



**ANTI-MONEY LAUNDERING AGAINST VIRTUAL
CURRENCY IN CASE OF USING BITCOIN**

BY

MR. PRATYA APAIYANUKORN

**A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF
THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF LAWS IN BUSINESS LAWS (ENGLISH PROGRAM)**

**FACULTY OF LAW
THAMMASAT UNIVERSITY**

ACADEMIC YEAR 2015

COPYRIGHT OF THAMMASAT UNIVERSITY

**ANTI-MONEY LAUNDERING AGAINST VIRTUAL
CURRENCY IN CASE OF USING BITCOIN**

BY

MR. PRATYA APAIYANUKORN

**A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF
THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF LAWS IN BUSINESS LAWS (ENGLISH PROGRAM)**

FACULTY OF LAW

THAMMASAT UNIVERSITY

ACADEMIC YEAR 2015

COPYRIGHT OF THAMMASAT UNIVERSITY



THAMMASAT UNIVERSITY
FACULTY OF LAW

THESIS

BY

MR. PRATYA APAIYANUKORN

ENTITLED

ANTI-MONEY LAUNDERING AGAINST VIRTUAL CURRENCY
IN CASE OF USING BITCOIN

was approved as partial fulfillment of the requirements for
the degree of Master of Laws in Business Laws
(English Program)

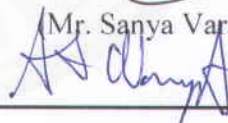
on August 11, 2016

Chairman



Mr. Sanya Varanyu

Member and Advisor



(Professor Amnat Wongbandit, D.Jur)

Member



(Associate Professor Pokpong Srisanit, D.enD)

Member



(Assistant Professor Nilubol Lertnuwat, Ph.D.)

Dean



(Professor Udom Rathamarit, Docteur en droit)

Thesis Title	ANTI-MONEY LAUNDERING AGAINST VIRTUAL CURRENCY IN CASE OF USING BITCOIN
Author	Mr. Pratyapa Apaiyanukorn
Degree	Master of Laws
Major Field/Faculty/University	Business Law (English Program) Faculty of Law Thammasat University
Thesis Advisor	Professor Amnat Wongbandit, D.Jur
Academic Years	2015

ABSTRACT

Anti-Money Laundering is a set of rules and guidelines designed and agreed among countries to use as standard policies and framework in establishing their domestic laws on prevention and suppression of money laundering activities. The expansion of the financial sector and businesses brings about the continuous development of innovative and new financial instruments to facilitate the businesses. In parallel with this development, criminals also take advantages of the unfamiliarity to the newly developed innovation and create new money laundering methods. In this circumstance, and whilst the financial sector is a foundation of the national economic, the government and relevant state authorities have to monitor closely and supervise such new innovations.

Among other innovations, virtual currency is created to facilitate financial transactions. It was found that virtual currency is the new financial innovation and also the system that used to connect with the customers through the online network via the internet. The key points of this currency are the description of it which are anonymous account and the system used in the transaction which is the peer-to-peer or blockchain connection system. These features are different from the standard financial instruments such as fiat currencies, financial institution, bank and non-bank business.

The virtual currency is considerably new in Thailand. To date, the laws have not been developed to effectively govern the transactions using the said virtual

currency. Exchangers, administrators, and users of the virtual currency are not within the scope of governance of the Anti-Money Laundering Act; nor are they subject to any other regulations. That is to say, the Anti-Money Laundering Act, including rules, regulations and guidelines established thereunder, only regulates performances of financial institutions and some other businesses as specifically determined. In other words, obligations and requirements under the Anti-Money Laundering laws do not apply to the virtual currency transactions and/or the involving parties. Thus, there are certain loopholes for some criminals to use the virtual currency instead of money in various financial transactions to avoid detection by the state authorities. Lacking of government supervision in this part leads to a new risk of money laundering through the virtual currency.

This thesis studies the Anti-Money Laundering processes in the United States in comparison with those in Thailand, specifically focussing on the issues of money laundering using a kind of virtual currency: Bitcoin. Bitcoin is the most prevalent kind of virtual currency and is addressed widely and extensively in US laws, regulations and court judgments. Those laws can be useful guidelines for Thailand to develop its appropriate solutions for the problem of money laundering through the virtual currency.

The key preventive measures under the Anti-Money Laundering Act are customers profile verification and transactions monitoring and recording. These measures are the essential procedures to control and monitor transactions to reduce the risk of money laundering. Also, it can also examine the suspicious transactions or suspect profiles of each customer. These methods could apply to the virtual currency and their relating business for supervision and manage the risk of money laundering as same as the other financial business under the Anti-Money Laundering law and regulation.

Keywords: Virtual Currency, Crypto Currency, Digital Currency, Bitcoin, Anti-Money Laundering, Customer Due Diligence

ACKNOWLEDGEMENTS

First of all, I would like to express my sincere thankfulness to my Advisor, Professor Amnat Wongbandit for his guidance and encouragement, without his observation and suggestion, this thesis would not have been accomplished. My other deeply gratitude to Professor Sanya Varanyu, for his comments on the munificent which making my topic even more interesting. I would like to thank Professor Pokpong Srisanit for his knowledge in many useful directions and make me going deeper insights into my contents. I would also like to give my gratefulness to Professor Nilubol Lertnuwat for her suggestions have given me improve my thesis become more complete.

My special thanks go to my colleagues and friends for their valuable consult and encouragement which made me strength to complete this thesis. For the last, I owe the deepest thank wholeheartedly to my family for their support and build up morale which made me focus on my studies.

Mr. Pratyapa Apaiyanukorn
Thammasat University
Year 2015

TABLE OF CONTENTS

	Page
ABSTRACT	(1)
ACKNOWLEDGEMENTS	(3)
LIST OF FIGURES	(7)
LIST OF ABBREVIATIONS	(8)
CHAPTER 1 INTRODUCTION	1
1.1 Background and Problems	1
1.2 Hypothesis	3
1.3 Objectives of study	4
1.4 Scope of study	4
1.5 Methodology	5
1.6 Expected Result	5
CHAPTER 2 ANTI-MONEY LAUNDERING LEGAL REGIME AND VIRTUAL CURRENCY ASPECT IN THAILAND	6
2.1 Introduction to Anti-Money Laundering	6
2.2 Characteristics of Money Laundering	8
2.3 The Measures and Approaches to Prevent and Combat Money Laundering and Financing Terrorism	10
2.3.1 Customer Due Diligence (CDD)	11
2.3.1.1 The Customer under CDD Process	12
2.3.1.2 The Risk-Based Approach to CDD	12
2.3.2 Record Keeping Measures	13

2.4 Virtual Currency Situations in Thailand	14
2.4.1 The Definitions of Virtual Currency	16
2.4.2 The Kinds of Virtual Currency	17
2.4.3 The Sub-Types of Virtual Currency	18
2.4.4 Virtual Currency System Participants	19
2.4.5 Virtual Currency Status in Thai Laws and Regulations	20
2.5 Introduction of Bitcoin	24
2.5.1 The Definition of Bitcoin	24
2.5.2 Risks of Bitcoin	26
2.5.3 The Legal Status of Bitcoin	27
2.6 Peer-to-Peer (P2P) System	27
2.7 Financial Technology (“FinTech”)	29
CHAPTER 3 ANTI-MONEY LAUNDERING AGAINST VIRTUAL CURRENCY AND THE CASE STUDY IN THE UNITED STATES	31
3.1 Current U.S. Regulations on Virtual Currency Money Laundering	32
3.1.1 The Financial Crimes Enforcement Network (FinCEN)	32
3.1.2 The Bank Secrecy Act (BSA)	34
3.1.3 The Patriot Act 2001	35
3.1.4 Internal Revenue Service	36
3.1.5 The Annunzio-Wylie Anti-Money Laundering Act of 1992 (“AWAML”)	37
3.1.6 The Money Laundering Suppression Act of 1998 (“MLSA”)	37
3.1.7 Money Laundering Control Act of 1986	38
3.1.8 New York Codes, Rules and Regulations	38
3.2 Case Study in the United States	41
3.2.1 The Liberty Reserve Case	41
3.2.2 Silk Road Case	44
3.2.3 Trendon T. Shavers Case	47

CHAPTER 4 ANTI-MONEY LAUNDERING AGAINST VIRTUAL CURRENCY UNDER THAILAND REGULATION	49
4.1 Current Thailand regulation on Virtual Currency Money Laundering	50
4.1.1 The Anti-Money Laundering Act B.E.2542	53
4.1.2 Anti-Money Laundering Office Regulation prescribing Guidelines on measures to mitigate the risks of money laundering and terrorist financing potential before introducing new products, new services or the using of new technologies.	68
4.2 Other Thailand Regulations which can apply to Virtual Currency	70
4.2.1 The Electronic Transaction Act B.E. 2544	70
4.2.2 The Computer Crime Act B.E.2550	76
4.2.3 The Exchange Control Act B.E. 2485	79
4.2.4 Financial Institution Business Act B.E.2551	82
4.3 The Decisions of Thai Supreme Court	83
4.3.1 Supreme Court Judgement 877/2501 [1958]	84
4.3.2 Supreme Court Judgement 6384/2547 [2004]	84
4.3.3 Supreme Court Judgement 5161/2547 [2004]	84
4.3.4 Supreme Court Judgement 9631-9632/2558 [2015]	86
CHAPTER 5 CONCLUSIONS AND RECOMMENDATIONS	87
5.1 Conclusions	87
5.2 Recommendations	88
5.2.1 Amendment the legislations to cover the offence against Virtual Currency	89
5.2.2 Monitoring Approach	90
REFERENCE	92
BIOGRAPHY	103

LIST OF FIGURES

Figures	Page
1. The three essential processes of AML onboarding procedures	11
2. The scheme of Bitcoin transaction between the clients.	25
3. The three crucial components of a Bitcoin exchange processes	26
4. How Liberty Reserve's Currency Works	43



LIST OF ABBREVIATIONS

Symbols/Abbreviations	Terms
AML	Anti-Money Laundering
AMLA	Anti-Money Laundering Act
AMLO	Anti-Money Laundering Office
AWAML	Annunzio-Wylie Anti-Money Laundering Act
BOT	Bank of Thailand
BSA	Bank Secrecy Act
CCC	Civil and Commercial Code
CDD	Customer Due Diligence
CFT	Combating the Financing of Terrorism
CIP	Customer Identification Program
DNFBP	Designated Non-Financial Businesses and Professions
ECA	Exchange Control Act
FATF	Financial Action Task Force
FinCEN	Financial Crimes Enforcement Network
FinTech	Financial Technology
IMF	International Monetary Fund
IRS	Internal Revenue Service
KYC	Know Your Customer
MLSA	Money Laundering Suppression Act of 1998
MSB	Money Services Business
US	The United States of America
VC	Virtual Currency

CHAPTER 1

INTRODUCTION

1.1 Background and Problems

“Money laundering and the financing of terrorism are financial crimes with economic effects. They can threaten the stability of a country's financial sector or its external security more generally. Effective anti-money laundering and combating the financing of terrorism regimes are essential to protect the integrity of markets and the global financial framework as they help mitigate the factors that facilitate financial abuse. Action to prevent and combat money laundering and terrorist financing thus responds not only to a moral imperative but also to economic need.”

-Min Zhu, Deputy Managing Director of the IMF¹

It is a Thai government's policy to drive the country towards the new era of the digital economy and digital society by promoting the use of innovations, including next generation technologies, computerized items as well as the advanced innovation of the money related administration. In this regards, the government establishes a national board of trustees with specific roles and missions to provide guidance to the achievement of the goal.²

The revolution in communications technology is no less extraordinary. Nowadays, we live in the digital age full of technologies for convenience. The advent and rapid improvements in modems, satellite communications, fiber optics, and compression technologies have allowed us to obtain information from around the globe virtually anywhere, anytime, and at great speed. The technologies allow wireless connection with another person via computers and mobile phones.

¹ Zhu, Min. Deputy Managing Director of the IMF, *"The IMF and the Fight Against Money Laundering and the Financing of Terrorism"*, (2016)

<http://www.imf.org/external/np/exr/facts/pdf/aml.pdf> (last visited April 5, 2016)

² Chan-o-cha, General Prayut. Prime Minister, *"Policy Statement of the Council of Ministers to the National Legislative Assembly"*, September 12, 2014.

This revolution in communications technology has also brought fundamental changes to the financial business.³ As the economy is developing steadily (sharply?), the financial sectors have to continuously improve accordingly to fulfill the increasing demand in the economic system. In these present days, not only money is used as intermediate to measure the value and the price of the goods or services; a number of other financial products are used as a medium of exchange in the transactions too such as cheque, bill of exchange, promissory note, and virtual currency.

The virtual currency has a specific particular. Unlike other financial products, transfer of the virtual currency will not result in movement of real money; the outcome changes in the amount on electronic record i.e. decrease in the transferor's amount and increase the transferee's amount. There are several ways that the users can exchange the virtual currency for real money, including selling it to a desiring buyer or to *bitcoin exchangers*.

Alongside with the growth of financial innovation, financial-related crimes also develop. Presently, money laundering is one of the critical issues at the international level. It is related or associated with severe crimes, including terrorism and/or transnational fraud, as the criminals use weaknesses in the laws to commit the money laundering to conceal their criminal sources of funds or assets. Money laundering is difficult to suppress, and it causes globally wide impacts which affect not only the economy but also society and politics.

Thai Anti-Money Laundering Act (AMLA) does not specifically address the virtual currency or parties related thereto as its regulated object. With the special characteristic of the virtual currency as described above, the virtual currency does not fall within the definition of "money" or "assets" under AMLA. According to the current AMLA, there are rooms for criminals to avoid being inspected by using the virtual currency instead of the actual money for the purpose of money laundering. Further, since the virtual currency exchanges are merely the exchanges of computer data, it is difficult to detect the transactions and examine users' profiles. Therefore, the virtual currency can be transferred or changed hands without being inspected.

³ Melanie, Law of Electronic Banking. **New York: Aspen Law & Business A division of Aspen Publishers, Inc.** page xxv-xxvi (2000).

In order to design efficient legal procedures to prevent and suppress money laundering using the virtual currency, firstly, the government authorities have to comprehensively understand the operating system of the virtual currency. Then, taking into account the special characteristic of the virtual currency, the government authorities shall consider applying the measures of seizing, freezing, or forfeiting currently used with money and assets to the virtual currency; or designing specific measures to specifically apply with the virtual currency.

1.2 Hypothesis

The Virtual Currency is a modern financial innovation that brings many discussions on the Anti-Money Laundering measures. Because of its particularities, the virtual currency is not categorized as money or assets and is out of the scope of governance of the existing Anti-Money Laundering laws in Thailand. The aforesaid results in a situation where the government authorities are not empowered to control, inspect, or enforce any provisions of the existing Anti-Money Laundering laws, on transactions related to the virtual currency. This can be a channel that criminals use to conceal the illegal sources of fund and finally launder the fund into eligible currency without being inspected. In this scenario, the government has to either improve the existing laws and regulations or design new regulations to specifically regulate the virtual currency related transactions.

1.3 Objectives of study

- (1) To analyze the status of the virtual currency under the Anti-Money Laundering Act of Thailand by analogizing with the interpretation of the Supreme court of justice of Thailand
- (2) To understand the mechanism of the virtual currency transaction as differ from real money transaction
- (3) To identify parties relating to the virtual currency transaction such as financial institutions, companies, and individuals that should be subject to AMLA
- (4) To recommend appropriate guidelines for supervising the transaction which use the virtual currency for the purpose of prevention of money laundering

1.4 Scope of study

This thesis will focus on Anti-Money Laundering Act of Thailand in comparison with anti-money laundering laws application in the United States, in particular: the Financial Crimes Enforcement Network; the Bank Secrecy Act; the Patriot Act; the Internal Revenue Service; the Annunzio-Wylie Anti-Money Laundering Act; the Money Laundering Suppression Act; the Money Laundering Control Act; and the New York Codes, Rules and Regulations. The scope of the study will also extend to other legislations indirectly related to the virtual currency transaction including the financial regulations applicable in Thailand and in the United States. In addition to the rules and regulations, it will highlight the fundamental of the electronic transaction to propose the possible guidelines for prevention money laundering through virtual currency.

1.5 Methodology

This thesis is based on Thailand and the United States laws and regulations. It also relies on information available on websites of domestic institutions of Thailand and international organizations. In addition, research is made into documents, books, articles, journal, academic works (including research, thesis, dissertations and academic opinions) published in Thailand or the United States, and decisions of Thai and US Supreme Court.

1.6 Expected Result

- (1) To promote an understanding of money laundering issue in a situation where the virtual currency is involved and to provide guidelines for an effectiveness anti-money laundering policies in Thailand;
- (2) To study on interpretation of related legislations, that might support the investigation of money laundering by authorizing government officials to search the real beneficiary or the source of the funds;
- (3) To introduce the possible scheme for the supervision and surveillance of virtual currency transaction in order to prevent money laundering;
- (4) To provide assistance to implement the AML/CFT standards through implementation planning and the provision of guidance.

CHAPTER 2

ANTI-MONEY LAUNDERING LEGAL REGIME AND VIRTUAL CURRENCY SITUATIONS IN THAILAND

The improvement of technology and communication brings the countries around the world including Thailand to the digital economy. These innovations provide convenience for the human. However, the criminals may apply these things to commit the crime. The prosperity of the technology effect to the pattern of the offence to be more complicated than before. For example, with the high technology, a simple offence within a country and relating to a few amount of assets (or per say a local crime) may transform to a transnational crime and involving with the huge amount of properties. Criminals form a multinational network and commit illegal activities by separating duties into parts and working coordinately from many jurisdictions. Financial resources for these crimes will be transformed through many processes to conceal the actual source of the money. Frequently, they use the financial institutions or the business firms to perform these proceedings and circulate the money to finance other crimes.

The money circulation is difficult to detect in this present. The existing laws and regulations are obsoleted and incompatible with a rapidly changing environment. As a result, the old legislations cannot enforce effectively. Therefore, new legal measures have been established to cope with the situation and to block movements of property or funds which involved in the offence.

2.1 Introduction to Anti-Money Laundering (AML)

A new criminal control strategy arose in 1980. The theory of the modern age is that no one should be allowed to get benefit from crime.⁴ However, offenders always develop a new method to receive the fruits of the crimes. The counter initiatives have

⁴ Ronald L. Akers and Christine S. Sellers, Oxford University Press Student Study Guide for **Criminological Theories: Introduction, Evaluation, Application** Sixth Edition, 2013. http://global.oup.com/us/companion.websites/9780199844487/guide1/study_guide.pdf

been created on the principle of economic crime through the business finances.

The sources of the legal regime on the money laundering initiate from the multilateral agreement entered into by most countries worldwide, namely the United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1998) (“Vienna Convention”). The Vienna Convention encourages the contracting countries to establish domestic anti-money laundering legal regime in accordance with the standard model recommended thereunder.⁵ This standard model is designed to confront the proceeds of crime. The contracting countries shall rely on the standard model as a baseline in drafting their domestic anti-money laundering laws. The Vienna Convention has brought globally effect; many countries began to develop their domestic legal strategy to strictly regulate money laundering activities to comply with the standard model.⁶

The Vienna Convention has characterized the premise for ensuring intergovernmental activities – for example, the G-7 Financial Action Task Force (FATF)⁷ and Thailand will keep on having some level of impact on the advancement of universal formula model. Imperatively, the Vienna Convention committed the signatories to criminalize the laundering of cash from the narcotic under their individual local laws, accommodated the confiscation (for example, freezing or forfeiting) of related property or got from such offenses, operate money laundering from drug trade as a ground for removal among nations. It also started a procedure for joint legislative support among countries with a specific end goal to encourage the examination and indictment of those included in the laundering of the narcotic trading proceeds.

In the twentieth century, the proceeds of crime turned up as a recent dangerous adversity which blazes through the global society. The drug trafficking and

⁵ Matthew S.Morgan, The London Institute of International Banking, Finance & Development Law, *Money Laundering : The United States Law and its Global Influence*, (November 1996), page 7.

⁶ M.Michelle Gallant, **Money Laundering and the Proceeds of Crime**, p 1.

⁷ FATF, *What is Money Laundering?*. http://www.fatf-gafi.org/faq/money_laundering/ (last visited Jan 10, 2016).

the massive illegal benefit are the most common relation. The situation was escalated by the other offense such as Corruption, Human Trafficking and committed the crime.

2.2 Characteristics of Money Laundering

The term of 'Money laundering' is presently broadly utilized. Its definition is provided differently in each country. The most common definition is the one used in the Vienna Convention and the United Nations Convention Against Transnational Organized Crime ("Palermo Convention") (2000): a procedure whereby the returns of proceeds from the offences changed into lawful money or different properties.

In other words, money laundering is a process by which the unlawful property will be laundered and transformed into legitimated property; or a procedure of making unlawfully obtained property (which is "dirty money") seem lawful (which is "clean"). The money laundering may be performed by an individual or legal entity through financial transactions.

