regulation. When Bitcoin being a case for money laundering, it was identified that the offender of Bitcoin was linked its activity through Silk Road, and then transferring funds to receiver's account at an unidentified bitcoin exchange service.

Organized Crime and The Vulnerability in Money Laundering's Stages: Money laundering as normally understood is a proceeds of crime. The money or assets that derived from criminal activity will be laundered through some activities by the criminals in order to get the "clean" money. Stessens (2000) explain the process of money laundering as: "Criminals who, through their criminal activities, dispose of huge amounts of money, need to give this money a legitimate appearances: they need to 'launder' it. The phenomenon of money laundering is essentiality aimed at two goals: preventing 'dirty money' from serving the crimes that generated it, and ensuring that the money can be used without any danger of confiscation." It mean that money laundering needs more aggressive activity in hiding illicit funds or assets that has been gained by criminals. Chaikin, as quoted by Garnasih (2003), explains:
A significant portion of money laundering for illegal purposes is carried out at the instigation of organized criminal group. Money laundering is the lifeblood of organized crime. It prevents the detection and punishment of those most responsible for directing and financing the criminal organization. Person at the top of organization is insulted from the physical acts of the crime, making them extremely difficult to investigate, let alone prosecute. Often the money organization and the crime itself. Here is Achilles' heel of the financiers of crime

Money laundering as a part of organized crime can cause another problem. It can create an organized financial crime and also being transnational crime. In this sense, Schneider (2012) mention: "The revenues of organized crime are scientifically extremely difficult to tackle. Organized crime is defined different and vary from country to country... To fight against organized crime is extremely difficult, as there are no efficient and powerful international organizations that can effectively fight against organized crime". As transnational crime, Boister (2012) warns that "At a broader economic level, transnational crime causes harm by compromising financial and commercial institutions, making economic management difficult..." Money laundering harms economical aspects either. The cooperation of technology advancement and criminal minded organization will endangering country.

In money laundering's steps, there are Placement; Layering; and Integration stage. Virtual currencies misuse can be done in each of stages of money laundering, from Placement, Layering until Integration. Bryans (2014) mentioned that "New virtual currencies, such as Bitcoin, add yet layer of anonymity by allowing users to transfer to transfer value without the collection of any personally identifiable information". In the placement steps, it is understood that so many transactions can take place into the Internet every hour. In the layering stage, criminals can transfer any value easily. The transaction is untraceable also. Inter alia with the explanation mentioned above, the characteristic of virtual currencies is anonymous. It is not face to face based transaction. The sender and the receiver can deal with their own agreement to transfer money, yet there is no regulation which can control their activity. Other vulnerable steps is in Integration step. It is not easy to distinct whether as a buyer in Bitcoin, they won't get a money laundering process coin or seller. It is difficult to recognise whether the Bitcoin is converting from any illegal activity or not, or it buy or sell by criminals offender. Through virtual currencies, there will be increased total amount of money that will be laundered. It will be easy also when criminals in join hands with other criminals to launder dirty money, and through transnational network, the transfer can be done in any jurisdiction without holding the physical money or coin as a physical assets. Richet (2013) has also warned that there is cybercriminal's methods

which can assist laundering money through online. Further, Richet (2013) explain that in Liberty Reserve, illicit money that were acquired by fraud, carding, will be connected to an exchanger, and change the form of money, from dollar to LR currency, and put in the Liberty Reserve account. The result is that the money is already laundered and integrated to prepaid cards, VCC, or using Western Union. Bitcoin is having a major problem also. It is that every transaction in bitcoin is public. Anyone can follow the moved coins between buyer and seller. Then it cause a difficulty to mention where is the coin came from after the proses of hiding, concealing, and integration happen. Virtual Currencies in its development, potentially explored by legitimate and/or criminal mind users to do transfer money fast, no high cost, no barriers to entry, and mostly anonymous.

Due Diligence, Registered Virtual Currency Possibility To Be Implemented: The FATF 2012 in its Recommendation has put Due Diligence responsibility to any institution in order to prevent money laundering. There are Customer Due Diligence (CDD) and Enhance Due Diligence (EDD). Recommendation 9 of Prevent Measure, states that "Financial Institutions should be prohibited from keeping anonymous accounts or accounts in obviously fictious names". The problem will arise regarding to the anonymous characteristic of virtual currencies. The buyer and the seller won't be physically in touch to deal with the money, etc. The CDD is the simple verificiation of customer's identity, which should be taken as a measurement in 4 (four) conditions, those are: Establishing business relations; Carrying out occasional transactions: (i) above the applicable designated threshold (UD/EUR 15,000); or (ii). That are wire transfers in the circumstances; there is a suspicious of money laundering or terrorist financing; or the financial institution has doubts the veracity or adequacy of previously obtained customer identification data.

Regarding with virtual currencies, the existence of CDD is not easy to solve. But as now as people know there is a legal problem related with virtual currencies, the founder, other third party, seller, and/or buyer should be profiling their identity. The regulation must be set out and all the record should be kept since virtual currencies is vulnerable to money laundering. It is a must to create system that may verify the customer's identity. The verification system can be using any cryptography methods, as well known in cyber. The principle of cyber of non-repudiation should be implemented. No one can deny that they are doing any transaction in internet. The CDD is not only for identifying and verifying customer's identity, but also understanding and obtaining information on the purpose and intended nature of the business relationship, and ensuring the customer's detail business and risk profile, and requirement of stating the funds of transfer. The FATF then request financial institution through Risk Based Approach, has been trying to identify the risks that may appear in regard with money laundering scheme. The EDD does deep verification process in the specific circumstances, like when transaction is done by Politically Exposed Persons, or other transaction. Even though in the context of virtual currencies is under special circumstances, but both CDD and EDD should be forced to be implemented.