The process of money laundering consists of three stages:⁸

1. Firstly, the criminal sourced fund will be divided into portions and kept with multiple persons in bank accounts or other financial institutions; or the fund may be used to purchase financial products (e.g. cheques, bill of exchange, cash orders, fund, securities, etc.)

2. Secondly, the portions of the fund will be changed (or move) over hands through a web of exchanges in order to conceal the original sources. These changes may involve purchase and sale of high-value property, investment in financial instruments, or foreign currency exchanges across the countries.

3. Thirdly, the fund will re-enter into its originated country in a form apparently legal. The returning fund may be used to purchase real estate or luxury assets or invest in business.

⁸ Duhaime Christine. *"What is Money Laundering? Duhaime's Financial Crime and Anti-Money Laundering Law"*. <http://www.antimoneylaunderinglaw.com/aml-law-in-canada/what-is-money-laundering>. Retrieved 7 March 2014.

There are various and sophisticated methods to launder money. The primary purpose of money laundering is to change the money or asset derived from illegal activities to be lawful money or property and to conceal the trace to its original criminal sources.

Many regulating bodies try to provide estimations on the amount of money being laundered each year, either at global economy or at the country-specific economy. It is hard to indicate the accurate amount of money laundered.⁹ In 1996, the International Monetary Fund (IMF) estimated that two to five percent of the money in

⁹ Financial Action Task Force. INTERNATIONAL STANDARDS ON COMBATING MONEY LAUNDERING AND THE FINANCING OF TERRORISM & PROLIFERATION', *"The FATF Recommendations"*. February 2012, Updated October, 2015. http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf (last visited Jan 13, 2016).

So the Financial Action Task Force on Money Laundering (FATF), is intergovernmental body begin to set up for the purpose of combating money laundering. Notwithstanding the trouble in estimation, the measure of money laundered every year is in the billions (US dollars) and represents a critical approach sympathy toward governments. FATF has created 40 proposals on money laundering and 9 exceptional suggestions with respect to terrorist financing. FATF evaluates every part nation against these proposals in distributed reports. Nations seen as not being adequately agreeable with such proposals are subjected to financial sanctions.

FATF's three essential capacities with regard to money laundering issues are:

1. Monitoring individuals' advancement in executing hostile to government evasion measures.
2. Reviewing and writing about laundering patterns, strategies, and countermeasures.
3. Promoting the reception and execution of FATF hostile to combat money laundering to the standards level.

The Financial institutions establishment have similarly attempted endeavors to forestall and identify exchanges including illegal cash, both as an aftereffect of government prerequisites and stay away from a chance of reputational risks involved.

the overall worldwide economy related to money laundering. Accordingly, the number and extent of laws and regulations have been increased and expanded considerably to suppress the money laundering. It was the year when the issue of money laundering turned out to be more truly than any time in recent memorial. Subsequently, governments and universal bodies actively put on endeavors to stop, avoid and catch money launderers.

2.3 The measures and approaches to prevent and combat money laundering and financing terrorism

Know Your Customer (KYC) is a significant measure of the anti-money laundering policy, which requires banks and financial institution to apply: the Customer Identification Program (CIP), a process to gather the client's information; the Customer Due Diligence (CDD), a process to analyze and evaluate information of new clients and indicate money laundering risk level as to low, medium or high¹⁰; and the Enhanced Due Diligence (EDD), a process to monitor high-risk customers and their transactions by reviewing more closely and more frequently.¹¹

¹⁰ **AdvisoryHQ**, KYC vs. CIP vs. CDD. | Know Your Customer Rules and Guidelines, Jan 24, 2016 <http://www.advisoryhq.com/articles/kyc-vs-cip-vs-cdd-know-your-customer-rules-and-guidelines/> (last visited May 28, 2016).

¹¹ Federal Financial Institutions Examination Council. "*Customer Due Diligence—Overview*". https://www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_013.htm (last visited May 31, 2016).

The sequence of Know Your Customer (KYC) processes are presented in the scheme below.

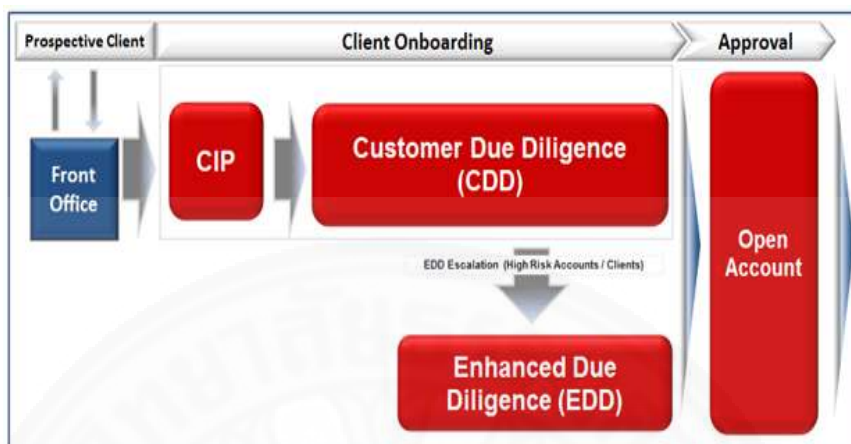


Figure 1. The three essential processes of AML onboarding procedures

2.3.1 Customer Due Diligence (CDD)

CDD is the process to collect information about a customer to know the profile of each client which are a fundamental principle of AML/CFT. Financial related organizations and/or institutions have to know their customers. In this regards, the client will be required to disclose essentials information based on the level of risks of money laundering and/or terrorist financing. Moreover, the related organizations and/or institutions are required to impose certain conditions on their customers according to the regulatory standards.

The client's information kept with the financially related organizations, and/or institutions are important for legal enforcement by relevant authorities. The information will facilitate legal investigation of money laundering, manipulation or possesses criminal or terrorist property. If there are any suspected activities, (for example, the purpose of the transaction is not commercially reliable), the organizations and/or the institutions will have to report such suspicious to the relevant authorities in pursuant with the term of procedures or regulations. In addition, according to a global standard, it is a fundamental principle that setting up anonymous accounts is restricted.

The minimum required information under the Know Your Customer measure is as follows:

1. Identity

2. Residence (verification of address)

3. Risk profiling

The obligations are imposed on both financial institution and the customer. That is to say, the financial institution has an obligation to request, and customers have an obligation to provide, the required information. This is an important measure as the client's information is a primary connection that can trace to parties involving with suspected transactions.

As part of the due diligence process, the financial institution ought to comply with measures to guarantee the profile accounts are up-to-date, and to monitor the transactions of the customers in pursuant with the measures required for the customers' risk level. It should take into consideration the risk level of the customers when reviewing the customers' transactions, especially when the activities conflict with the normal commercial practices.¹²

In practice, these measures are not strictly complied by the financial related organizations or institutions. Consequently, some customer's information are fake, unreliable, inaccurate, or not updated. This noncompliance makes it difficult to ascertain the true identity and impacts the efficiency of legal enforcement in case of the offence.

2.3.1.1 The customer under CDD process

Customers being under CDD process are those entering into a business relationship with the financial related organizations or institution. The CDD process is also imposed on potential customers, even if they did not actually enter into the business relationship with the financial related organization or institution.

The business relationship establishes where the customers express the desire to create a relationship with the financial related organization or institution and continues until termination of the relationship.

2.3.1.2 The risk-based approach to CDD

The international standard model specifies threat-based strategy to be applied in performing customer due diligence and classifying customer risk level. The criteria are contingent with the particular of clients, their business activities, and

¹² *Id.*

their transactions. The risk classification strategy aims to improve qualification of the due diligence. The risk classification will determine the list of information required from the customers as described below:¹³

- 1) Only disentangled or essential record opening data may be required from a low-adjustment, low-turnover accounts. The degree of data that checked can confine to the recognizable proof confirmation and data concerning wellspring of the assets and the regular recurrence of deposits and withdrawals.
- 2) For basic-risk customers, i.e. the individuals who are for all time inhabitant in the nation, with a salaried employment or another straightforward wellspring of pay, the standard information may be required.
- 3) More strict due diligence will be required to higher-risk customers. In this regards, information of the ultimate beneficiaries and the controller of the customers will also be required.
- 4) Listed companies with their completely claimed backups are considered lower-risk customers and are required only normal due diligence procedure.

Private organizations or other substances, such as investors, are considered as higher risk customers than listed companies because they have a lower standard of external examination. The connections and characters of ultimate proprietors and controller should likewise be sufficient to confirm corporate validity. The ultimate owners in this regards might be official executives or trustees.

2.3.2 Record Keeping Measures

This process relating to the CDD process, when the financial institutions gathered all of the information of customers and the transaction records,

¹³ Advanced Certification in Anti Money Laundering and Counter Financing of Terrorism. <http://www.int-comp.com/members/attachments/Mal-module4.pdf> (last visited 7 Jul, 2016).

they have a duty to maintain such information for a specified period according to the relevant laws and regulations.

The law required the financial institutions to keep storage of all records of both domestic and international customers as well as their transactions under the requirements for a period as determined for at least five years from the completion of the transactions or at least five years from the termination of the business relationship. These records have to be sufficient to verify the identity of such customer or the particular of the transactions.¹⁴

In addition to the record keeping processes, the financial institutions also have to assist the competent authority to determine and investigate such information as requested by state authority.

2.4 Virtual Currency Situations in Thailand

Money is the innovation designed to facilitate people exchanging of things. It has been recognized internationally to use everywhere in the world. Money is the intermediary of exchange for goods and services. Money has been used and circulated in the form of coins and notes.¹⁵ The monetary unit is identified by currencies utilized in each country such as U.S. dollars, European Euros, British pounds or Thai baht. These financial forms are aiming to maintain the quality, and can exchange between countries in the prevailing market; that characterize the relative estimations of the various kind of money.¹⁶

Governments determined currency used in their nation, so there are many currencies in this world. They can divide into two monetary systems: the first one is fiat

¹⁴ FATF, Methodology: Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT systems technical compliance assessment, Feb 2013.

¹⁵ Collins English Dictionary – Complete and Unabridged, 12th Edition 2014.

¹⁶ Marc Levinson, The Economist, **"Guide to the Financial Markets"** 4th Edition 2006. https://drive.google.com/file/d/0B_Qxj5U7eaJTZTJkODYzN2ItZjE3Yy00Y2M0LTk2ZmUtZGU0NzA3NGI4Y2Y5/view?hl=en&pli=1

money, and the second one is commodity money. The value of the currencies is unequal, depending on two main factors i.e. the economic stability and the mineral reserves of the governments. Gold is used to guarantee the value of money. It makes the confidence to everyone to use the money to exchange for other objects.¹⁷ In conclusion, the circulations of funds in the world economy come from these exchange transactions.

The medium of exchange has been developed continuously from past till present. The forms of having been developed to electronic money (E-money): for example, cash cards are used by the cardholder topping up the money and spending that money using the card to travel by BTS sky train or refill the money of prepaid mobile phone. Nowadays, the digital world or the online network has created another form of exchange medium, so called a virtual currency, which has specific particular different from the particular of money described above.¹⁸

The progressive of the human technology changes rapidly from the former times to the digital age. The innovation has created the cryptocurrency that can be easily referred to as the virtual currency (not real money). Since the virtual currency is digital data, it can be called digital currency. It is starting from the private placement that limited and nobody knows what it is. Nevertheless, this financial innovation has been used widely and affected the current financial system and the medium of exchange. This thing may impact the world economy because the virtual currency is conveniently

¹⁷ Bernstein, Peter, and A. Volker. 2008. A Primer on Money, **Banking and Gold** (3rd ed.). Hoboken, NJ: Wiley. <https://books.google.co.th/books?id=LE2pzHjek4sC&pg=PT4&lpg=PT4&dq=Bernstein,+Peter,+and+A.+Volker.+2008.+A+Primer+on+Money,+Banking+and+Gold&source=bl&ots=uhYTOcUC8U&sig=o-EbxxkgyUiPHFII3LFw43p7wWA&hl=th&sa=X&ved=0ahUKEwjSkoXNzaXOAhUMpI8KHfmBCv4Q6AEIRjAF#v=onepage&q=Bernstein%2C%20Peter%2C%20and%20A.%200Volker.%202008.%20A%20Primer%20on%20Money%2C%20Banking%20and%20Gold&f=false>

¹⁸ ศรีชาติ, กัณตภณ. 'เงินเสมือน (**Virtual Currency**) ต่างจากเงินจริงอย่างไร'. ธนาคารแห่งประเทศไทย, (2556). (Srichart, Kantaphol. '**How was the difference between Virtual Currency and Real Currency?**'. Bank of Thailand, (2013).

exchangeable by using the peer-to-peer (P2P) network to connect users to each other via the internet, and its exchanging fee is cheaper than the fee imposed by the current financial institutions.

2.4.1 The Definitions of Virtual Currency

There are various implications of Virtual currency. It is a complicated subject that involves not only anti-money laundering issues but also other issues such as consumer protection, tax, network IT security standards.

A standard definition that explains the meaning of this term and categorizes the types of virtual currency is based on the business plans and manners for their activity. The proposed definition is from the conceptual harmonization of meanings of the term given in various regulations by governmental bodies of different jurisdictions.

Consequently, the harmonized definition of the Virtual currency (or Cryptocurrency or Digital currency) is the new financial innovation in this century. It is a computer algorithm generated by individual groups or persons. It can be further classified according to action plans of businesses, system techniques, and recognizing members in the frameworks. This currency is a digital representation¹⁹ of worth that can digitally exchange, having capacities as a medium of trade among the virtual currency users. The virtual currency is not issued or endorsed by any state authorities, nor does it has the legitimate capacity to pay the monetary debt.

It is not quite the same as money or formal currency which is the tangible material (coin and bank notes) accepted as an exchange. It is comparable to e-cash by the fact that they both are exchanged electronically. However, e-cash refers to a fiat monetary under the delicate legitimate status; but virtual currency does not. Virtual currency works on a match-based system which makes it private and secured. The technology is complex and difficult to counterfeit. It is also free from the government control or state regulation. It is easier to transfer money between the parties using the public and private keys for the security of transactions. These processes

¹⁹ FATF REPORT: Virtual Currencies - Key Definitions and Potential AML/CFT Risks, June 2014.

succeeded with cheaper fees than the electronic transfer via banks or financial institutions.

Notwithstanding, a weakness of the virtual currency is that it is not real money and does not have a central storage. Therefore, the balance of virtual currency can be lost in the event of a computer crash or data hacking. Another thing is that the credibility of virtual currency which is not acknowledged as legitimate by any government. That means value or prices of the virtual currency depends on demand and supply of the virtual currency users; possibly, the value may come down to none in the future as it is actually only digital codes. Nevertheless, nowadays the virtual currency can be sold to accepting users in an exchange for legitimate currency.²⁰

The anonymity function of the virtual currency transactions system is a channel for criminals to facilitate illegal activities such as tax evasion and money laundering.

2.4.2 The Kinds of Virtual Currency²¹

Virtual currency can be separated into two types: convertible and non-convertible, based on its appearance and usability function.

(1) Convertible virtual currency has the same worth of the genuine currency and can be traded back for real money directly through the issuing administrator or the third party exchanged (virtual currency exchange).

(2) Non-Convertible virtual currency is tradable in a particular virtual web space, such as Amazon.com or online gaming websites under the rules control set by the administrator of such website. This type of virtual currency is not exchangeable directly into legitimate currency. However, it can be exchanged with legitimate currency in certain circumstances, for instance: selling in an underground market. This type of virtual currency can be transformed into a convertible virtual currency, so it is not a static feature.

²⁰ The Financial Crimes Enforcement Network, *FIN-2013-G001: Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies*, 2013.

²¹ FATF REPORT, *supra* note 19.

2.4.3 The Sub-Types of Virtual Currency

Non-convertible virtual currency forms are centralized because they are issued by a central authority having administrator power to control the usage. Convertible virtual currency may be either centralised or decentralised.

(1) Centralised virtual currency is the currency issued by an administrator who also has duties to announce regulations of use, retain records, and control the payments and determine the value of the virtual currency. The administrator also has authority to withdraw the currency from circulation. The exchanging rate of the virtual currency may be floating in each market sector in accordance with demand and supply for that currency in the market; or it can be fixed in accordance with the governor set worth quality measured in fiat money, or other official recognized things that have a valuation, such as gold. Currently, most of the virtual currency exchange transactions are centralised.

(2) Decentralised virtual currency is a shared or opened-source virtual currency that does not have a particular administrating center to monitor and oversight its issuances and exchange transactions. Examples of decentralised virtual currency are Bitcoin and Litecoin. The well known innovation system used with decentralised currency is a peer-to-peer system or a blockchain system. Users can obtain this decentralised virtual currency from the internet through their computer or produce ones by themselves.²²

Nowadays, Convertible virtual currency is a type of virtual currency that creates essential risks in AML/CFT. It can be utilized to move the fund into an unofficial area out of the standard financial sector; and criminals use this advancement and the absence of supervision from the governmental regulator as a new channel for money laundering by conversion, transfer, concealment or disguise the source/origin of unlawful money. The third party which is an individual or corporation that involved in a transaction relies on the sort of business or financial exchanges transaction. It is not the principals or affiliations which identified with the other participants in the

²² *Id.*

transaction, for example, PayPal the online payment proceeds as a third party in an exchange transaction.

2.4.4 Virtual Currency System Participants

Virtual currency system proceeds as a software or application used with a computer, mobile phone and connected each user or any related person via a digital online connecting network. There are many parties participating in the virtual currency system that should be considered such as exchanger, administrator, user, miner, virtual currency wallet and wallet provider.²³

The above is not a complete list of all participants in the system, but it shows overall environment of the network system, the development of virtual currency technologies, business model and potential risks of AML/CFT.

1. An exchanger refers to a person who has a business to arrange the transactions of exchanging the virtual currency with the real currency, funds or another form of things that have a value such as gold or other precious metals and receives a commission fee. The exchange of virtual currency can be paid by money, wires, credit cards and other virtual monetary. In this regards, the exchanger roles can be compared to a capital market sector or an exchange desk. The users use the exchanger to store and withdraw cash from virtual money accounts.²⁴

2. An administrator is a person who takes a part in virtual currency exchange transactions as a regulator issuing operating rules for customers. The administrator also retains payment accounts and supervises on the issuance or recovering the virtual money.²⁵

3. A user who is a person using the virtual money for the purpose of purchasing goods and services by transferring the virtual currency to other users; or acquiring the virtual currency for investment. There are several ways that a user can receive the virtual currency:

(1) a user can purchase the virtual currency from the exchanger or directly from the administrator or the issuer and pay by actual money;

²³ *Id.*

²⁴ *Id.*

²⁵ *Id.*

(2) a user can accept the virtual currency payment against products or activities such as: react to the advancement, finish online questions or supply a genuine or virtual goods.

(3) a user can create units of the virtual currency by themselves through the mining (unlock the digital data code on the system or solve the equation) and obtain them as gifts or rewards. This method is only available for obtaining a decentralised virtual currency (e.g., Bitcoin).²⁶

4. A miner is a person participating in a decentralized virtual currency system. A miner initiates particular programming to tackle complex encryptions in a dispersed proof-of-work or other checking framework used to accept exchanges in the virtual money network. The miner can also be a user if it can make all alone convertible virtual money singularly for their reasons for instance: to speculation, use to pay a commitment or buy products and administrations. The miner might likewise act as the exchanger, maintaining the virtual currency by creating the own virtual money accounts with an intention to finally exchange it for money or other virtual money.²⁷

2.4.5 Virtual Currency Status in Thai Laws and Regulations

The legal status of virtual currency in Thailand is still as unclear as in other countries. The government and the financial related authorities are trying to understand this type of financial innovation thoroughly. Now Thailand has no specific legislations to regulate the virtual currency and/or parties involving in virtual currency system.

In 2013, The Bank of Thailand (BOT) had set up a conference on the issue of money exchange licensing concerning Bitcoin. The participants of the meeting included 15 members of the board of the BOT, consisting of various Thai governmental agencies, and Bitcoin Company Limited. It was concluded from the meeting that Bitcoin Company Limited is not qualified to obtain a money exchange license. Furthermore, it was addressed by seniors of the Foreign Exchange Administration and the Policy Department that activities of Bitcoin Company Limited are not legally acceptable in Thailand because the lack of governing laws and competent regulator and

²⁶ *Id.*

²⁷ *Id.*

relate with different budgetary angles the accompanying. Bitcoin Company Limited has many kinds of activities such as;

- buying and selling Bitcoin,
- buying and selling any merchandise or administrations in return for Bitcoin,
- sending Bitcoin to persons situated outside of Thailand, and
- receiving Bitcoin from persons located outside of Thailand.²⁸

This meeting has brought further consideration and discussion concerning Bitcoin as well as other digital currencies having the same or higher level of complication. BOT did not explicitly ban Bitcoin related activities. Instead, it has issued a preliminary decision that utilizing bitcoin as portrayed is unlawful because there are no laws to regulate the new anonymous field or cryptographically technology which protected virtual currencies and further affair like many other countries in this world.²⁹

In addition to this issue, another concern especially cautioned by the BOT is on capital movements by the use of Bitcoin which may cause an impact on the value of the official currency i.e. Thai Baht³⁰. This situation has led to the more attention to a status of Bitcoin in the aspect of law in Thailand. In this regards, the relevant authorities' position against the Bitcoin is positive as they also take into consideration

²⁸ bitcoin.co.th., *"The results of the Meeting between Bitcoin Co.Ltd. and BOT on July 29th, 2013"*. <https://bitcoin.co.th/trading-suspended-due-to-bank-of-thailand-dvisement/?bettertitle> (last visited Feb 20, 2016).