Other responsibility that has been pushed by the FATF, is about the Record Keeping implementation. The record keeping here is related with the record of any individual transaction, account files of customer, stc. Jeffrey Sparshott in the Wall Street Journal (2013), headlining "Web Money Gets Laundering Rule". In its news, the contributor mention that the U.S is applying money laundering rules to "virtual currencies". There is new forms of cash bought in the Internet are being used to fund illicit activities. The regulation covers the obligation of institution that issued or exchanged online cash transaction above US$ 10,000 should reporting the transaction to the authority, and also fulfill the requirement to do book keeping. The regulation is also regulating that the institution that receive legal tender in exchange for online currencies or anyone conducting a transaction on someone's behalf, would be subject to new scrutiny. They should monitor the transaction.

There are 3 (three) regulation given by AML program. Each of them will meet with the requirements of: Implemeting strictly of customer identification, verification and implement automated transaction monitoring policies and procedures; They should be protection, processess, visibility and reporting to build and maintain partnership; and Save money and time. Hence Personal identification and verification should be implemented, and protected from identity theft. The U.S creates the rules needed to monitoring and analysing transactions in real time, or over specific periods of time, to detect money movements that could be associated with laundering activity. The regulation also force virtual currency exchanges to implement the

same regulation as implemented for traditional financial institution. Since some of the virtual currency provider are decentralised and unregistered virtual currency exchanger, then each nation should make regulation that the exchanger should be centralised and registered. At least it will minimize the risk of money laundering exploitation through virtual currency. The regulation should be having a sanction imposed mechanism also to be implemented to anyone (buyer, seller, third party, or the exchanger itself) who did not fulfill the requirement. It needs an International cooperation between countries through regulating the same methods and mechanism that will be implemented for virtual currencies exchanger.

4. Solution

Virtual currencies is vulnerable to money laundering problems. It is based on the characteristic that were found in the virtual currencies. Since it is an internet based payment, therefore the virtual currencies offer easiness to people to gain money. Its anonynimity of identity of both parties triggered an exploitation of money laundering. Then mechanism of CDD, EDD, record keeping, and other specific regulation designated to prevent money laundering should be implemented.

Recommendation: Virtual currency should be developed more wider but containing safety to the users. It is not about how to fulfill the needs of society regarding the newest issues, but more than that, the safety transaction should be protected. Law enforcement agents should strictly imposed any violation with strict and proper sanction.

References

APG. (2014). APG Yearly Typologies Report 2014: Methods and trends of Money Laundering and Terrorism Financing. APG Secretariat: Australia, 10.

Boister, N. (2012). An Introduction To Transnational Criminal Law. London: Oxford, 7.

Bryans, D. (2014). Bitcoin and Money Laundering: Mining for an Effective Solution, Article. *Indiana Law Journal*, 89(441), 443-444.

Emily, F. (2014). Prominent Bitcoin entrepreneur charged with money laundering. Retrieved from http://www.reuters.com.

FATF Report. (2014). Virtual Currencies: Key Definitions and Potential AML/CFT Risk., Retrieved from: http://www.fatf-gafi.org.

Garnasih, Y. (2003). Kriminalisasi Pencucian Uang (Money Laundering). Jakarta: Universitas Indonesia, 52.

Ibrahim, J. (2006). Teori & Metodologi Penelitian Hukum Normatif. Malang: Bayumedia Publishing, 147.

Richet, J. L. (2013). Laundering Money Online: A review of Cybercriminals' Methods, retreived from http://arxiv.org/ftp/arxiv/papers/1310/1310.2368.pdf.

Rothe, D. L. & Friedrichs, D. O. (2015). Crimes of Globalization: New Directions in Critical Criminology, London: Routledge, 16.

Santora, M., Rashbaum, W. K. & Perleroth, N. (2013). Online Currency Exchange Accused of Laundering $6 Billion, retrieved from: http://www.nytimes.com/2013/05/29/nyregion/liberty-reserve-operators-accused-of-money-laundering.html?_r=0.

Schneider, F. (2012). The Hidden Financial Flows of Organized Crime: A Literature Review and Some Preliminary Empirical Results in (2012). Illicit Trade and The Global Economy. C.C. Storti & P.D. Grauwe (eds). London: Cambridge, 44.

Smith, R. G., Grabosky, P. & Urbas, G. (2006). Cyber Criminals on Trial. Australia: Cambridge University Press, pp. 48-49.

Stessens, G. (2000). Money Laundering: A New International Law Enforcement Model. United Kingdom: Cambridge, 5.

Wignjosubroto, S. (2009). Penelitian Hukum dan Hakikatnya Sebagai Penelitian Ilmiah", in S. Irianto & Shidarta (Eds), Metode Penelitian Hukum: Konstelasi dan Refleksi, Jakarta: Yayasan Obor Indonesia, pp. 114-115.

www.CoinDesk.com.

www.identitymindglobal.com/bitcoin.

www.wikipedia.com.