²⁹ Watts, Jake Maxwell. *"Thailand's Bitcoin ban is not quite what it seems"*. July 31, 2013. <http://qz.com/110164/thailands-infamous-bitcoin-crackdown-is-not-quite-what-it-seems/> (last visited Feb 20, 2016.).

³⁰ ข่าวหนังสือพิมพ์กรุงเทพธุรกิจ. "ธนาคารแห่งประเทศไทยชี้แจง ระงับ **Bitcoin** เพราะห่วงเก็งกำไรค่าบาท", (31 กรกฎาคม 2556) (2556). (Bangkokbiznews. *'Bank of Thailand explanations that suspended Bitcoin because worried about the speculation of Thai Baht'*. (July 31, 2013) (2013))

that this innovation contains both advantages and disadvantages to the people in the country.

On 18 March 2014, after the meeting, the BOT has issued a statement regarding the information and details of Bitcoin and other electronic data unit of the same particular³¹. The first important point of this statement is to confirm an illegal status of the virtual currency under laws of Thailand. The statement provides warnings to users which can be explained in three subject matters:³²

(1) Virtual currency definition

Virtual currency is created by a person or group of persons using computer mechanism for the purpose of being used as a medium of exchange. These electronic data will be stored in computerized devices such as computer, laptop, or smartphone of the users and can be transferred to other users. The virtual currency can be used to buy goods and services in the same manner the actual money works. The value of the virtual currency is also prescribed by determination of exchange rates; however, the virtual currency exchange rate determination is made by private individual or group, and not by governmental organizations.

Virtual currency or Bitcoin is not considered as money and cannot be used to pay debt like the real currency. It is valueless in itself because the value of the virtual currency is vary according to the demand of trades. In other words, the value of the virtual currency can be changed quickly and become worthless when nobody wants it.

³¹ ธนาคารแห่งประเทศไทย. 'ข่าว สปท. เรื่องข้อมูลเกี่ยวกับ **Bitcoin** และ หน่วยข้อมูลทางอิเล็กทรอนิกส์อื่นๆ ที่ลักษณะใกล้เคียง', ฉบับที่ 8/2557, (18 มีนาคม 2557) (2557). (Bank of Thailand. '*BOT news: the information about Bitcoin and other electronic data which similar to Bitcoin*', no.8/2014, (March 18, 2014) (2014))

³² Palmer, Daniel. "*BOT Suggests Bitcoin Not Illegal But Warns Against its Use*", (2014). <http://www.coindesk.com/bank-thailand-says-bitcoin-illegal-warns-use/> (last visited Feb 20, 2016).

(2) The risk of possessing virtual currency

The virtual currency is tradable only in a specific marketplace where users can use real money to bid for the virtual currency. As a result, the value of the virtual currency, in comparison with actual currency, can fluctuate rapidly. It also included the store which began to receive payment by this currency. The trend of using virtual currency increasingly more than the regular pattern.

In addition, there are many news and information reporting incidents causing a sharp reduction in value of the virtual currency such as data stolen by the hacker, money laundering issues, the closing of online businesses. The central banks around the world also issue similar statements notifying the public about the risk of using virtual currency.

(3) General suggestions

The BOT makes caution to users of the virtual currency that digital currency is not money and not considered as a legal tender which can be refused in payment of debt. The risk increased as these data are stored only in a computer device and can be stolen by hackers. Another caution is the fluctuation in value independently from and not related to the real economy. The users of the virtual currency are not protected by any laws because it is not a legally valid currency. If the users have any problems in using the virtual currency, there is no legal measure to gather evidence or to track the electronic data, unlike transactions through bank or financial institution under the supervisions of the state authorities which contains the reliable regulatory process and tracking data system to check the source of the transaction.

The legal status of virtual currency in Thailand is still, like other countries around the world, unclear. There is also the licensing issue concerning exchanges or trades of virtual currency which needs further study in order to determine whether such activities are illegal or not.³³ The Bank of Thailand itself does not have the constitutional power to outlaw the activities. The other governmental organizations do not manage or control this situation by issuing any appropriate laws.

³³ *Id.*

2.5 Introduction of Bitcoin

Bitcoin is the first virtual currency captured by the state officials. It is the most popular virtual currency and has the highest value compared to the others.³⁴ Under this thesis, the writer intends to focus the study on the virtual currency especially Bitcoin which is more likely to develop and play a role in the financial sector in the future.

2.5.1 The Definition of Bitcoin

Bitcoin is a virtual currency or digital data created in 2009. The creator of this innovation is Satoshi Nakamoto, whose real identity has not verified yet. He created bitcoin that is an electronic coin as a chain of digital signatures. Bitcoin is used as an intermediate of exchange goods and services instead of the real currency. Bitcoin payment is made through a secured electronic payment system using cryptographic technology. This security system allows parties to deal directly with each other without being interfered by any the third party.³⁵

Bitcoin offers lower transaction fees than the traditional online payment through banks or other financial institutions. The most important feature of Bitcoin is its decentralized system being independent from the government authority. Bitcoin is intangible and is not present in physical form. It only appears as balances shown on digital accounts. Bitcoin is invented with an intention to keep privacy and secrecy of transactions between the users. Each Bitcoin transaction will process through multi-layer complex codes designed to verify the transaction accuracy.³⁶ For this reason, it operates comply with the idea of privacy and anonymity must be outright,

³⁴ FATF REPORT, *supra* note 19.

³⁵ Nakamoto, Satoshi., "*Bitcoin: A Peer-to-Peer Electronic Cash System*", (2009), <https://bitcoin.org/bitcoin.pdf> (last visited Jun 5, 2016).

³⁶ Calvery, Jennifer S., "*Statement of Director Financial Crimes Enforcement Network United States Department of the Treasury Before the United States Senate Committee on Banking, Housing, and Urban Affairs Subcommittee on National Security and International Trade and Finance Subcommittee on Economic Policy*", 2013.

however, that clients should even now have an approach to entrust in the validness of the transaction.³⁷ The pattern of Bitcoin transaction is presented in the scheme below:

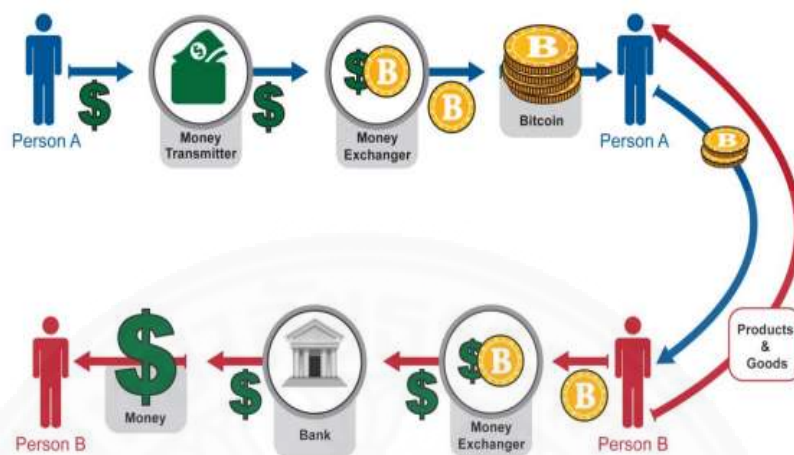


Figure 2: The scheme of Bitcoin transaction between the clients.³⁸

The main difference between the centralised and decentralised virtual currency is in the process of money flows: the administrator serves as an intermediary in the transaction of centralized virtual currency; but there is no such administrator involving in the transaction of decentralised virtual currency, including Bitcoin.³⁹ The lack of supervision in the decentralised virtual currency transactions causes risk of the offence, especially money laundering.

It is a set of electronic data, created by a group of people, using a computerized technology, for usage as a medium of exchange. Bitcoin is stored in a “Wallet” application compatible to install on a laptop or smartphone. The Wallet is used to transfer Bitcoin. Recently, Bitcoin has been used for payment of goods and services, particularly those purchased over the internet, as well as for currency exchange where

³⁷ Greene, Olivia. *Risk Advisory, Risks and Challenges Associated with Bitcoin Transaction Monitoring for AML*, 2015. https://www.dhglp.com/Portals/4/ResourceMedia/publications/Risk-Advisory_Bitcoin.pdf (last visited Jun 5, 2016).

³⁸ Calvery, *supra* note 36.

³⁹ *Id.*

the exchange rates set by a group of people equipped with a computerized system to support Bitcoin storage and transfer.⁴⁰

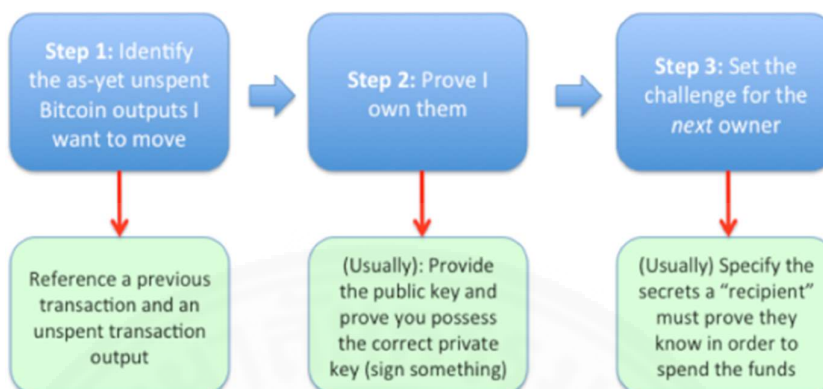


Figure 3. The three crucial components of a Bitcoin exchange processes⁴¹

2.5.2 Risks of Bitcoin

Most central banks consider Bitcoin and other similar electronic data as a non-legal tender. It has no value in itself, and the trading value varies according to solely to demand and supply among investors. Thus, Bitcoin value is highly unstable and can become worthless anytime when there is no longer a demand. As such, the following risks can arise:

(1) The value is highly volatile because it is dictated purely by users' demand, irrespective of actual economic conditions.

(2) Data theft is common since electronic data must store on a computer. Thus, users can easily lose such data through theft or equipment damage.

(3) The absence of consumer protection can be a problem. Bitcoin was not considered as a legal medium of exchange. It is not issued for transfers through commercial banks or other authorized service provider. Therefore, there is no proper

⁴⁰ King, Douglas. Federal Reserve Bank of Atlanta, *"Retail Payments Risk Forum Working Paper: Banking Bitcoin-Related Businesses: A Primer for Managing BSA/AML Risks"*, 2015.

⁴¹ Brown, Richard G., *"A simple explanation of bitcoin 'sidechains'"*, 2014. <http://gandal.me/2014/10/26/a-simple-explanation-of-bitcoin-sidechains/> (last visited Feb 22, 2016).

tool in place to track and monitor systematic data and money collection.⁴² In the event of fraud or any problem in usage (e.g. incorrect transfer and non-delivery of promised goods and services), there can be difficulties in enforcement of legal actions.⁴³

2.5.3 The legal status of bitcoin

There is a broad range of discussions among nations to indistinct or changing in a significant number of them. While a few nations have legalized and permitted utilization and exchange of virtual currency, others have banned or limited the use of it. Moreover, different governmental agencies, institutions and courts have characterized Bitcoins in an unexpected way. While this article explains the status of Bitcoin in a legal aspect, there are regulations involving this type of virtual currency toned to be studied in comparative frameworks too.

2.6 Peer-to-peer (P2P) System

The peer-to-peer allows two or more people to simultaneously work together, without substantially requiring focal coordination, on suitable data and communication networks.⁴⁴ As opposed to customer/server systems, P2P systems guarantee enhanced versatility, the lower expense of possession, self-sorted out and decentralized coordination of formerly underused or constrained assets, a unique adaptation to non-critical failure, and better backing for building appointed systems especially. P2P systems offer an alternative in situations where the transactions are hardly performed by standard methodologies.⁴⁵

⁴² Bank of Thailand, "*Payment System Report*", 2013. https://www.bot.or.th/English/PaymentSystems/Publication/PS_Annually_Report/Documents/Payment_2013_E.pdf. (last visited Feb 22, 2016).

⁴³ *Id.*

⁴⁴ Schoder, D., and Fischbach, K., "*Peer-to-peer prospects: Communications of the ACM*". ACM, New York SA, Volume 46. Issue 2 (2003). 27–29

⁴⁵ Schoder, D., Fischbach, K., and Christian, S., "*Core Concepts in Peer-to-Peer Networking*", University of Cologne, Germany, 2005.

P2P selecting or structures association is an appropriated application advancement exhibiting that areas attempts or work weights between accomplices. Accessories are essential as uncommon, equipotent people in the application. They are said to diagram a scattered course of action of focus concentrates. The pairing makes an area of their points of interest, for occurrence, dealing with force, circle stockpiling or transmission system limit, open apparently to other structure people, without the essential for focal coordination by servers or stable hosts. This mechanism is the digital payments operating directly between users via the internet.⁴⁶

The Bitcoin system itself was expressly intended to serve as electronic payments through peer-to-peer network tools and to operate on the internet trade basis. The network enables users to transfer Bitcoin or other decentralised virtual currencies directly to each other and settling those exchanges simultaneously without the involvement of financial institution or any third party. Subsequently, there is no intermediation cost, such as exchange charges.⁴⁷

Bitcoin does not have the central administrating authority and is not subject to control or supervision of any governmental bodies. P2P network is used not only for Bitcoin transactions, but also transactions related to another kind of virtual currency. The issue about the decentralised system causes the effect to the financial situation in a way that makes it difficult to determine and oversight the virtual currency transaction.

⁴⁶ The Financial Action Task Force. *"Guidance for A Risk-Based Approach Virtual Currencies"*, 2015.

⁴⁷ *Id.*

2.7 Financial Technology (“FinTech”)

The Advances in network infrastructure technology have improved the innovation to connect internationally. It provides the opportunities for the creators to gather information from the internet network and provide services through the internet network. From the data sources and numerous amounts of obtainable data, the new financial innovation and new algorithms can be useful to enhance the competence of the financial innovation services to the customers.⁴⁸

The Advancements of FinTech are exceptionally dynamic at the global scene. An exploration led by Business Insider demonstrates that administrative instability of FinTech advancements is a unique challenge. There are significant obstacles in supervising such advancements, and these impact the financial and the investment sectors. The regulators tend to diminish administrative responsibility while maintaining public’s advantages. In this regards, the regulators request the cooperation of innovators and creators to permit them to experiment the ideas and to help to analyze potential administrative issues at an early stage.⁴⁹

In conclusion, FinTech startups have a capacity to openly improve quickly. However, it confronts challenges in balancing clients need with administrative measures. Therefore, there is a consistent developing pattern of Co-request (co-operation and competition) among the officeholders from budgetary, speculation and telecom areas working with new businesses to influence the best from both universes. FinTech creates the tools and the facilities which impact directly to the commercial sectors. The virtual currency and Bitcoin are one of FinTech, in a category of Payment System Innovations which is the core of the digital economy. The mainstream focuses on the technique about user-friendly, secure and productive; it is hard to empower a compelling computerized economy. Thai Government realizes that the innovation on payment system is important for the development of financial tools

⁴⁸ The Securities and Exchange Commission, Thailand. FinTech Forum: FinTech Ecosystem. <http://www.sec.or.th/EN/Pages/FinTech/fintech.aspx> (last visited 16 Jul, 2016).

⁴⁹ *Id.*

and administrations in Thailand. With more than 83 million mobile number subscriptions and increasing, Thailand has more mobile memberships than the amount of its population. This is a great opportunity to introduce the innovative items, services, or administrations to formerly inaccessible clients through mobile phones, who may somehow remain unbanked customers; serving the unserved and possibly accomplishing budgetary incorporation.⁵⁰

⁵⁰ *Id.*

CHAPTER 3

ANTI-MONEY LAUNDERING AGAINST VIRTUAL CURRENCY AND THE CASES STUDY IN THE UNITED STATES

US Dollar is the primary currency of the world; it is a preferable currency in international financial transactions, and it is liquidly exchangeable. As a result, US Dollar is a primary target for the criminals who try to launder the dirty money or asset and transform it to the legitimate currency (US Dollar). Consequently, the United States (US) has faced problems with the virtual currency, in particular, adoption of the money laundering. The virtual currency plays a role in criminal activities as a new channel of money laundering, apart from the former methods using loopholes in transactions through financial institutions or banks. This circumstance increases the risk of money laundering because it is difficult to monitor and supervise the virtual currency transaction.

To cope with the situation, the US has amended its laws, regulations, and guidelines concerning virtual currency transactions and relating business to control and manage the risk arising out of the use of the virtual currency. It also determines the definition of virtual currency, the relating business, and the involving persons, to make it clear under the applicable law and regulations.

The fundamental regulations related to the virtual currency in the United States are The Financial Crimes Enforcement Network (“FinCEN”); the U.S. Internal Revenue Service (“IRS”); and the Patriot Act. There is also the state regulation, namely the regulation of New York State which is the beginning endeavor by Regulators at legalizing this kind of currency as a feature of payment in the United States.

The amendments to these laws and regulations have been made to extend the provisions of the existing regulations to be applicable to the virtual currency. The amendments include creations of new provisions to especially prevent money laundering activities using virtual currency. In the aspect of law enforcement, this thesis focuses on case studies that show the possible process which can be used as guidelines on interpretation of the existing laws of the countries around the world including Thailand. This thesis will study and understand these regulations in order to provide a

suggested definition of the virtual currency that covers all types of innovations criminals use in committing the crimes.⁵¹

3.1 Current U.S. Regulations on Virtual Currency Money Laundering

3.1.1 The Financial Crimes Enforcement Network (“FinCEN”)

The Financial Crimes Enforcement Network (“FinCEN”) has presented FIN-2013-G001 which is a guideline for implementation of FinCEN’s regulations to regulate administration, exchange, or use of the virtual currency. The explanation of financial transaction and the financial institution is provided in 18 US Code § 1956 Laundering of Monetary Instruments. The statute explains an overview of financial transactions involving money (coin or currency) in the United States or other countries.⁵² The statute is not applicable to virtual currency or Bitcoin as the currency as it is decentralized and not accepted as legally valid by any country. Financial Institutions described in the statute as banks, financial firms, and Money Service Business (“MSB”) that convey the money. Parties involving in Bitcoin transactions are not within the definition scope of Financial Institutions. However, the guideline stated that Bitcoin exchanges or administrators could be classified as an MSB and, thus, makes it subject to the U.S. anti-money laundering regulations.

FinCEN issues this interpretive guideline to illustrate the enforcement of the rules implementing the Bank Secrecy Act (“BSA”) on persons creating, obtaining, distributing, exchanging, accepting, or transmitting the virtual currency. These individuals are defined separately as “users”, “exchangers” and “administrators”. The definitions are provided based on characters and activities of each person. The user of virtual currency is not an MSB under the regulations and therefore is not subject to MSB requirements of registration, reporting, and recordkeeping. However, an

⁵¹ Pamplin, Berkley A., "Virtual Currencies and The Implications for U.S. Anti-Money Laundering Regulations". Master of Science in Economic Crime Management, Utica College, 2014.

⁵² Henning, Peter. *"For Bitcoin, Square Peg Meets Round Hole Under the Law"*, December 9, 2013. http://dealbook.nytimes.com/2013/12/09/for-bitcoin-square-peg-meets-round-hole-under-the-law/?_r=0 (last visited Feb 24, 2016)

administrator or an exchanger is an MSB operator under the regulations as it acts as a money intermediary; unless a limitation to or an exemption from the definition specifically applies. The administrator or the exchanger is not a supplier or a vendor of prepaid access, or a merchant in foreign exchange, under the regulations.⁵³

The definitive classification under the FinCEN guideline makes it very easy to identify those who are subject to the regulations of the BSA. Under this guidance, Virtual currency or Bitcoin administrators and the exchangers are required to report details of transactions including the identity of their clients.⁵⁴

FinCEN's guideline extends to some extent to include the virtual currency into the scope of application of the regulations. However, there is still a gap. Criminals using virtual currency or bitcoin for illegal activity can avoid U.S. anti-money laundering regulations by establishing the exchanger and/or the administrator in a country where financial regulations are weak. Users of Bitcoin who want to avoid the strict requirements on Bitcoin exchanges in the U.S. can also use exchangers or wallet services in countries with the lowest financial regulation. When the money is converted to Bitcoin, the user is free to transfer the funds without being monitored under the BSA and the US Patriot Act ("UPA"). Until there is a solution established, Bitcoin can be a channel for criminals to launder the money.

The FinCEN guideline does not make any difference to the interpretation of individual users. Therefore, unless clients are holding Bitcoin and executing the transactions through a regulated entity under to the U.S. anti-money laundering laws, the activities and movements of the Bitcoin will not be regulated.⁵⁵ FinCEN should also bring into its consideration of the situation where the Bitcoin transactions involve financial institutions in the countries in which regulations on virtual currencies are weak. The aforesaid is to efficiently prevent the conversion of the proceeds of crime back into the standard financial system.⁵⁶

⁵³ The Financial Crimes Enforcement Network, *FIN-2013-A001: Update on Tax Refund Fraud and Related Identity Theft*, 2013.

⁵⁴ Pamplin, Berkley A., *supra* note 50.

⁵⁵ Henning, Peter., *supra* note 51.

⁵⁶ *Id.*

3.1.2 The Bank Secrecy Act (“BSA”)

This BSA does not address the law of money laundering, but it imposes obligations of record keeping, record maintenance, and reporting models on the financial institutions. This allows the regulators to identify the information about the source, volume, and movement of money through financial institutions within the United States.⁵⁷

The record keeping and reporting requirements under the BSA include Currency Transaction Reports (“CTR”). The CTR requires financial institutions to report cash transactions involving an amount more than \$10,000.⁵⁸ It requires that the individual conducting the transaction be legitimately recognized. The financial institutions have to appropriately maintain records of financial transactions. The financial institutions also have to file CTR to FinCEN additional financial information according to the law requirements. The BSA characterizes a financial institution in the United States broadly to prohibit an escape from the reporting requirements. Consequently, there are several types of “financial institution” under this act which state in appendix d thereof.⁵⁹

The BSA sets standards of identification requirement for the individual conducting cash transactions. For the purpose of helping the government agencies to prevent and to suppress the money laundering activity, the financial institution is required to report cash transactions of value as specified as well as transactions suspicious of involving with money laundering. The Act prescribes punishment on financial institutions and related business that fails to comply with the requirements.

⁵⁷ *Id.*

⁵⁸ Cornell University Law School. 31 CFR 103.22 - Reports of transactions in currency. | US Law | LII / Legal Information Institute (2015), Legal Information Institute (2015), <https://www.law.cornell.edu/cfr/text/31/103.22> (last visited May 25, 2016)

⁵⁹ Federal Financial Institutions Examination Council. Bank Secrecy Act anti-money laundering examination manual appendix d: Statutory definition of financial institution. https://www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_104.htm (last visited May 24, 2016).

The Act also imposes both civil and criminal liabilities, including fine and/or imprisonment, for operating an unlicensed or unregistered money transmitting business.⁶⁰

3.1.3 The Patriot Act 2001

In this thesis, the writer focuses on Title III of the Act re International Money Laundering Abatement and Antiterrorist Financing Act of 2001 relating to the anti-money laundering regulation. Under this title, the law encourages anti-money laundering and prevention of terrorism financing in the international scheme. It essentially revises segments of the Money Laundering Control Act of 1986 (MLCA) and the Bank Secrecy Act of 1970 (BSA). It can further divide into three subtitles as follows:

- (A) International Counter Money Laundering and Related Measures
- (B) Bank Secrecy Act Amendments and Related Improvements
- (C) Currency Crimes and Protection

Subtitle A is to escalate capability of banking rules against money laundering, especially on the international field. Subtitle B is to create the coordination between state agencies and financial institutions, as well as to expand record-keeping and reporting information according to the requirements. Subtitle C deals with currency smuggling and counterfeiting, including the increasing the maximum penalty for counterfeiting foreign currency.

This Act supplemented the BSA outline by improving the processes of customer identifications require to performed by financial institutions to meet the requirement through the Know Your Customer (“KYC”) procedures. This process is a merger of two requirements i.e. Customer Identification Program (“CIP”) and Customer Due Diligence (“CDD”). It requires the financial institutions to gather minimum information of their customers in the process of opening accounts and customer identity authentication.

⁶⁰ 18 U.S.C. § 1960 <https://www.gpo.gov/fdsys/pkg/USCODE-2010-title18/pdf/USCODE-2010-title18-partI-chap95-sec1960.pdf> (last visited May 31, 2016).

There is also a requirement to monitor information of their customers using CDD procedures depending on the risk level of each customer.⁶¹ CDD requires the financial institutions to review the consistency of the transactions in accordance with the customer's expressed objective of using their account. The financial institutions are also obliged to create a security system to detect suspicious transactions and to provide alerts of relating suspicious activities.⁶² Moreover, this Act orders the financial institutions to create anti-money laundering programs up-to-date with the money laundering situation and strategy.⁶³

The disclosure of beneficial owner of the fund is essential to supervise the transaction which related to the money in pursuant to the legal requirement.⁶⁴

3.1.4 Internal Revenue Service

The U.S. Internal Revenue Service ("IRS") issued Notice 2014-21 which contains tax regulations and guidelines concerning virtual currency and virtual currency economics under the governance of the IRS. The Notice appears that the IRS has adopted different meaning virtual currency from the meaning provided by FinCEN guideline released in 2013. While FinCEN defines virtual currency as a store of value⁶⁵, IRS treats virtual currencies as property, similar to stocks and securities and will apply capital gains tax, unearned income tax, and ordinary income tax.

Virtual currency involves in exchange for goods or services as a payment instrument. Value of the virtual currency can be determined by its fair market value and may be considered as taxable income.⁶⁶

⁶¹ Federal Financial Institutions Examination Council, *supra* note 11.

⁶² The Patriot Act 2001, Title III, Subtitle B, sec 362. [hereinafter *The Patriot Act*]

⁶³ The Patriot Act, *supra* note 61, Title III, Subtitle B, sec 354.

⁶⁴ The Patriot Act, *supra* note 61, Title III, Subtitle A, sec 311.

⁶⁵ FATF REPORT, *supra* note 19.

⁶⁶ Langhirt, Joseph H., Plewa, David., and Greenberg, Michael. "Bitcoin is property, not currency, IRS says – Notice leaves many open questions about convertible virtual currencies", Apr 3, 2014. <https://www.dlapiper.com/en/us/insights/publications/2014/04/bitcoin-is-property-not-currency/> (last visited May 24, 2016).

By the fact that the IRS defines virtual currency as property, there is discrepancy in meaning used by IRS and the one given in FinCEN's guideline in which virtual currency is considered as money (the guideline requires virtual currency exchangers and administrators or any person who engages in an activity that facilitates the transfer of money domestically or internationally to register as a Money Service Business, the term is defined as a licensed sender of money).⁶⁷

3.1.5 The Annunzio-Wylie Anti-Money Laundering Act of 1992 (“AWAML”)

AWAML mandates the Nonbank financial institution to comply with general regulations regarding the filing of Suspicious Activity Reports (“SAR”), which are reports of suspicious financial activity required to be submitted to FinCEN and agencies of the U.S. Department of the Treasury when such activity meets specified criteria.⁶⁸ It also prescribes the requirements for identification and verification of individuals conducting wire transactions and retaining records of such transactions in the United States.

In addition, AWAML has been amended to support and strengthen the punishment for infringement of BSA.⁶⁹ It is stated in the Act that “Amends the Federal criminal code to establish criminal penalties for persons participating in an illegal money transmitting business.”⁷⁰

3.1.6 The Money Laundering Suppression Act of 1998 (“MLSA”)

The MLSA requires the owner or authorized person of the Money Services Business (“MSB”) to register with relevant authorities and to maintain a list of businesses in connection with the financial services offered by the MSB in which the

⁶⁷ Smith, Bryan. 'A Close Look at the IRS' Bitcoin Guidance', 2014.

<http://www.law360.com/articles/524285/a-close-look-at-the-irs-bitcoin-guidance>
(last visited May 29, 2016)

⁶⁸ Annunzio-Wylie Anti-Money Laundering Act subtitle b [hereinafter *AWAML*].

⁶⁹ Federal Financial Institutions Examination Council. *History of Anti-Money Laundering Laws*, https://www.fincen.gov/news_room/aml_history.html (last visited May 29, 2016)

⁷⁰ AWAML, *supra* note 67.

MSB acts as an agent. The MLSA also makes an operation of MSB without a license a federal crime and recommends the states to adopt the same into their state laws concerning MSB.⁷¹

3.1.7 Money Laundering Control Act of 1986

Money Laundering Control Act outlines fundamental principle of anti-money laundering regulations to categorize money laundering offence as a federal crime. It forces the State or Federal laws to follow the guidelines for the process of reporting the required transactions.⁷²

It also imposes civil and criminal penalties for infringement of BSA regulations and guides the financial institutions to build and maintain strategies to guarantee comply with the reporting and recordkeeping requirements under the BSA.⁷³

3.1.8 New York Codes, Rules and Regulations

New York State's financial regulators announced a proposal which is the first regulations concerning virtual currency. It defines more precise definitions of virtual currency and relating business so that they are under efficient supervision. According to the definition provided under the Regulations, "virtual currency" means any digital unit used as a medium of exchange in a form of digitally stored value or that was incorporated into the payment system. The term virtual currency shall be broadly construed to include digital units of exchange that (i) have a centralized repository or administrator; (ii) are decentralized and have no centralized repository or administrator; or (iii) may be created or obtained by computing or manufacturing effort. Virtual currency shall not be construed to include digital units that are used solely on online gaming platforms, and are not usable with any application outside those gaming platforms. Nor shall the term virtual currency be interpreted to include digital units that are used exclusively as part of a customer affinity or rewards program, and can be

⁷¹ *Id.*

⁷² Money Laundering Control Act of 1986, Title 18, Part 1, Chapter 95, § 1956. Laundering of monetary instruments, article (a).

⁷³ *Id.*,

claimed solely for payment from the issuer and other designated merchants, but cannot be converted into, or redeemed for, Fiat Currency.⁷⁴

Another important defined term “Virtual Currency Business Activity” to which meaning is given as the conduct of any one of the following types of activities performed in New York or by a New York Resident:

(1) receiving Virtual Currency for transmission or transmitting the same;

(2) securing, storing, holding, or maintaining custody or control of Virtual Currency on behalf of others;

(3) buying and selling Virtual Currency as a customer business;

(4) performing retail conversion services including the conversion or exchange of Fiat Currency or other value into Virtual Currency, the conversion or exchange of Virtual Currency into Fiat Currency or other value, or the conversion or exchange of one form of Virtual Currency into another form of Virtual Currency;

(5) controlling, administering, or issuing a Virtual Currency.⁷⁵

Bitcoin supporters view that the definitions above are very strict. The regulation is similar to FinCEN’s as it by requires a virtual currency related business to apply for a license to operate the business, known as a Bitlicense. The Bitlicense holders are required to implement anti-money laundering schemes, particularly, the CDD and Enhanced Due Diligence (“EDD”) prescribed by the Patriot Act. Accordingly, the holders will need to have tools to collect and store information of the customers, and to examine the information of clients. The holders must also establish a cyber-security program to protect their customers from digital crimes.⁷⁶

The Code also determines a recordkeeping program imposing the virtual currency businesses to keep document and transaction records for not less than

⁷⁴ New York Codes, Rules and Regulations, sec 200.2 (m) [hereinafter *New York Codes*].

⁷⁵ New York Codes, *supra* note 73, sec 200.2 (n).

⁷⁶ Alvarez, Edgar. “*New York wants Bitcoin exchanges to be heavily regulated*”. 2014. <https://www.engadget.com/2014/07/18/new-york-cryptocurrency-regulations/> (last visited May 30, 2016).

ten years from the date of execution and made available for the regulator to review compliance with requirements of laws and regulations.⁷⁷ The data requirement that obtained from the customer and the transaction records have to maintain without limitation by each licensee as described in section 200.12 (a).⁷⁸ The objective of the data retention requirement is for the purpose of auditing transactions trail.⁷⁹

⁷⁷ New York Codes, *supra* note 73, sec 200.12.

⁷⁸ New York Codes, *supra* note 73, sec 200.12 (a)

“...The books and records maintained by each Licensee shall, without limitation, include:

(1) for each transaction, the amount, date, and precise time of the transaction, any payment instructions, the total amount of fees and charges received and paid to, by, or on behalf of the Licensee, and the names, account numbers, and physical addresses of the parties to the transaction;

(2) a general ledger containing all assets, liabilities, capital, income, expense accounts, and profit and loss accounts;

(3) bank statements and bank reconciliation records;

(4) any statements or valuations sent or provided to customers and counterparties;

(5) records or minutes of meetings of the board of directors or an equivalent governing body;

(6) records demonstrating compliance with applicable state and federal anti-money laundering laws, rules, and regulations, including customer identification and verification documents, records linking customers to their respective accounts and balances, and a record of all compliance breaches;

(7) communications and documentation related to investigations of customer complaints and transaction error resolution or concerning facts giving rise to possible violations of laws, rules, or regulations;

(8) all other records required to be maintained in accordance with this Part; and

(9) all other records as the superintendent may require.”

⁷⁹ New York Codes, *supra* note 73, sec 200.16.

This regulation intends to ensure that virtual currency service business (which is a new financial innovation playing a role in the business or transaction at this present as a mimic of the fiat currency) and relating persons thereto are supervised and regulated by the rules and regulations. It provides a good direction to supervise virtual currency by requiring the operator of the virtual currency business to be licensed; so that such operator is obliged to comply with the requirements of this regulation. Therefore, New York State intends to treat virtual currency and related parties in the same manner regular payment, financial institutions, banks and other business related to regular payment are treated.

3.2 Case Study in the United States

3.2.1 The Liberty Reserve Case

In 2013, the US Department of Justice arrested Liberty Reserve, a Costa Rica-based cash transmitter, and seven of its principals and supporters which are the biggest online money laundering operation ever. This company operated unlicensed money transfer businesses and participated in money laundering activities that have solicited procession of plenty of funds. It was found that digital currency had taken important roles in the processes to launder more than 6 billion US dollars illegal money.

Liberty Reserve was established in 2006, having an objective to eliminate loopholes in legal enforcement or investigation that allow criminals to distribute, store and launder the proceeds of credit card fraud, computer hacking, identity thieves, child pornographers, drug trafficking⁸⁰ via a system that functions anonymous and untraceable transactions. There are about a million user accounts on this system internationally, in which about two-hundred thousand accounts in the United States. The system administers about fifty-five million online transactions mostly of which are unlawful. Liberty Dollar (LR) is a virtual currency used in

⁸⁰ Robbins, Seth. *"Liberty Reserve Case Exposes New Frontiers in Laundering Digital Cash"*, June 4, 2013. 2013 <http://www.insightcrime.org/news-analysis/liberty-reserve-case-exposes-new-frontiers-in-laundering-digital-cash> (last visited May 24, 2016).

transactions on this system and can be converted into a real currency i.e. US Dollar.⁸¹ Liberty Dollar is different from Bitcoin because it is a centralized virtual currency under central operation and control of Liberty Reserve.

The processes of using this currency started from a user opening an account on the website of Liberty Reserve by providing basic identifying information such as e-mail address, name, and physical location. There was no process to verify the information. Thus, such information could be fake. Most users created accounts with fake names or addresses to conceal their actual identity.

To further enhance privacy, the users were required to process transactions through outsourcing exchangers designated by Liberty Reserve. These illegal money exchanges were generally made to countries where government's supervision or regulations are weak, for example, Malaysia, Russia, and Vietnam. Liberty Reserve maintained a strategic distance from direct stores and withdrawals from clients to dodge gathering data about them through keeping money exchanges or other action that would make records, making it tough to verify or collect real information of any transactions.

The Liberty Reserve currency could be traded only among Liberty Reserve clients, and was exchangeable with anything including benefits from crime for the purpose of money laundering. The company charged one percent fee for each exchange, which was much lower than any fee of the bank, plus an extra charge at 75 cents as a privacy fee to ensure that clients could conceal their account when doing the transaction, making them an entirely trackless account. The process to withdraw the money was switched, with the Liberty Reserve money doing a reversal to a cash exchanger who then transformed it into any legal currency.

Liberty Reserve's money framework had qualities that were alluring to criminal associations. The attractive primary characteristic of Liberty Reserve was anonymity. To build up an account, a client was just expected to give a name, address, and date of conception, yet there were no personality confirmation forms for the benefit of Liberty Reserve account to verify the character of its clients. As per the creators, covert specialists could open a record utilizing a false name and portrayed the

⁸¹ FATF REPORT, *supra* note 19.

motivation behind the record as "for cocaine" however Liberty Reserve never detected this. The second particular being attractive to criminal associations was the accessibility of the system. Liberty Reserve clients could get to their accounts online and approve exchanges within a few minutes. The diagram which shows beneath gives a graphical representation of the Liberty Reserve architectural planning.

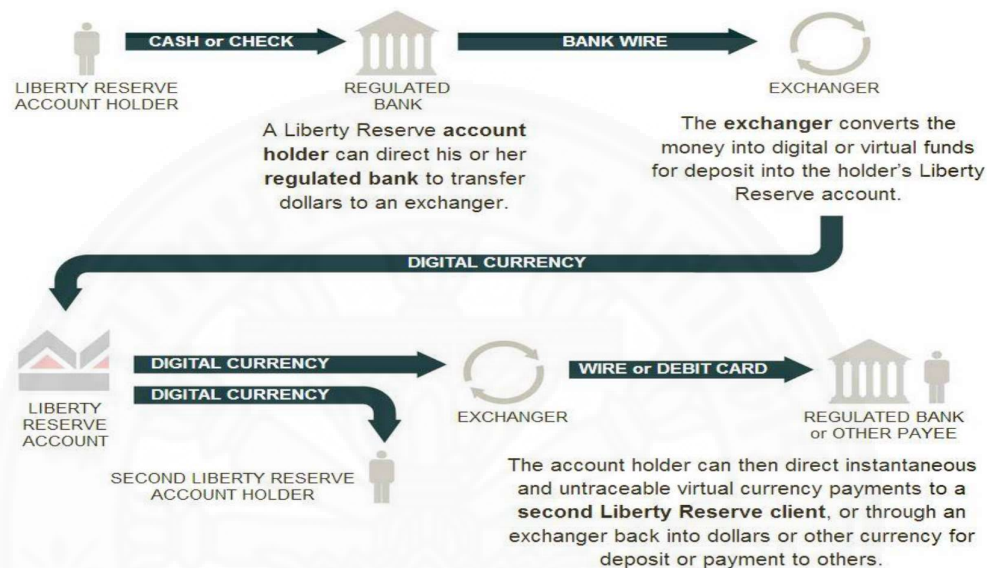


Figure 4. How Liberty Reserve's Currency Works⁸²

According to US federal indictment unsealed in May 2013,⁸³ there are three offenses in the indictment as follows:

1. Conspiracy to Commit Money Laundering
2. Conspiracy to Operate Unlicensed Money Transmitting Business
3. Operation of an Unlicensed Money Transmitting Business

It was the Patriot Act that eventually prompted the suppression of Liberty Reserve. These criminal activities violated the MLSA and the Patriot Act. During the operation of Liberty Reserve, 6 billion U.S dollars had been laundered and conveyed through the site to facilitate crimes including human or drugs trafficking,

⁸² The New York Times. "How Liberty Reserve's Virtual Currency Works", 2013. http://www.nytimes.com/interactive/2013/05/29/nyregion/how-liberty-reserves-virtual-currency-works.html?_r=0 (last visited Feb 10, 2016).

⁸³ US Federal Indictment 13 CRIM 368, United States v. Liberty Reserve S.A. (2013).

stolen identities, child pornography, and other illicit activity.⁸⁴ The Liberty Reserve action is cited as the largest money laundering indictment in the history of the United States. This case researched and captured included law implementation activities in 18 nations and locales, for example, Costa Rica, Netherlands, China, the United Kingdom, Canada and the United States to prevent criminal continues, relinquish area names, and seize servers.

The Liberty Reserve's site was removed from the internet on May 24, 2013, and supplanted with a notification saying the domain had been "seized by the United States Global Illicit Financial Team." In Costa Rica, a court request was issued to grab the "money related items and administrations" of Budovsky, Maxim Chukharev, and the six evident shell organizations. More than a million dollars of extravagance autos alone were seized.

The lesson learnt from this case was that the law should focus on the licensing requirement on a money transmitting business operator, who may relate to the money laundering in a way of providing a virtual currency service to be used among its users as a medium of exchange instead of fiat money. It also has the additional service that intends to make anonymity account to conceal the real owner and difficult to verify the information of the transaction. For this reason, it creates a convenient financial transfer system for customers and also criminals who can use it to launder the money by the digital services and virtual currency without any monitoring on data of their customers in compliance with KYC & CDD procedures according to the law and regulations. Therefore, this operator has to be punished for the offence of operating the unlicensed business in violation to the relating regulations.

3.2.2 Silk Road Case

Another company charged of committing criminal offences related to digital currency was Silk Road which was the hidden website for the purposes of buy and sell illegal drugs, weapons, stolen identity information and other unlawful goods and services through anonymous criminal transactions not being within scope of legal

⁸⁴ Perlorth, Rashbaum, Santora, *"Online Currency Exchange Accused of Laundering \$6 Billion"*, 2013. <http://www.nytimes.com/2013/05/29/nyregion/liberty-reserve-operators-accused-of-money-laundering.html> (last visited Feb 10, 2016).

enforcement and also outside the regulations of drug trafficking, computer hacking, and money laundering conspiracies.⁸⁵ These operation involved over a hundred thousand users who allegedly made total sales income of about 1.2 billion US dollars (more than 9.5 million bitcoins or 4.2 ten billion Baht) and the revenue from the commissions for Silk Road about 80 million US dollars (Commissions fee ranged from 8-15 percent of total sales price). Thus, it can be seen that the vast amount of money laundered could be performed via these outlaw transactions causing impact directly on the world economy and wider society.⁸⁶

Beginning from January 2011, Silk Road operated as a worldwide cyber market trade society acting as a middleman to service money laundering process via anonymous transactions between unlawful users and vendors to distribute illegal goods and services to other users. It operated on a hidden network called "Tor" connected through the Onion Router, an underground system of PCs online arranged by the web. It had essential capacities that cover valid IP addresses and personalities of the clients. These capacities performed by steering interchanges and exchanges, passing through different PCs around the globe and pressing data in a differentiated layer of encryption. Therefore, this network created a serious problem to the legal enforcement and regulators to monitor and investigate illegal transactions because it was difficult to find real locations of the computers facilitating or getting to the sites through the system.⁸⁷

In addition to the network complexity, the site accepted only bitcoins for payment. Silk Road only used this virtual currency as the intermediate for buyers and sellers to another conceal their identity via the shared peer-to-peer (P2P) framework. Bitcoin exchanges are distinguished just by the unknown bitcoin address or record which clients can get boundless addresses and can choose one location for every exchange. Also, there was another additional choice known as "anonymisers"

⁸⁵ United States v. Ulbricht, USA-33s-274 U.S. 1, 1-4 (2014).

⁸⁶ Calvery, *supra* note 36, page 12-13.

⁸⁷ Olson, Parmy. "The man behind Silk Road – the internet's biggest market for illegal drugs", November 10, 2013. <https://www.theguardian.com/technology/2013/nov/10/silk-road-internet-market-illegal-drugs-ross-ulbricht> (last visited May 31, 2016).

which passed the general administration into Silk Road exchanges to hide and cover the real identity and the source of the transaction.⁸⁸

The trail analysis issues about privacy, anonymity, and the practices of law enforcement. However, the most important factor is the capability of the law enforcement to examine and detect the criminals online. The concept of the anonymous is the core of the problem because it brings the complex data and process to examine the real person behind each account. The criminal will use this closed network system in committing the money laundering via online network to make it difficult to detect any related party to the transaction.⁸⁹

The task force was able to identify the sites creator “Dread Pirate Roberts” as Ross Ulbricht, who based in San Francisco, CA. However, the ability of investigators to identify Ulbricht was again, not the result of following a trail of transactions, or determining an IP address. Law enforcement identified Ulbricht by a series of careless missteps by the creator. These missteps led to the arrests of large merchants and administrators of the Silk Road.⁹⁰ Other mistakes made by Ulbricht were simple, like Ulbricht using an open Gmail account on an online forum discussing the Silk Road that traced back to Ulbricht possibly being the creator.

Ulbricht was arrested in October 2013, and indicted in a federal court for narcotics trafficking conspiracy, continuing criminal enterprise, computer hacking conspiracy, and money laundering conspiracy. The indictment states that “the defendant (Ulbricht), knowing that some of the property involved in certain financial transactions represented the proceeds of some form of unlawful activity, would and did conduct and attempt to conduct such financial transactions with the intent to promote the carrying on of such specified unlawful activity.” Therefore, Ulbricht was charged with money laundering conspiracy. The website was also seized, and approximately

⁸⁸ FATF REPORT, *supra* note 19.

⁸⁹ Morrison, Kimberlee. “*Silk Road Trial Becomes Case Study for Law Enforcement Online*”, Jan 13, 2015. <http://www.adweek.com/socialtimes/silk-road-trial-becomes-case-study-for-law-enforcement-online/612298> (last visited Jun 1, 2016)

⁹⁰ *Id.*

173,991 bitcoins, which has valuable about 33.6 million USD at the time of the seizure, was seized together with all of the computer tools.⁹¹

Bitcoin exchanges were intended to be entirely anonymous. However, the aftereffect of the Silk Road examination brings up the issue of the monitoring in virtual currency users that could be distinguished and supervising the Bitcoin framework.

Examiners could perform a legal investigation of the Silk Road servers to recognize a \$2.9 million account held by Dwolla, an auxiliary of the world's biggest Bitcoin trade, Mt.Gox, and two Wells Fargo accounts holding \$2.1 million that utilized by the overseers of the Silk Road. Even though investigators located \$5 million in real currency in the Dwolla account and the Wells Fargo account, another \$28.5 million was discovered in a Bitcoin wallet tide back to Ulbricht, and investigators were not confident that all of the Bitcoins owned by Ulbricht contained in this one wallet.

3.2.3 Trendon T. Shavers Case

This case is about the fraud trading of securities by Shavers and the Bitcoin Savings and Trust (“BTCST”), a Bitcoin-designated Ponzi scheme established and performed by Shavers. It was involved with Bitcoin, so the court has defined that Bitcoin (“BTC”) as “a virtual currency that may trade on online exchanges for conventional currencies, including the U.S. dollar, or used to purchase goods and services online. BTC has no single administrator, or central authority or repository.”⁹²

The essential issue that should be considered is the legal status of Bitcoin and BTCST. Hereupon, the Court must determine whether the Bitcoin Savings and Trust (“BTCST”) investments constitute an investment of money. It is clear that Bitcoin can use as money. It can be used to purchase goods or services, and as Shavers stated, used to pay for individual living expenses. The only limitation of Bitcoin is that

⁹¹ Leger, Donna L., USA TODAY. *"How FBI brought down cyber-underworld site Silk Road"*, 2014. <http://www.usatoday.com/story/news/nation/2013/10/21/fbi-cracks-silk-road/2984921/> (last visited Jun 1, 2016).

⁹² Securities and Exchange Commission v. Trendon T. Shavers, et al. The Complaint, (2014). <https://www.sec.gov/litigation/complaints/2013/comp-pr2013-132.pdf> (last visited Jun 7, 2016).

it is limited to those places that accept it as currency. However, it can also be exchanged for conventional currencies, such as the U.S. dollar, Euro, Yen, and Yuan. Therefore, Bitcoin is a currency or a form of money, and investors investing in BTCST are considered investing money.

The Court finds that the BTCST investments meet the definition of investment contract, and as such, are securities. Accordingly, the Court concludes that it has subject matter jurisdiction over this matter⁹³, under the Securities Act of 1933⁹⁴ (the “Securities Act”) Sections 20 and 22 and the Exchange Act of 1934 (the “Exchange Act”) Sections 21 and 27.⁹⁵

In this case, the court accepted bitcoin as money or a form of money which is an intermediary in exchange of goods and services depending on each or social that recognize this thing can use instead of the money.⁹⁶ So, it can exchange to the other formal currency such as U.S. dollar, Euro or Baht. It also can be used as a channel to get the interest from the bitcoin investment.

Consequently, to compare with the laws and regulations in the United States described herein above, Thailand does not have any laws and regulations that relating to virtual currency. The Bank of Thailand (“BOT”) just give some cautions about virtual currency notably bitcoin to the public because it can be used to commit the crime through the virtual currency system. Moreover, the legal status of virtual currency is still unclear in Thailand. For this reason, the government and related organization or institutions must manage and supervise the virtual currency and other involving business or person to be under the laws and regulations especially in the prevention and suppression of money laundering. Because these things can use as a channel for laundering illegal money or asset and it is still not regulated by the legislations.

⁹³ Mazzant, Amos L. United States Magistrate Judge, Case No.4:13-CV-416, 'Memorandum Opinion Regarding the Court's Subject Matter Jurisdiction', 2013.

⁹⁴ 15 U.S.C. §§ 77t and 77v.

⁹⁵ 15 U.S.C. §§ 78u and 78aa.

⁹⁶ Securities and Exchange Commission v. Trendon T. Shavers, *supra* note 91.

CHAPTER 4

ANTI-MONEY LAUNDERING AGAINST VIRTUAL CURRENCY UNDER THAILAND REGULATION

The Virtual Currency situation has played more role than before and causes an impact at the international level and also in Thailand, which has several virtual currency businesses operate in the country. People begin to recognize and use the virtual currency as the financial tools like the money or credit. The method of the virtual currency causes a higher risk of money laundering when it can be used instead of the usual money because there are no specific legislations to be considered in the case about virtual currency. However, the government, related institutions, and other authority beware and warn about this currency and try to manage or control against the offense.

The criminal knows about the problem of the laws, so they changed the process of laundering the dirty money from the real currency to use the virtual currency to conceal the sources of funds in order to obstruct the trace back to the real beneficial owner. The other issues that should be considered include the investigation and the enforcement against the criminal that uses virtual currency as a medium of illegal exchange of things or money.

Like other countries, and as per the universal focal managing accounting standards, in Thailand, there is the Bank of Thailand (BOT) which is the central organization that maintains and administers the monetary economy, the money related foundation framework and the installment framework security and effectiveness of the nation. Also, Thailand has the act of legislations involving the financial and banking, namely Financial Institution Businesses Act, Currency Act, and Exchange Control Act. In Thailand, there is no any regulation specifically governing virtual currency. The government does not accept this kind of the digital data unit as money that can be used to pay in legal tender. However, it is not illegal or forbidden. Nevertheless, the Bank of Thailand (BOT), which is the central organization that supervises the financial sectors of the country, has issued comments about the information of this financial innovation.

There are many regulations that could be used to enforce or regulate the virtual currency. However, in this thesis, the writer will focus on the Anti-Money Laundering Act B.E. 2542 first and try to interpret and adapt other provisions to resolve this issue.

4.1 Current Thai Regulations on Virtual Currency Money Laundering

Thailand has joined as a party to United Nations Convention against Illicit in Narcotic Drugs and Psychotropic Substance (1988) (“Vienna Convention”) already. This convention determines each member state to establish and update its domestic law to meet the universal standard. In addition to this covenant, there are the recommendations on Anti-Money Laundering method provided by the Financial Action Task Force (“FATF”)⁹⁷ for use in setting up the rules and regulations. Thailand is the party of the Vienna Convention, so the government has to amend and set up the internal laws and procedures to meet the international standard.

These convention and recommendation are the important principles which apply to formulate the Anti-Money Laundering Act B.E.2542 (1999) of Thailand, which has been used for more than ten years. From the enactment, the social surrounding has changed dramatically. For this reason, the laws and the regulations are out-of-date and cannot be enforced efficiently. The gap in the law causes impact to the whole economic of the country, and may trigger the sanction by FATF because of these lack-of-supervision circumstances.

The key fundamental principle about the Anti-Money Laundering is the predicate offence that determines about the crime which is the cause of the interest or any property that acquired from the offence. Almost all of the criminal offences stipulated in the AMLA are predicate offences. The AMLA addresses certain predicate offences but less than the recommendations of FATF, so Thailand has improved the regulation by adding more predicate offences to the standard level. In AMLA there are

⁹⁷ Financial Action Task Force (FATF) was established by G-7 countries which have 40 recommendations about the Anti-Money Laundering to be the guidelines of the amendment the new laws and regulations of the country.

the regulations which have the criminal and civil measures to force and punish the wrongdoer and the asset or proceeds which obtained from predicate offences.

The AMLA has been continuously developed and updated to suit with the developing countries and the modern edge of technology. For purposes of efficient legal enforcement and competence of the law to monitor new offences that have changed all the time, the whole related divisions have to be more proactive than before and build up the synergy between the government organizations and private sectors.

The trend of business crime is rising according to the Basel AML Index Ranking in 2012-2015 (Public version)⁹⁸ which is a yearly positioning evaluation nation risk on

⁹⁸ The fourth version of the Basel Anti-Money Laundering (AML) Index created by the Basel Institute on Governance. The Basel Institute distributed the Basel AML Index without precedent for 2012 and has from that point forward been the main non-benefit association to make an exploration construct positioning centering in light of the danger of money laundering and terrorist financing. The Basel AML Index gives the accompanying key elements to an overview of 152 nations as indicated by their risk level in money launder and terrorist financing. And composite record taking into account on the public sources and outside evaluations. In this index, it is independent exploration based risk positioning which is updated every year so AML nation risk evaluation instrument for consistency purposes of development the effective laws and regulations of the country to reduce the risk of money laundering and terrorist financing.

The Basel AML Index 2015 Report abridges the key discoveries and gives an itemized clarification about the approach in yearly audit segment diagrams the primary examinations and input got from external specialists with scholastic, supervisory and law enforcement basis.

This Index creates the measures the risk of money launder and terrorist financing of countries taking into account from publicly available sources. A sum of 14 indicators that deal with AML/ CFT regulations, defilement, monetary principles, political revelation and the rule of law are amassed into one general risk point. By consolidating these different information sources, the overall risk score demonstrates a holistic assessment addressing structural as well as functional elements in the

money laundering and terrorism financing structures and other related variables, for example, money related/open straightforwardness and the right quality.

Year	Overall Score	Ranking
2012	6.46	40
2013	6.56	41
2014	6.53	49
2015	6.52*	45

(0 = Low Risk, 10 = High Risk)

(* Overall Score based on a new FATF evaluation, which includes an effectiveness assessment)

This chart shows the overall score and ranking of Thailand. In 2015, Thailand was scored 6.52 point and ranked at the 45th of 152 countries, down from the year 2014 which indicated the trend of money laundering in Thailand is likely higher.

From the result, Thai government has to bring this matter to its priority because this is the important issue which relates to the economic in overall of the country. If Thailand is still in the high-risk ranking, it will be impacted by the economic conditions and the commercial, both domestically and internationally, because the other countries have concern that contractor doing business in Thailand may involve in money laundering. This ranking makes the countries aware of this important issue to find the way to handle it as a high feature of the civilized country. Money Laundering is the criminal offence of the Economic and Commercial Crime which affected the economy system, the security of the country, and also take more effect to the regulation.

The criminal have changed their process and behavior to avoid the law. Therefore, it causes an increase of proceeding of crime more than the past. Anti-Money

AML/CFT framework. As there are no quantitative data available, the Basel AML Index does not quantify the genuine presence of the operation of money laundering or amount of illicit financial money within a country but it is intended to display the level of risk through the delicateness of money laundering and terrorist financing inside of the nation.

Laundering is the fundamental principle of the international legal structure⁹⁹ that every country have to amend or provide this principle to the new statute or regulation in domestic law.

4.1.1 The Anti-Money Laundering Act B.E.2542

This act aims to prevent money laundering, force against the offender and manage the asset or money from the offence to eliminate the proceeds of crime which can be the fund for the criminal to commit another offence. It is significant to have the regulation that follows the international standards. This law has to update the rule and process to be recognized and enforced effectively because the criminal has changed the way to commit the offence. The old laws are not suitable for the new offences. Therefore, the AML is a specific regulation to govern the offences by increasing the powers to conduct investigations and seizures and to attack the controversial issue of perceived government corruption.

A further amendment in 2009 was made to expand the types of businesses under the governance of the Act, and to impose reporting requirements on certain nonfinancial business in addition to financial institutions. Under this amendment, non-financial businesses, such as jewelry traders, car dealers, and real

⁹⁹ **The Government Gazette**, Vol. 120, Part 76a, page 4, dated 11th August 2003.

“There is a revision of the Penal Code recommending offenses identifying with terrorism. Financing of terrorism is a component helping the more brutal terrorism, which influences national security and which the United Nations Security Council encourages each nation and locale to coordinate with one another in the battle against terrorist acts, and additionally against procurement of money related backing of different implies that are expected for use in the terrorist demonstration, in order to end the terrorist issue. Terrorism should be recommended as a predicate offense under the Anti-Money Laundering Act B.E. 2542 (1999) so that these two laws can be facilitated in real life which will empower more noteworthy viability in the execution of this procurement in the Penal Code. Overriding need and crisis for defending the security of the Kingdom and the general population make it unavoidable to take and pressing measure. Thus, this Emergency Decree must be issued.”

estate brokers, are now required to report transactions that exceed the values prescribed in the relevant ministerial regulations.

Thai law enforcement officials initially proposed the enactment of a money laundering law to target the regular transfer of money and property derived from the rampant trade in illegal drugs, in order to comply with requirements for membership under the Vienna Convention. Additional predicate criminal offenses were added both during the legislative process and during subsequent amendments. The February 2013 amendments not only added twelve new categories of predicate offenses ¹⁰⁰ but also

¹⁰⁰ Ramirez, Michael. "*Jurisdiction update: Thailand — AML*", July 2, 2013.

http://www.tilleke.com/sites/default/files/2013_Jul_Complinet_AML_Thailand.pdf
(last visited April 2, 2016)

“Currently, the Act covers the transfer or conversion of funds or property obtained from the following predicate offenses:

1. Drug trafficking
2. Prostitution and other sexual offenses
3. Fraud against the public
4. Fraud involving financial institutions
5. Abuse of position by a government official
6. Extortion
7. Trade in contraband
8. Terrorism
9. Gambling offenses, with particular emphasis on large-scale organization of gambling games
10. Participation in racketeering groups or participation in a criminal association
11. Receiving stolen property only as it constitutes assisting in the selling, buying, pawning, or receiving, in any way, property obtained from the commission of an offense with the nature of business conduct

confirmed the application of the Act to predicate offenses committed outside Thailand, provided such acts would have constituted a predicate offense had they committed in Thailand.

There are three issues that should be considered in AMLA in the aspect of virtual currency

(1) Predicate Offence

There are many definitions about predicate offence depends on each country. It is the basis of the money-laundering offence under the AMLA. It is the

-
12. Counterfeiting or alteration of currencies, seals, stamps, and tickets with the nature of business conduct
 13. Criminal trading only where it is associated with the counterfeiting or violating of intellectual property rights to goods or the commission of an offense under the laws on the protection of intellectual property rights with the nature of business conduct
 14. Forgery of a document of right, electronic cards, or passports with a nature of regular or business conduct
 15. The unlawful use, holding, or possessing of natural resources or a process of illegal exploitation of natural resources with a nature of business conduct
 16. The commission of an offense relating to murder or grievous bodily injury which leads to the acquisition of assets
 17. Restraining or confining a person only where it is to demand or obtain benefits or to negotiate for any benefits
 18. Theft, extortion, blackmail, robbery, gang-robbery, fraud, or misappropriation with a nature of regular conduct
 19. Acts of piracy under anti-piracy law
 20. Unfair securities trading practice under the law on securities and stock exchange
 21. Offenses related to arms and arms equipment which is or may be used in combat or war under the law on arms control”

source of the criminal offence and become the subject matter of this offence. Originally, Thailand determines just a few crimes as predicate offences under AMLA. After that, there has been an updated version which adds in more serious crimes in order to meet the international standard. The predicate offence is a ground that leads to the application of the AMLA. In other words, the AMLA can be applied only when there is a suspect of the predicate offence listed therein. It is the subject under the AMLA and the subject to a characterized punishment under this regulation.¹⁰¹

It does not have predicate offences which related to the virtual currency or virtual currency service business as this is a new financial innovation and new business which is not under this regulation or other laws. So, this situation causes a risk of money laundering through the virtual currency instead of the money.

(2) Assets under AMLA

Under the AMLA, the regulator can inspect assets being suspect as proceeds of the predicate offence. The AMLA provides list of assets under its regulation, including money and property. It refers to the money or property that obtained from the commission of the predicate offence or money laundering offence or received from aiding and abetting or rendering assistance and also include the assets that used or possessed to use in the predicate offence. It also included the money or property that obtained from the distribution, disposal or transfer in any feature of money or property. It also including the fruits of the money or property of the money or property as mentions above. However, virtual currency does not fall within the definition of the assets provided thereunder.

The purpose of this law is to eliminate the cycle of the money laundering offence by focusing on the money or property that involved with the predicate offence; notwithstanding how many times the money or property has been transferred or changed hands from a person to another, or transformed into or exchanged for other property.

¹⁰¹ United Nations Office on Drugs and Crime,. *"Legislative framework: Criminalizing the laundering of proceeds of trafficking in persons"*. https://www.unodc.org/documents/human-trafficking/Toolkit-files/08-58296_tool_3-5.pdf (last visited Mar 3, 2016).

Furthermore, virtual currency is not acknowledged as money or property. Its status is still unclear. The government or BOT just caution about the risk of using virtual currency, but they do not confirm recognition of the legal status of virtual currency in Thailand. The status of the virtual currency in the eye of the law should be ascertained in order to mitigate the risk in using it.

(3) The Financial Institutions and Designated Non-Financial Businesses and Professions

Another important issue in the preventive measure is the data and risk management on specific businesses and their customers governed under this regulation. The issue is critical because the money laundering offence mostly involves banking or financial business which is the channel for criminal to exchange or transfer the proceeds of crime to other criminal or conceal the real source of the money or property.

Firstly, it focuses on The Bank of Thailand under Bank of Thailand Act, a commercial bank under the Commercial Bank Act or the provisions of a specific law not only the banking business but also including the Financial or Funding Business, credit foncier companies and Securities Business. This law aims to regulate the banking and financial business which are the source of the fund for the whole economy. These are essential for the supervision of financial transactions including the transfer of assets or exchange of money or things to other property.

The other risky business is the Insurance Business, including life insurance and casualty insurance. Some criminals launder the money through insurance business by paying the high insurance premium and receiving great interest in return. Again, it is difficult to detect or investigate the source of the funds.

The last one is the juristic person undertaking non-bank business related to finance as provided by the Ministerial Regulations. This kind of business is similar to the regular financial business or banking that the criminal will use as the channel for money laundering.

The Act does not mention about the business or any institution involving with virtual currency such as system operator or virtual currency market (like the capital market). It should consider the kind of virtual currency business in comparison with financial institution and other financial-related business. The purpose

of virtual currency service business is to function as the intermediary in exchange by servicing the exchange system or network to their customer. They can operate the exchange transaction or proceed the contract between the users by using virtual currency as to make payments instead of the real money. It seems to be a non-bank business, but it does not use money to pay for the transaction. Therefore, virtual currency is not in the financial system or the under any supervision of the country. This issue brings the risk of money laundering because of the lack of control and supervision of any authorities.

The virtual currency service business should be considered as one of the financial institution or other relating financial business; so that it would be under this Act and be imposed with the same duties as the financial institution or relating business as defined in this regulation to protect, prevent and detect the offence of the money laundering.

The Act requires financial institutions and other related business to fulfill three main duties as follows:

(3.1) The duty to report the transaction

This procedure is a very important step in the protection and promotion of law enforcement to be more effective. When the transaction takes place at the financial institution, the law requires a financial institution to report the transaction to the Anti-Money Laundering Office (“AMLO”).

In the process of money laundering, criminal will need to process transactions to move money or property received from the crimes. Therefore, it is important to consider the definition of the term “Transaction” under the law. According to the AMLA, Transaction means “any activity related to the juristic act, contract, or any commitment with other persons dealing with finance, business or involving assets.”¹⁰² It focuses on the transaction which is the basis for monitoring and supervision of the money or assets which are the trail of the money laundering offence.

¹⁰² Anti-Money Laundering Act B.E. 2542 sec. 3 [hereinafter AMLA]

“ ‘Transaction’ means any activity related to juristic act, contract, or any commitment with other persons dealing with finance, business or involving assets”

In addition to this law, there are other regulations that define the definition of the transaction which is quite the same as AMLA.

According to Civil and Commercial Code (“CCC”), the term “transaction” is not specifically defined. However, this law describes the primary principle of the juristic act and contract and provides definition of “Juristic Act” as “the voluntary lawful acts, the immediate purpose of which is to establish between person relations, to create, modify, transfer, preserve or extinguish rights”¹⁰³ ; and “Contract” as the “Juristic Act which formed by several parties under the intention of the parties by the intent of the offer and the corresponding must be matched that cause arises, modify or suspend the juristic relation.”¹⁰⁴

Applying the definitions given in the CCC, the virtual currency transaction in this matter can be regarded as the transaction under AMLA, and it can interpret as a juristic act or contract under CCC too. In a virtual currency transaction, there is a person using virtual currency to make payment, and another person accepting the virtual currency as payment. To execute a transaction to constitute a juristic relationship, a party has to express its intention to make an offer to another party and the latter has to express its intention to accept the same. However, these circumstances proceed through the online system network or the internet. It could compare to internet banking or electronic fund transfer which have a similar pattern of the transaction.

AMLA specifies the transactions which have to be reported in several categories depend on the object and objective of the transaction.¹⁰⁵

The first is the transaction that involves with cash in an amount equal to or exceeding the amount according to the criteria specified in the

¹⁰³ Civil and Commercial Code sec. 149 [hereinafter CCC]

¹⁰⁴ เณดิบัณชิตยศกา ในพระบรมราชูปถัมภ์. 'ลักษณะของสัญญา การแบ่งประเภทของสัญญา และการก่อให้เกิดสัญญา',

2555. (The Thai Bar under The Royal Patronage. *Feature of contract , Classification of contract and Causing of contract*, 2012). <https://www.thethaibar.or.th/thaibarweb/fileadmin/DAM/2555/PDF/Lecture/LectureTerm1/20/1.pdf> 9 (last visited Mar 4, 2016).

¹⁰⁵ The Anti-Money Laundering Act B.E. 2542 sec. 13 [hereinafter The AMLA].

Ministerial Regulations. The amount of the cash that triggers the obligation to report to the AMLO is two million baht for the general transaction, or a hundred thousand baht for money transfer or electronic payment by the cash; or seven hundred thousand baht in the case for money transfer by deduction the value of the money in a bank account.

The second is the transaction that involves with the asset of value equal to or exceeding the amount specified in the Ministerial Regulations. The value of the asset that triggers the obligation to report is five million baht.

The last one is the suspicious transaction, whether or not it relates to the transaction involving with the cash or the asset. This criterion does not have the stipulation about the transaction that must be reported to the AMLO. However, this regulation requires the financial institutions to use their discretion to review their customers' transactions, taking into consideration the ability of the customers to do the transaction.

These kinds of the transaction are the source of the financial institution duty to report to AMLO for the purpose of prevention, transaction management, and detection about the money laundering offence. However, it does not mention about the virtual currency business or business that involving with it. In this regards, it can be seen that there is no regulation or law to supervise or control the virtual currency, virtual currency service business, customer or the related person in this present. The lack of supervision in the reporting procedure in case of a suspicious transaction, cash transaction or asset transaction as defined above bring some problems leaving channels for money laundering through the virtual currency transaction. This is because virtual currency status is still unclear, and parties involve thereto are not under the obligation to report the transactions under the AMLA.

The objective of the law is trying to oversee the transactions. The reporting obligation is the significant duty of a financial institution and other related business, as this is a first step for supervising and monitoring the money laundering offence. Moreover, the law defines "Suspicious transaction" as "a transaction that is more complicated than the norm by which that transaction is usually conducted, a transaction that lacks economic rationale; a transaction where there is probable cause to believe that it was conducted for the purpose of avoiding the compliance of this Act; or a transaction related to or possibly related to a commission

of any predicate offense, whether the commission of such transaction is conducted once or more”.

The transaction in which virtual currency or bitcoin is used to make payment or to exchange with things or service may be considered as “Suspicious transaction” by analogy. Due to the main objective that the customer of virtual currency or bitcoin system to use it instead of the money but they have the same intention as the proceeding transaction normally.

It can be an activity related to the juristic act, the contract between the users, or the commitment to other customers by dealing with virtual currency because the customer or user accept to use its as medium of exchange like the money. For this reason, it has no doubt in the interpretation of this matter. It has to be treated under this law as well.

However, it does not have the regulation to control or supervise the virtual currency service business and also includes the requirement about the criteria of the amount of virtual currency transaction which have the duty to report to AMLO like the cash or property transactions.

(3.2) The duty to identify and review the information of the customers.

Another significant procedure to prevent and detect the money laundering offence in addition to the transaction reporting in 3.1 is the process of examining the identification of the customer. This procedure will reduce risks associated with the predicate offense under the AMLA, according to the international standards.

This process requires the financial institution and DNFBP to focus on their customer. “Customer” is given with different meanings, depending on the financial institution’s business. The “Customer” of the financial institution is an individual or a juristic person who has a relationship or transactions with the institution. Alternatively, the person who receives the benefit of a relationship or transaction at the end, or the authority who has the power to control or decision-making related to the relationships or transaction with other in the final stretch; while the “Customer” of DNFBP means a buyer or seller, according to the CCC.

Know Your Customer and Customer Due Diligence policies under this regulation apply to the financial institution. It can apply to DNFBP as it is not contrary to normal business operations. However, it must require its customer to have a presence in case of cash transactions which have a value from one million baht, unless they already have a presence. It also reports the suspicious transactions to AMLO, although it is not a cash transaction.

Under this principle, the financial institution and DNFBP have to consider especially and watch out for some customer. The definition of “Customers need to pay particular attention” means a customer who has a relationship involved with politics or has a resident or a source of their money is from a country that is not in uses or not applies under the recommendations of Financial Action Task Force on Money Laundering (“FATF”). Moreover, it does not have measurements to prevent and combat money laundering or the customer that proceed the suspicious transaction, or customers who have a career in the high-risk groups, such as businesses, trade gems or precious metals or International Exchange Business.¹⁰⁶

(3.2.1) Know Your Customer (“KYC”) process

It is a process of identifying information of the customers. Under the procedures as prescribed by the announcement of ministerial regulations. The financial institution must require all clients to show their identification before processing any transaction unless the customers have previously identified already.¹⁰⁷ The law also requires the financial institution to request their clients to

¹⁰⁶ สำนักงานป้องกันและปราบปรามการฟอกเงิน (ปปง.). 'มาตรการป้องกันปราบปรามการฟอกเงิน และการต่อต้านการสนับสนุนทางการเงินแก่การก่อการร้าย เรื่อง นโยบายการปฏิบัติตามหลักเกณฑ์การรู้จักลูกค้า/การตรวจสอบเพื่อทราบข้อเท็จจริงเกี่ยวกับลูกค้า ของสถาบันการเงิน และหน่วยธุรกิจ หรือผู้ประกอบการวิชาชีพที่ไม่ใช่สถาบันการเงิน' 2553. (Anti-Money Laundering Office (AMLO). *'Anti-Money Laundering Measures and Combating the Financing of Terrorism policy guidelines Know Your Customer / Customer Due Diligence of Financial Institutions and Designated Non-Financial Businesses and Professions, DNFBP'*, 2010). [http://www.amlo.go.th/amlofarm/farm/information/files/1\(3\).pdf](http://www.amlo.go.th/amlofarm/farm/information/files/1(3).pdf) (last visited Apr 6, 2016).

¹⁰⁷ AMLA, *supra* note 104, sec. 20.

record all facts that involving with the transactions.¹⁰⁸ If a client declines to record the fact in a report, the financial institution has to record all of the facts including the refusal of the client and then, report to AMLO immediately.¹⁰⁹

(3.2.2) Customer Due Diligence (“CDD”) process

Recommendation 5 of FATF sets the measure of CDD requiring financial institutions to identify and testify the identity of every client every time that a client proceeds a transaction. The requirement imposing on the institution is not only to processing identification and verification the information of customer but also but also to detect suspicious in term of the authenticity of that data. For example, the financial institution should question and inspect the authenticity of the information in the following circumstances; there is a suspicion of money laundering in connection with that customer; or there is a significant change in the way that the customer normally records its transaction and which is not reasonable considering the customer's business profile and situation.¹¹⁰

In addition to KYC process, there is CDD process which requires a financial institution, non-financial institution and other risky business under AMLA to review the information and identification of their customers periodically and also monitoring the movement of their account that is informed by the AMLO. The obligations to review and monitor as such remain until the account of their customers are closed, or the relationship with the customers is ended.¹¹¹

(3.2.3) Level of the monitoring Knowing Your Customer / Customer Due Diligence (KYC/CDD) processes

KYC / CDD are the measures against Anti-Money Laundering and Combating the financing of terrorism that need consistency. In practice, the measures are required based on the level of risk of the customer that is an imperative

¹⁰⁸ *Id.*

¹⁰⁹ AMLA, *supra* note 104, sec. 21.

¹¹⁰ United Nations, FATF-GAFI, "*FATF Recommendation 5: Customer due diligence and record-keeping*", May 2015. <http://www.un.org/en/sc/ctc/docs/bestpractices/fatf/40recs-moneylaundering/fatf-rec05.pdf> (last visited August 8, 2016).

¹¹¹ AMLA, *supra* note 104, sec. 20/1.

factor to supervise and manage information of each customer and data of the transaction. If the customer is ranked at a high risk level, the KYC / CDD processes will be very strict. On the other hand, if there is a low risk so, it could make KYC / CDD not strict like the high-risk customer or transaction.

This level of the Risk is determined by an independent organization or government agency in pursuant to a framework and guidelines for the implementation to financial institutions issued by the government authorities, such as the Bank of Thailand (BOT) or The Securities and Exchange Commission (SEC). The risk level is the guidelines and practical tools for financial institutions to treat their customers properly. These tools are convenient for both parties in the transaction and are efficient monitoring processes.

In addition, from the resolution of the Cabinet on February 27, 2007,¹¹² the DNFBP is determined as other business which has to be under this regulation too. Therefore, the rules for financial institutions shall be used to regulate DNFBP and their customers.¹¹³

The level of risk that determines the details of KYC / CDD of commercial banks and other relating business including DNFBP should be rated with the same criteria divided into three levels: low risk, medium risk and high

¹¹² มติคณะรัฐมนตรี. 'มาตรการป้องกันปราบปรามการฟอกเงิน และการต่อต้านการสนับสนุนทางการเงินแก่การก่อการร้าย เรื่อง นโยบายการปฏิบัติตามหลักเกณฑ์การรู้จักลูกค้า/การตรวจสอบเพื่อทราบข้อเท็จจริงเกี่ยวกับลูกค้าของสถาบันการเงินและหน่วยธุรกิจ หรือผู้ประกอบการวิชาชีพที่ไม่ใช่สถาบันการเงิน', 27 กุมภาพันธ์, 2550. (The resolution of the Cabinet. '*Anti-Money Laundering and Combating the Financing of Terrorism: AML/CFT on the KYC / CDD policies for financial institution and business or non-financial business*', February 27, 2007). http://www.amlo.go.th/amlofarm/farm/web/index.php?option=com_content&view=article&id=863&Itemid=880 (last visited Apr 18, 2016).

¹¹³ รุ่งเรืองสภาคกุล, วรณทณี. 'การรู้จักลูกค้า (KYC) และการพิสูจน์ทราบลูกค้า (CDD) ตอนจบ', 2552. (Ruugruangsapasakul, Wantanee. '*Know Your Customer (KYC) and Customer Due Diligence (CDD) the final chapter*', 2009). <https://www.gotoknow.org/posts/288336> (last visited Apr 18, 2016).

risk, depending on the circumstances, the status of customers or the manner of conducting the transaction.

(3.2.4) The principles used to determine the facts and information about the customers of financial institution¹¹⁴

The following are the methods to manage the risk of money laundering that may occur by the customers:

(1) To identify and testify the identity of customers by using documents, data or news from public sources which have reliability information, apart from the information that obtained from customers.

(2) To identify the real beneficiaries by using appropriate measures.

(3) To check the information of clients and beneficiaries with the customer's data defined by the CFT.

(4) To request a declaration of the purposes or the intentions to establish a business relationship with the customers.

(5) To Monitor the financial movement, transactions activity and other information related to the business relationships and proceeding transactions throughout the period that business relationship continues, to review the consistency of the purpose of business relationships or transactions that customers have described to the financial institution. They also have to review economic data of customers, the level of risk of money laundering that the customer estimated and other existing data of customers especially the information regarding the sources of revenue. This information and data of customers must be up to date.

The financial institutions are required to review the specification of the customers and the real beneficial owner of the fund in the

¹¹⁴ แสงนตรสว่าง, สรรเพชญ. สำนักงานป้องกันและปราบปรามการฟอกเงิน, 'การป้องกันปราบปรามการฟอกเงินและการ

ต่อต้านการสนับสนุนทางการเงินแก่การก่อการร้าย', 22 กรกฎาคม 2557. (Sangnatesawang, Sunpetch.

Anti-Money Laundering Office, '*Anti-Money Laundering and Combating the Financing of Terrorism*', July 22, 2014). http://www.tlaa.org/2012/images/activities/pdf/info_file_1_2014_07_22_110605.pdf (last visited April 20, 2016).

transaction and decide whether they need more information to identify the customers or not. If the customers have a low-risk profile, they may request only necessary information according to the KYC and not request for additional details, except that presented information is not complete or insufficient to prove that the customer is existing legally. Alternatively, in the case that customer has higher risk level, they must request the customers to provide full information, and obtain other information as prescribed in the Ministerial Regulation Prescribing Rules and Procedures for Customer Due Diligence B.E. 2556. Furthermore, the Customers that have a high-risk level may be required to perform more than the requirement established under this regulation for the purpose of their identity verification. Besides the processes to identify the customers, the financial institutions shall also verify the actual beneficiaries of the customers. They must obtain sufficient information of the ultimate person who actually receives benefits and prove (i) the legal existence of such beneficiary under the laws of a particular country; (ii) relationship with the customers especially the relevant aspects of business or occupation of the customer taking into account the accuracy and reasonableness.

This approach can apply to the virtual currency business by requiring providers to have the obligation to perform KYC / CDD on customers who enter into their services and constitute electronic transactions via the online network. Identity and information of the customers using online transactions are hardly traceable. Therefore, the online customers should be classified in the category of the high-risk business that requires strict measures to prevent the possibility of money laundering. There is no regulation in Thailand that regulates and imposes obligations or guidelines requiring the virtual currency business provider to do KYC / CDD. Consequently, the management of the risks in this matter is imperative to prevent and combat money laundering.

(3.3) The duty of retaining the data

When the institutions have already done the KYC / CDD processes on their customers, the law also requires the operators to store the data of customers within the specified time depending on each type of information.

Financial institutions and traders shall retain all customer identification records for five years from the date that an account is closed or the

termination of relationship with a customer. They shall maintain a record of facts and information relating to the transaction for five years from the date that such transaction occurred unless the competent official notifies that financial institution in writing to do otherwise.¹¹⁵

In addition to the duty of keeping the information within the period above, the law also requires them to maintain details of the verification of their customer identification relating to the CDD processes for a period of ten years from the date that the account is closed or the termination of relationship with their customer. If it is necessary and appropriate for the purpose of implementation of this law on a particular customer, The Secretary-General may issue a notice in writing to the institutions or traders to extend the period of data retention of that customer no longer than five years after the expiration of ten years.¹¹⁶

The duty of maintaining such data is vital to the competent authority under the law because the data of the customers is the key goal of the investigation process for the purpose of finding the offender to the justice. It also helps to manage the risk of the customer. The law requires not only the data storage duty but also a duty to maintain a system that allows relevant authorities to inspector access to the information easily. They must cooperate with the state officer to investigate and report the information according to the request from the authorities. If there is doubt in the transaction or the business profile of the customer, the financial institutions or traders must report to the AMLO in pursuant to the law and regulation.

The virtual currency business should have a duty to retain the information and data of their customer and transaction too. The virtual currency business has a particular associating with electronic data stored in the system or the computer or mobile device. In other words, it is a paperless business that all of the services are performed online via the specific network system or application on the internet. This particular brings about the high risk of the money laundering activity as it is difficult to identify the data of the customer in the transaction, unlike the financial institution or traders under the regulation.

¹¹⁵ AMLA, *supra* note 104, sec. 22.

¹¹⁶ AMLA, *supra* note 104, sec. 22/1.

The virtual currency service business is not the business under this regulation because its particular is different from the financial institution as determined under this law. In conclusion, the law can regulate neither virtual currency transaction such as trading or exchanging, nor virtual currency business providing services such as transaction system, virtual currency account like a wallet.

AMLA does not have any regulations relating to the virtual currency or virtual currency business at all. For this reason, it is necessary to consider other laws that may be applicable to the particular of virtual currency or virtual currency business by analogy.

4.1.2 Anti-Money Laundering Office Regulation prescribing Guidelines on measures to mitigate the risks of money laundering and terrorist financing potential before introducing new products, new services or the using of new technologies.

This regulation regulates the financial institutions and professionals under AMLA section 16 (1) and (9) to establish rules within the organization. It is used to monitor and assess the risks of money laundering and terrorist financing. It contains measures to mitigate the risk that may occur before using new products, new services or new technologies through the using of computer systems or equipment.¹¹⁷

To mitigate the risk, this regulation primarily controls the use of computer systems and equipment, as these systems and equipment are used by financial institutions and professionals in creating business relationship or transactions with their customers and providing services or financial products to customers electronically.¹¹⁸ Also, information technology systems and equipment are new technologies that will come into a role in the provision of services in the future.¹¹⁹ The regulation sets the guidelines to be implemented in monitoring, performing risk assessment and risk

¹¹⁷ Anti-Money Laundering Office Regulation prescribing Guidelines on measures to mitigate the risks of money laundering and terrorist financing potential before introducing new products, new services or the using of new technologies. Article 2 [hereinafter *AMLO Regulation Guidelines*].

¹¹⁸ AMLO Regulation Guidelines, *supra* note 116, article. 2 (1).

¹¹⁹ AMLO Regulation Guidelines, *supra* note 116, article. 2 (2).

mitigation measures on the information obtained as required by this regulation. The purposes of the guidelines can be divided into three parts.

The first part is to note that the using of information technology systems or devices may cause the risk of money laundering and financing of terrorism more or less.¹²⁰

The second one is to know that the using of information technology systems or devices may cause the risk of violation to the law of the anti-money laundering act and counterfeit financing terrorist including ministry regulations and relating regulations.¹²¹

The last one is to manage the risks in the case of using of information technology systems or devices that specified above and to comply with measures to mitigate those risks.¹²²

From the guidelines above, the financial institutions and the professionals as defined have to comply with these approaches. It also requires them to review and develop the measures for risk mitigation in the case of using information technology systems or equipment.¹²³ In the case that the using of technology systems or equipment under this regulation caused the risk of money laundering including the related rules and regulations without the ability to impose measures that relieve the risk, the financial institutions and professionals shall cease to use or not approve the using of those systems and/or equipment.¹²⁴

This notification also determines that financial institutions and professionals under this article may impose measures to assess the risks and mitigate the risk of money laundering and the financing of terrorism for serving or selling products with other financial that unrelated to the using of technology.¹²⁵

¹²⁰ AMLO Regulation Guidelines, *supra* note 116, article. 2 paragraph 2.

¹²¹ *Id.*

¹²² *Id.*

¹²³ AMLO Regulation Guidelines, *supra* note 116, article. 3.

¹²⁴ AMLO Regulation Guidelines, *supra* note 116, article. 4.

¹²⁵ AMLO Regulation Guidelines, *supra* note 116, article. 5.

4.2 Other Thai Regulations which can apply to Virtual Currency

None of any provisions of the AMLA mentions the virtual currency or the business relating thereto. From the primary rules on Anti-Money Laundering, it relies on the other regulations which can be applied to regulate or supervise the use of virtual currency for a purpose to comply with AMLA. Therefore, this part will diagnose the regulations concerning financial and electronic transaction for the purpose of finding the proper guidelines to determine and regulate the virtual currency and related business.

4.2.1 The Electronic Transaction Act, B.E. 2544

In general, the virtual currency transaction is executed on the online network and which does not require face to face dealing. Therefore, the transaction should be regulated under the provision of the Electronic Transaction Act.

The Electronic Transaction Act B.E. 2544 applies to all civil and commercial transactions that performed by using data message¹²⁶ that is “information generated, sent, received, stored or processed by electronic means, such, as electronic data interchange (EDI), electronic mail, telegram, telex or facsimile.”¹²⁷ Virtual Currency is data message and subject to this law. Because it is information that was in the same pattern of the data message that all of the operations performed in the form of electronic.

¹²⁶ The Electronic Transaction Act B.E. 2544 sec. 3 [hereinafter *The Electronic Transaction Act*].

¹²⁷ The Electronic Transactions Act, *supra* note 125, sec. 4.

This law provides the definition of the electronic transaction as “a transaction¹²⁸ in which an electronic¹²⁹ means is used in whole or part.”¹³⁰ Virtual currency transactions, such as payment and exchange, are performed wholly through the electronic means i.e. computer connecting to the internet; thus, the transactions are electronic transaction under this law.

In terms of reliability of information, the law establishes the initial assumption procedures. The electronic transaction will be considered reliable if it proceeds in pursuant to the requirements of this law which stated that “Any electronic transaction made by the security procedure prescribed in the Royal Decree is presumed to make by a reliable method.”¹³¹ In the context of virtual currency transaction, it must comply with the security procedures prescribed by Royal Decree for the purpose of reliability in the business or economy under the regulation.

- The Royal Decree on Security Procedures for Electronic Transactions Act B.E. 2553

This Royal Decree is an extension of the Electronic Transactions that encourages the administration and security of information in the transactions. To have acceptance and confidence in the electronic data, even more, the Electronic Transactions Act section 25 stipulates that “any electronic transaction is done by the security procedures prescribed in the ordinance; then it presumed to be reliable.”¹³²

¹²⁸ The Electronic Transactions Act, *supra* note 125, sec. 4.

“ ‘Transaction’ means any act relating to a civil and commercial activity or carrying out of the affairs of the State as prescribed in Chapter 4.”

¹²⁹ The Electronic Transactions Act, *supra* note 125, sec. 4.

“ ‘Electronic’ means an application of an electron means, an electrical means, an electromagnetic means or any other means of a similar nature including an application of an optical means, a magnetic means or a device in connection with an application of any of the aforesaid means.”

¹³⁰ The Electronic Transactions Act, *supra* note 125, sec. 4.

¹³¹ The Electronic Transactions Act, *supra* note 125, sec. 25.

¹³² *Id.*

The security model of this regulation can be divided into three levels: strict level, middle level, and basic level.¹³³ These security procedures are set to use with the electronic transaction which has an impact on the security or public order of the country or the public.¹³⁴ Considering the virtual currency business and format of the virtual currency transaction, it should be regarded as an electronic transaction. In addition, the transaction should be considered as having an impact on the security or public order of the country or the public as prescribed in section 5 (1) of this Royal Decree¹³⁵ because it is the business related to the electronic transaction which can be used as one of the channels for the criminal to launder the money and resulting in impact to the society and economy of the country. Then, it must use the security procedures with virtual currency transaction under this regulation for the reliability of such transactions. From the pattern of the virtual currency transaction, it should be classified in the strict level of the electronic transaction due to the decentralized system and anonymity account.

(1) The electronic transaction committee

Therefore, the law also set up the electronic transaction committee to have the duties to announce and determine the aspect of the electronic transaction. The committee intends to amend the regulation to evaluate the impact of the electronic transaction, taking into consideration the effect in term of value of damage that may occur to the users and the influence of the social and economic of the state.¹³⁶ These security levels may have different criteria based on notification of the committee depending on the necessity of each information systems model. However, it will have to define the security model to the minimum standard.¹³⁷

¹³³ The Royal Decree on Security Procedures for Electronic Transactions B.E. 2553 sec 4. [hereinafter *The Royal Decree on SPET*].

¹³⁴ The Royal Decree on SPET, *supra* note 132, sec. 5 (1).

¹³⁵ *Id.*

¹³⁶ The Royal Decree on SPET, *supra* note 132, sec. 6 paragraph 1.

¹³⁷ The Royal Decree on SPET, *supra* note 132, sec. 7. Security procedures according to section 4 must have the standard of information security according to the committee notification. In Each security level may have the different rules and

The virtual currency business is a new type of business which is not under any specific provisions of laws. Accordingly, it is necessary to consider the way to regulate this business. Based on the notification of the committee about the security model of an electronic transaction, virtual currency business needs to comply with the security procedures under this regulation in order to be recognized and reliable on the virtual currency and their relating business. Accordingly, the committee has the power to establish the new rule about the electronic transaction to specifically control and supervise the virtual currency business operated and implemented on the digital network. If the company acts in compliance with the standard criteria according to the rule that was defined by the committee, the electronic transaction processes shall be assumed reliable.¹³⁸

regulations depending on the necessity of such level but at least it must define the basic criteria as follows:

- (1) creating of administrative security
- (2) structuring the information security systems in the part of the administrative security systems in Both inside and outside the organization.
- (3) the management of information property
- (4) creating of information security system in the personnel part
- (5) creating of physical and environment security
- (6) management and operation of the communications network, computer network system, computer system and information system
- (7) supervision of the access to computer networks, computer system Computerized System, Information data, electronic data and computer data
- (8) providing or arranging for the development and maintenance of computer networks system, computer system, computerized system and information system
- (9) management of the undesirable security or maybe not unexpected
- (10) management services or operations of the agency or organization in order to have the continuity.
- (11) monitoring and evaluating the implementation of policy, measures, rules and procedures including the terms of any information security system

¹³⁸ The Royal Decree on SPET, *supra* note 132, sec. 9.

To execute an electronic transaction, the owner and user have to consider about the fundamental principle of confidentiality, integrity, and availability. It also includes the information security under the policy and practicality of each organization or institution.¹³⁹

(2) Service business relating to electronic transactions

This regulation also sets up the rule about the service business involving with electronic transactions which state that “Persons shall have the right to operate service business relating to the electronic transaction. In the event where it is necessary to maintain financial and commercial stability, or for the benefit of strengthening the credibility and acceptance of electronic transactions system, or prevent damage to the public. The Royal Decree is prescribing the service business relating to the electronic transaction which shall be subject to prior notification, registration or licence shall be issued.”¹⁴⁰ It must evaluate the impact, risk, and the preventive measure which shall occur from the business.¹⁴¹

The released about the transaction which related to a virtual currency such as virtual currency transfer between users was not considered as payment that defined by any regulations. The virtual currency service provider acts as a medium of exchange between the users by providing a service to deposit or to withdraw virtual currency and also to store virtual currency of each account in the system. The virtual currency service provider is not considered the financial institutions or professionals. However, the virtual currency service provider serves its customer through the electronic means, and the whole business occurs in the electronic form and involves with electronic transactions. Therefore, the service provider should be considered as being under this regulation as a provider of the service relating to electronic

¹³⁹ The Royal Decree on SPET, *supra* note 132, sec.10.

¹⁴⁰ The Electronic Transactions Act, *supra* note 125, sec.32 Para. 1.

¹⁴¹ The Electronic Transactions Act, *supra* note 125, sec.32 Para. 2.

“As to which case would require notification, registration or licence under paragraph one, the determination shall be taken based on the appropriateness of damage prevention in accordance with degree of severity of the impact which may occur from such business operation.”

transactions. According to The Electronic Transactions Act, a provider of service relating to electronic transaction requires a license. Accordingly, the virtual currency service provider shall apply for a license to operate its business.¹⁴² If it violates or unable to comply with the licensing requirement for operating the business as prescribed or breaches the conditions of the permit, it will be punished by this law.¹⁴³

¹⁴² The Electronic Transactions Act, *supra* note 125, sec.33

“In the event where there is a Royal Decree prescribing the service business relating to electronic transactions which shall be subject to prior notification or registration, the person wishing to operate such business shall notify, or apply for registration with the competent official as prescribed in the Royal Decree prior to the commencement of such business operation.

The rules and procedures for notification or registration under paragraph one shall be as prescribed in the Royal Decree. When the competent official under the Royal Decree is notified or accepts the registration, he or he shall issue a certificate of notification or a certificate of registration as evidence of the notification or registration on the date of notification or registration. The person making notification or applying for registration can operate such business as from the date of the notification or registration. If, subsequently, the competent official under the Royal Decree finds out that the notification or the registration has been made inaccurately or incompletely, the competent official shall have the power to order the person having made the notification or having applied for the registration to correct or complete it within seven days from the receipt date of such order.

In operating the business, the person having made the notification or having applied for the registration under paragraph one shall comply with the rules prescribed in the Royal Decree and those prescribed by the Commission.”

¹⁴³ The Electronic Transactions Act, *supra* note 73, sec.34

“In case where a Royal Decree is issued prescribing the service business relating to electronic transactions which shall be subject to prior licence, the person wishing to operate such business shall apply for such license with the competent official as prescribed in the Royal Decree.

The virtual currency operates by using a computer or mobile phone to transfer the virtual currency online. The virtual currency transaction is an electronic transaction being governed this regulation because its all processes have to be performed through the electronic process on the online network via the internet.¹⁴⁴ Although the legal status of virtual currency still not confirmed, its feature is the electronic data stored in the digital form. Therefore, the provision of the act concerning electronic data exchange can be applied to the exchange of virtual currency¹⁴⁵ in this regulation.

4.2.2 The Computer Crime Act B.E. 2550

The virtual currency and virtual currency services business are related to computer and may be a target for the criminal to commit the crime by using virtual currency through the computer or data theft. Moreover, the issue about the status of virtual currency that is still unclear so this law can be adopted to interpret the virtual currency service business and the related person including how to operate or manage

The qualifications of the applicant for the license, the rules and procedures for applying for the licence, the licence issuance, the licence renewal, the return of the licence, the suspension or revocation of the licence shall be as prescribed in the Royal Decree.

In operating the business, the person who has obtained the licence under paragraph one shall comply with the rules prescribed in the Royal Decree and those prescribed by the Commission or conditions stipulated in the licence.

In case the person who has obtained the licence violates or fails to comply with the rules for operating the service business relating to electronic transactions under paragraph three, the Commission shall be empowered to consider and issue an order imposing an administrative fine not exceeding two million Baht, taking into account of the severity of the offence. In case where it deems fit, the Commission may issue an order requiring such person to take any corrective action as appropriate. In this connection, the provisions of section 33, paragraph five, shall apply mutatis mutandis.”

¹⁴⁴ The Electronic Transactions Act, *supra* note 125, sec. 4.

¹⁴⁵ *Id.*

this thing and to make it clear on the status of its. According to the Computer Crime Act B.E., 2550, the definitions and the details about the computer data and system and also includes the service provider that can be applied to use with virtual currency and their relating business.

The Act defines Computer System as “a piece of equipment or sets of equipment units, whose function is integrated together, for which sets of instructions and working principles enable it or them to perform the duty of processing data automatically.”¹⁴⁶ From the definition, virtual currency system is a computer system as it consists of sets of the instructions combining each function together and operates the data processing automatically through the online network. The virtual currency system is a decentralized system which used P2P network, so it does not have the central of the system. This system brings the risk of business or transactions and can be the channel for criminal to launder the money.

The second is the definition of Computer Data which is provided as “data, statements, or sets of instructions contained in a computer system, the output of which may be processed by a computer system including electronic data,¹⁴⁷ according to the Law of Electronic Transactions.”¹⁴⁸ In this regards, virtual currency is computer data it is the data code on the computer that has to operate on the computer system or mobile application on the internet network.

The third one is the definition of Computer Traffic Data described as “data related to computer system-based communications showing sources of origin, starting points, destinations, routes, time, dates, volumes, time periods, types of services or others related to that computer system's communications.”¹⁴⁹ The features of virtual currency transaction between the customer and also the owner of the virtual currency service business have the data record in the system which shows the information about each customer involving in the transaction.

The fourth one is the definition of Service Provider which includes:

¹⁴⁶ The Computer Crime Act B.E. 2550 sec. 3 [hereinafter *The Computer Crime Act*].

¹⁴⁷ The Electronic Transactions Act, *supra* note 125, sec. 4.

¹⁴⁸ *Id.*

¹⁴⁹ The Computer Crime Act, *supra* note 145, sec. 3.

“(1) A person who provides service to the public with respect to access to the Internet or other mutual communication via a computer system, whether on their own behalf, or in the name of, or for the benefit of, another person.

(2) A person who provides services for the storage of computer data for the interests of the other person.”¹⁵⁰

Virtual currency service provider can be interpreted as a service provider according to the definition given in this law. This is because the purpose of the service is to provide the customer access to the particular communication of the customer. The service provider facilitates the use of virtual currency as the medium of exchange via the computer system or mobile application and receives fees from the use of such services.

The last one is the definition of Service User which means “a person who uses the services provided by a service provider, with or without a fee.”¹⁵¹ The customer of virtual currency must register the account to the virtual currency service business before using the service. Therefore, the customer of virtual currency is within the definition of service user subject to this law.

In considering of the definitions above, the virtual currency service business and all relating persons are governed under the Computer Crime Act. They are obliged to perform in pursuant to the provisions thereunder. This law imposes the duty of service provider to store computer traffic data or information of service user about the data input into a computer system for at least ninety days or not exceeding two years depending on the order of relevant competent official.¹⁵² The virtual currency service

¹⁵⁰ *Id.*

¹⁵¹ *Id.*

¹⁵² The Computer Crime Act, *supra* note 145, sec. 26

“Section 26. A service provider must store computer traffic data for at least ninety days from the date on which the data is input into a computer system. However, if necessary, a relevant competent official may instruct a service provider to store data for a period of longer than ninety days but not exceeding two year.

The service provider must keep the necessary information of the service user in order to be able to identify the service user from the beginning of the service

business must store their information and computer traffic data within the period to be supported to the formal and establish the credibility and a clear status of virtual currency, including reducing the risk of a channel for money laundering.

4.2.3 Exchange Control Act B.E. 2485

The legitimate premise for trade control in Thailand is mentioned in the Exchange Control Act B.E.2485. This law sets out the standards of controlling, confining, or precluding the execution of all trade or different operations in which foreign currency is concerned in whatever structure.

Currently, the foreign exchange businesses in Thailand are regulated under the ECA. The operators of businesses to buy, sell, exchange, loan or transfer foreign currency have to obtain a license from Ministry of Finance via Bank of Thailand (“BOT”).¹⁵³ There are five kinds of licenses¹⁵⁴ as follows:

- 1) Bank or Legal Entity established by law which is allowed to withdraw, deposit, trade, or lend foreign currency.
- 2) A person who is allowed to do the businesses to buy and sell foreign banknotes, and purchase travelers cheque from customers.

provisions, and such information must be kept for a further period not exceeding ninety days after the service agreement has been terminated.

Definitions and details of instructions that the provisions under paragraph one shall apply and the timing of this application shall be established by a Minister and published in the Government Gazette.

A service provider who fails to comply with this Section must be subject to a fine of not more than five hundred thousand baht.”

¹⁵³ Flurrywong. 'ธนาคารแห่งประเทศไทยประกาศให้ธุรกรรมทั้งหมดเกี่ยวกับ **Bitcoin** เป็นสิ่งผิดกฎหมาย', 30 กรกฎาคม 2556 (*'Bank of Thailand declared that all transactions with Bitcoin are illegal'*, July 30, 2013). <https://www.meconomics.net/content/577> (last visited May 17, 2016).

¹⁵⁴ ธนาคารแห่งประเทศไทย. 'ธุรกิจบิ๊จจยชำระเงินต่างประเทศ'. (Bank of Thailand. *'Types of Foreign Exchange Licenses'*). <https://www.bot.or.th/Thai/FinancialMarkets/ForeignExchangeRegulations/ForeignMeansOfPaymenBusinesses/Pages/default.aspx> (last visited May 17, 2016).

3) International money transfer agent who is allowed to transfer foreign currency out of the country and to receive transfer foreign currency for the purpose to pay baht to recipients in the country.

4) Corporation, which is allowed to trade traveler cheques to the people that are leaving the country or payment baht to the credit card holders.

5) Treasury Center, which is authorized to do business with the management of foreign currency to the conglomerate in Thailand or in other countries that located, connects to Thai border which is manufacturing and international trade business or companies that have a business or business related field of manufacturing and international trading company from three companies above.

According to this regulation, the Minister have the power “to issue the Ministerial Regulations to control, restrict or prohibit the disposal of all exchange or other performance involving with foreign currency and also have the authority to issued regulations under concerning the exchange activity as stated in this regulation.”¹⁵⁵ Consequently, the person or legal entity who is granted the license to operate the foreign exchange business under this Act must comply with the requirement under this regulation.¹⁵⁶ If they cannot perform in accordance with the notifications or directions of the Minister, they shall be punished under this law.¹⁵⁷

Moreover, there is the measure to prevent and combat the illegal export or import of currency and exchange by using the Customer rules to apply to it. Notwithstanding, virtual currency is not within the meaning of “currency”¹⁵⁸ or “foreign currency”¹⁵⁹ as given under this law; thus, it is not the subject of this law.

¹⁵⁵ The Exchange Control Act B.E. 2485 sec. 4 [hereinafter *The Exchange Control Act*].

¹⁵⁶ The Exchange Control Act, *supra* note 154. sec 4 bis

¹⁵⁷ The Exchange Control Act, *supra* note 154. sec 8

¹⁵⁸ The Exchange Control Act, *supra* note 154. sec 3

“ ‘Currency’ means legal tender in Thailand.”

¹⁵⁹ The Exchange Control Act, *supra* note 154. sec 3

“ ‘Foreign exchange’ means bank balance, bill of exchange, cheque promissory note, telegraphic transfer, mail transfer, or money order payable in foreign currency.”

Consequently, this regulation cannot be used to enforce or control the business which related to the virtual currency. This circumstance poses a risk about supervision in the business that involving with virtual currency such as the exchange of virtual currency between users that may involve an illegal activity or relate to money laundering.

- Ministerial Regulation No. 13 B.E. 2497

This regulation issued under the Exchange Control Act B.E.2485 for the purpose of consolidating all previous laws to explains and improve the processes that are associated with the Exchange Control Act B.E.2485 to be used more clearly and appropriately with the exchange business. Under this regulation, to operate the foreign exchange business the person as prescribed by this regulation must get prior permission from the Minister.¹⁶⁰

Therefore the issue about the virtual currency business is not a new affair, although its status is still unclear under the laws and regulations in Thailand. If the authorities grant the business license to the company which operates as the medium of exchange in virtual currency without any regulations so, it will bring another legal issue in the future because this is the particular business which has the different feature from the financial institution or the bank. Therefore, it is not appropriate to

¹⁶⁰ Ministerial Regulation No. 13 B.E. 2497 article 3[hereinafter *Ministerial Regulation No. 13*].

“No person shall transact business relating to foreign means of payment unless the permission has been granted by the Minister.

Any person wishing to undertake business relating to foreign means of payment shall apply for permission in prescribed forms to the Minister through the Bank of Thailand.

The Minister may issue notifications prescribing rules to be followed by applicants in applying for and on being given permission.

In the case where the person given permission is an authorized bank or an authorized company, it shall be deemed that the branches of such authorized bank or company is likewise covered by such permit unless otherwise stated in the permit. Whatever the case may be, the Minister has the power to alter the permit so as to exclude any specific branch of the authorized bank or authorized company.”

interpret this business as the person or organization eligible to get the license under the Exchange Control Act B.E.2485 and also the Ministerial Regulation No. 13.

4.2.4 Financial Institution Businesses Act B.E. 2551

The goal of this regulation is to improve the danger administration measures of the budgetary organizations, to guarantee the Prudential and shield the harm which may come about because of the money related establishments undertaking. It additionally has the plan to keep up monetary steadiness and endow the contributors and people in general by recommending the high administration rules for any individual who performs the obligation of an executive, an administrator, an officer or a man with the force of administration of budgetary establishments.

Typically the financial institution business under this act also includes “the commercial banking business, finance business, and credit foncier business and shall include the undertaking of specialized financial institution business.”¹⁶¹ These business operators must be public limited companies being granted the license from the Minister with the recommendation of the Bank of Thailand. The license may be granted with conditions as the Minister deems appropriate.¹⁶²

Although this act does not mention virtual currency or virtual currency service business which is not the subject under this law, it has the provision that may be applicable to virtual currency and virtual currency service business. Such provision is the one concerning other business involving with public fundraising through deposit acceptance or any other means, granting of credits or undertaking financial business, affects the overall economy of the country. It does not have a particular law governing such business. BOT may propose for an enactment of a Royal Decree prescribing such business to be subject to the enforcement of this Act, either in whole or in part, including related penalty provisions. In this regard, supervisory regulations of such business may also be prescribed.¹⁶³ The virtual currency service business activity may relate to the deposit of fund where customers make a deposit for a purpose to exchange the fund

¹⁶¹ The Financial Institution Businesses Act B.E. 2551 sec. 3 [hereinafter *The Financial Institution Business Act*].

¹⁶² The Financial Institution Businesses Act, *supra* note 160. sec 9.

¹⁶³ The Financial Institution Businesses Act, *supra* note 160. sec 5.

into virtual currency, or payment of the fund to the customers and receive the virtual currency back. These matters have an effect on the economy of the country because it is the channel to transfer the money domestically or internationally without the participation of law or any regulation. This virtual currency related business can be interpreted as one of the financial business under this provision. Therefore, the BOT can propose a legislation of law to supervise and to enforce under this act.

4.3 The Decisions of Thai Supreme Court

The subject matter is the status of virtual currency under Thai laws and regulations. The related agency or government did not accept this financial innovation as one of the media of exchange or payment method or treat it like the money. If there is the issues that involved with virtual currency in Thailand, the court or the state authorities have to interpret its status not only the object under the laws but also include a process to implement the preventive measure and suppression measure. The status of the virtual currency shall be considered in two aspects as described below:

1) The things or property under the laws

If virtual currency is considered as the things or asset under the laws, it can be used as an object in payment transactions in the same manner as money, or for exchange with valuable things. Maybe it can use as an investment tool for investor to trade with other currency.

2) The Data or Electronic Information

The nature of virtual currency is digital data stored in a computer connected to the online network system. It could be treated as one of the data or electronic data under the laws.

In Thailand, it does not have the case directly related to virtual currency, but there are the Supreme Court decisions which could be adapted to determine the format or status of the virtual currency by using the existing law to correlate with the feature of the virtual currency.

4.3.1 Supreme Court Judgement 877/2501 [1958]

The resolution by the general meeting of the Supreme Court was made to decide the offence of electricity theft under Section 334.¹⁶⁴ The legal issue, in this case, is the “things” that is the object of the theft offence. The defendant claims that electricity is not a thing under the meaning of things in Criminal Code Section 334 or Section 335, so stealing electricity is not an offence under the law. However, the Supreme Court considered on this issue and had the decision that electricity is the things so that it can be the object of the theft offence. It is the first time of the Supreme Court Judgement on the issue about the electricity which is the guideline for the judge in the case later that have the same issue.

4.3.2 Supreme Court Judgement 3684/2547 [2004]

This case is about the theft offence of the telephone signal wave transmitted through the signal cable by stealing the signal stream from the cable line and the public telephone booths. The problem in this case, likely the same as SCJ 877/2501 as mentioned above, is that the telephone signal wave is the things under the offence of theft like the electricity or not.

The court convicted that telephone signal stream is the things which can be stolen by the offender. The defendant has the guilty on the offence of theft under the Criminal Code Section 334. The another issue which supports this verdict about the interpretation of this signal wave is the things. The fact that the court comment on the decision about the reimbursement of the price of the things which is the value of the telephone signal wave. Therefore, it can be seen that the court ruling about the things is in the same manner.

4.3.3 Supreme Court Judgement 5161/2547 [2004]

In this case, the plaintiff alleged that the defendant committed the offence of theft by copying the data information (the translation documents and the drafts of contract in English) stored in the computer of the plaintiff. The point, in this case, is whether the data in the computer can be the object of the theft offence under Section 334 of the Criminal Code like the electricity or signal wave. The important

¹⁶⁴ Criminal Code Section 334.

factor in this crime is the action of taking away the things of the other person. The court must diagnose the issue about the status of the objective of the theft offence in this case.

The point that should mention is the meaning of the data. According to Thai-Dictionary, the meaning of Information or Data is “Fact or the thing that considered or recognized as the fact which use as the principle to finding the factor calculation.” Moreover, the meaning of Fact is “message of incidence which is the arising or the actual being and the message or the event which have to be considered the true or false.”

The court relied on the judgments given that the electricity and telephone signal wave are the things that can be an object of the theft under the Criminal Code. Under this law, it does not have the meaning of the things. Therefore, it has to require other legislation to interpret the meaning under the law by analogy. On the issue of the things or property, it has to use the Civil and Commercial Code to understand the meaning of things or property. However, the court also determined that the Civil and Commercial Code section 137 states that “things” are the tangible object. In this case, it related to the data which storage in the memory disk. The judgement stated that the data was not considered as the things under this law, so it cannot be theft because the computer data is not the object of the theft offence.

Nevertheless, there is a legal opinion from the prof. Jitti Tingsapach, which is the top of the professional lawyer in Thailand, providing that section 334 of Criminal Code use the wording “taking away the things of other.” The meaning of things under the CCC is the tangible things so that it can be the subject of the theft offence under this law. According to the fact, in this case, the issue is about the computer data that can be stolen by other or not and the data is the tangible things or not. This data is the electronic data under the electronic transaction act B.E.2544 defined that is “a transaction in which an electronic means used in whole or part.”¹⁶⁵ So it is not considered the data is tangible things under the theft offence but if the data be transformed to the document or compact disc so it is the things that could have been theft and can comply with Criminal Code as prescribed in section 334.

¹⁶⁵ The Electronic Transactions Act, *supra* note 125.

4.3.4 Supreme Court Judgement 9631-9632/2558 [2015]

This case is about the drug trafficking offense which is the one of the predicate offense under AMLA. From the fact, there are reasons to believe that the property 29 items, which are lands, cars, bank deposit, jewelry, guns, and cash from the auction of the car are related to the drug offense. As a predicate offense under section 3 (1) of the Anti-Money Laundering Act 2542, the Transaction Committee has considered and resolved to seize assets and freeze them. It is also seeking a court order to assets totaling 29 items with a total value of 5,396,793.25 Baht included the interest of these properties are belong to the State.

The issues are about the property which can be enforced by the AMLA. The property that can be confiscated must relate to the predicate offense as prescribed in section 3 (1). It has to meet the asset definitions under this regulation. If there is the case that involving with the virtual currency, it will have a problem in processing confiscation under the AMLA. This is because it is not clear whether virtual currency should be interpreted as an asset under this law. It also has another problem in the process of the confiscation by the officer due to the feature of the virtual currency, which is data stored in digital form on the internet network. These circumstances have to be considered by the government in coordination with other private sector and also including the related state organizations for the purpose of effective enforcement.

The virtual currency is not the subject under any laws and regulations because it is the data in the network which is intangible. Applying the supreme court's decision that computer data is not the things and cannot be theft, the virtual currency which is electronic data may be interpreted in the same way . Also, the virtual currency may be interpreted as the medium of exchange in the transaction between the customers, but it does not have the exact definition under the law like the common currency which is the medium of exchange in the financial transaction. This problem must be solved urgently because it is the risk in the financial sector in the term of money laundering which could impact the financial system of the country and also could effect to the law enforcement in the case that involving with virtual currency that cannot enforce and supervise adequately.

CHAPTER 5

CONCLUSIONS AND RECOMMENDATIONS

5.1 Conclusions

With the participation of modern technology, money laundering has embraced a universal character. To viable battle money laundering, worldwide nations need to adopt a more aggregate methodology. Consequently, the rise of the different global activities remains as a noteworthy accomplishment, and the proceeded with the improvement of against money laundering structure is critical.

The problem of money laundering is not only associated with drug trafficking or tax avoidance offences, but it also increases the risk of each customer and business transaction. Bank directors and controllers should likewise combat with the impacts and potential outcomes of money laundering on the banking frameworks. The Basel Committee thinks about the issue at a multinational level, to develop the international legal structure on money laundering to address not only the real money but also the virtual currency (digital money).

By the way, the government has to continuously improve the domestic legal structure, so as to innovatively utilize its discretion in assistance of worldwide union on the issue.¹⁶⁶ The regulations should begin with guaranteeing that any currencies (fiat currency and virtual currency) and the corporation under each location appropriately enlisted with the regulation.¹⁶⁷

The electronic trading system of service providers or businesses relating to virtual currency must stick to the same extensive variety of hostile to money laundering, recordkeeping, and reporting obligations as the financial institutions or banks. These

¹⁶⁶ Morgan, Matthew S., '**Money Laundering: The United States Law and its Global Influence**', The London Institute of International Banking, Finance & Development Law. November 1996. P.50-51

¹⁶⁷ Angotti, Alma. "*Advantage Risk & Regulation*", May 25, 2016.
<http://www.navigant.com/insights/library/gic/2016/advantage-risk-and-regulation-spring-2016/> (last visited Jun 1, 2016).

responsibilities incorporate, but not constrain to build up a composed hostile to government evasion system; leading Money administration business free audits, reporting cash exchanges, and Suspicious Activity Reporting.

The two most important issues to regulate virtual currency are the legal jurisdiction over the internet and the anonymity feature of virtual currency.¹⁶⁸

The internet is the overarching network of individual networks. The system flows freely between states, countries, and contents. This free movement of information and commerce creates an issue in regulating the contents and its users. The laws are inconsistent among jurisdictions both in term of definitions and supervisions. It creates a barrier to the necessary regulation for preventing online economic crime or enforcing regulations. Each state decides to regulate the internet according to their values and morality act. The virtual currency in many countries are still under development, but once it is operational and offered to criminals, it will be an effective means of facilitating money movement to aid criminal organization in money laundering.

5.2 Recommendations

With its operation on the open network which is easily accessible by anyone through a digital process at fewer fees compared with the general financial process, virtual currency has become more popular than before. It operates on a network as a commodity and has the own value in itself depends on the demand of the users. The decentralized system can cause the risk of money laundering that absence of the supervision from the administration of any regulations.

Virtual Currency or Bitcoin keeps the clients' record untraceable by utilizing cryptography or peer-to-peer innovation. It is hard to distinguish the majority of the exchanges which running using the computerized, so the particular framework or organization has essential influence in the advancement of Bitcoin or other virtual

¹⁶⁸ Chambers, Clare. "The article *"Can You Ever Regulate the Virtual World Against Economic Crim"* 2012.

currency, however, it does not decide its prosperity.¹⁶⁹ The government has to propose specific procedures for relevant authorities to enforce against wrongdoers of the anti-money laundering laws. In this regards, the procedures can be proposed in two parts as follows:

5.2.1 Amendment the legislations to cover the offence against Virtual Currency

The Regulator and Legislator of the country have to explore the option of escalating punishment of the criminal based activity which caused the money laundering offence to restrict the illegal used of virtual currency. The existing laws do not have the inhibitor to the use of virtual currency in the commission of a crime during the period of the offence. If the regulators can inquire the supplement option to control and enforce the subject matter in the case, the virtual currency was used to facilitate the criminal activity. Therefore, it is appropriate to directly regulate money laundering in the case of using virtual currency so that the users, companies, and exchangers are the subject under the regulations and could be subject to a penalty the same as other offence.

For this recommendation, the writer suggests amending the Anti-Money Laundering Act (AMLA) to add provisions about the virtual currency. The first one is to provide a definition of virtual currency and virtual currency service business in order to affirm their legal status under the law. Then, the Financial Institution Act should be amended to include virtual currency related business as a kind of financial institution thereunder.

The AMLA should be the primary law to supervise and regulate the virtual currency to manage the risk of money laundering through virtual currency by the criminals in the future. The other regulations have to be amended inconsistent with this act. Therefore, it should treat virtual currency in the same manner as the real currency because it is used as the medium of exchange for the money and in this present, it tended to be used more widely instead of the real currency.

Another key provision of this Act that should be amended is the requirement of financial institutions and other businesses that tend to be used as

¹⁶⁹ Peng, Starry. *"BITCOIN: Cryptography, Economics, and the Future"*. School of Engineering and Applied Science, University of Pennsylvania, December 2013.

vehicles for money laundering to report all cash transactions of THB two million or more. Property transactions value more than THB five million must be reported. Also required for reporting are all suspicious transactions that may be related to one of the enumerated criminal offenses, are more complex than normal, lack economic plausibility, or appear to have been undertaken to avoid compliance with the Anti-Money Laundering law. For such transactions, the financial institutions must require their customers to provide a detailed record of the transactions. The latter requirement left to the reasonable discretion of the financial institution which must then choose between customer confidentiality concerns and compliance with the Act. According to this provision, the institution which related with the Virtual Currency or Bitcoin (Money Exchangers, Website-Administrators, and other related business) should have the same duty as the other financial institution under this act. It has to record the information of virtual currency transaction and report the transaction to the AMLO if the value of such virtual currency transaction reaches or exceeds THB two million. In addition, if there are suspicious in any virtual currency transaction, the financial institution have to report that transaction to the AMLO too for the purpose of supervising and control the cash flow and can detect the suspicious transaction based on the risk assessment in each account.

5.2.2 Monitoring approach

This method concerns with the acquisition of customer data and data preservation. This method is significant for monitoring the virtual currency because all of the processes of virtual currency transaction are performed on the internet and, thus, it is connecting every country together in the system to do the transaction via the computer or mobile phone. There is no any documents and the whole part happen in the network.

The methods and procedures of the virtual currency are operating in the digital world through the internet. The user has to register the account on the service provider website before they use the virtual currency services such as buy, sell or transfer the virtual currency to the other users via the system of the operators or the exchangers. The involving person and corporation acting as the intermediary in the transaction should have duties under the regulation and security procedures which related to the information of the customer; data transfer history and another valuable

data that involved with the transaction to do KYC and CDD with every customer. They must keep the record within the specified period for the purpose of examination in the case that Law enforcement officer asks to send the information and data of their customer under the state authority.



REFERENCES

Books and Book Articles

1. Books

1.1 English

Collins English Dictionary. Complete and Unabridged, 12th ed., 2014.

Gallant, M. Michelle. '**Money Laundering and the Proceeds of Crime: Economic Crime and Civil Remedies**', Canada: Faculty of Law (University of Manitoba), 2005.

Melanie, L. Fein. *Law of Electronic Banking*. New York: Aspen Law & Business
A division of Aspen Publishers, Inc., 2000.

Morgan, Matthew S., '**Money Laundering: The United States Law and its Global Influence**', The London Institute of International Banking, Finance & Development Law. November 1996.

1.2 Thai

เจริญพานิช, ศรีราชา. คำอธิบายกฎหมายว่าด้วยทรัพย์สิน. 2nd ed., 2010. (Charoenpanich, Sriracha.
Property Law 2nd ed., 2010).

บุญญากาศ, วีระพงษ์. อาชญากรรมทางเศรษฐกิจ. พิมพ์ครั้งที่ 5. กรุงเทพฯ, 2549. (Boonyopas, Veerapong.
Economic Crime. 5th ed. Bangkok, 2006).

2. Articles

2.1 English

Calvery, Jennifer S., "*Statement of Director Financial Crimes Enforcement Network United States Department of the Treasury Before the United States Senate Committee on Banking, Housing, and Urban Affairs Subcommittee on*

National Security and International Trade and Finance Subcommittee on Economic Policy", 2013.

Chambers, Clare. *"The article "Can You Ever Regulate the Virtual World Against Economic Crime", "* 2012.

Chan-o-cha, General Prayut. Prime Minister, *'Policy Statement of the Council of Ministers to the National Legislative Assembly'*, September 12, 2014 (2014).

Morgan, Matthew S. *'Money Laundering: The United States Law and its Global Influence'*, **London Institute of International Banking, Finance & Development Law**, November 1996, (1996).

Zhu, Min. Deputy Managing Director of the IMF, *'The IMF and the Fight Against Money Laundering and the Financing of Terrorism'*, (2016) Accessed April 5, 2016. <http://www.imf.org/external/np/exr/facts/pdf/aml.pdf>

2.2 Thai

ศรีชาติ, กัณฑ์ภณ. 'เงินเสมือน (**Virtual Currency**) ต่างจากเงินจริงอย่างไร'. ธนาคารแห่งประเทศไทย, (2556). (Srichart, Kantaphol. **'How was the difference between Virtual Currency and Real Currency?'**. Bank of Thailand, (2013).

3. Electronic Media

3.1 E-books

Bernstein, Peter. **A Primer on Money, Banking and Gold**. Ebook. 3rd ed. Hoboken, NJ: Wiley. 2008. <https://books.google.co.th/books?id=LE2pzHjek4sC&pg=PT4&lpg=PT4&dq=Bernstein,+Peter,+and+A.+Volker.+2008.+A+Primer+on+Money,+Banking+and+Gold&source=bl&ots=uhYTOcUC8U&sig=o-Ebx xkgvUiPHFII3LFw43p7wWA&hl=th&sa=X&ved=0ahUKEwjSkoXNzaXOA hUMpI8KHfmBCv4Q6AEIRjAF#v=onepage&q=Bernstein%2C%20Peter%2C%20and%20A.%20Volker.%202008.%20A%20Primer%20on%20Money%2C%20Banking%20and%20Gold&f=false>

Levinson, Marc. The Economist, "**Guide to the Financial Markets**", Ebook. 4th ed. London: Profile Books Ltd, 2006. https://drive.google.com/file/d/0B_Qxj5U7eaJTZTJkODYzN2ItZjE3Yy00Y2M0LTk2ZmUtZGU0NzA3NGI4Y2Y5/view?hl=en&pli=1

Ronald L. Akers and Christine S. Sellers. "**Student Study Guide for Criminological Theories: Introduction, Evaluation, Application**". Ebook. 6th ed. New York: Oxford University Press, 2013. http://global.oup.com/us/companion.websites/9780199844487/guide1/study_guide.pdf

3.2 Online Reports

Bank of Thailand, '*Payment System Report*', 2013. Accessed February 22, 2016. https://www.bot.or.th/English/PaymentSystems/Publication/PS_Annually_Report/Documents/Payment_2013_E.pdf.

The Financial Action Task Force, '*FATF REPORT Virtual Currencies Key Definitions And Potential AML/CFT Risks*', 2014. Accessed January 15, 2016. <http://www.fatf-gafi.org/media/fatf/documents/reports/virtual-currency-keydefinitions-and-potential-aml-cft-risks.pdf>.

3.3 Websites

AdvisoryHQ.com, "*KYC vs. CIP vs. CDD. | Know Your Customer Rules and Guidelines*" January 24, 2016 (2016). Accessed May 28, 2016. <http://www.advisoryhq.com/articles/kyc-vs-cip-vs-cdd-know-your-customer-rules-and-guidelines/>.

adweek.com, Morrison, Kimberlee. "*Silk Road Trial Becomes Case Study for Law Enforcement Online*", January 13, 2015 (2015). Accessed June 1, 2016. <http://www.adweek.com/socialtimes/silk-road-trial-becomes-case-study-for-law-enforcement-online/612298>.

bitcoin.co.th, "The results of the Meeting between Bitcoin Co.Ltd. and BOT on July 29th, 2013". Accessed February 20, 2016.

engadget.com, Alvarez, Edgar. "New York wants Bitcoin exchanges to be heavily regulated". 2014. Accessed May 30, 2016. <https://www.engadget.com/2014/07/18/new-york-cryptocurrency-regulations/>.

fincen.gov, Federal Financial Institutions Examination Council. "History of Anti-Money Laundering Laws." Accessed May 29, 2016. https://www.fincen.gov/news_room/aml_history.html.

meconomics.net, Flurrywong. "ธนาคารแห่งประเทศไทยประกาศให้ธุรกรรมทั้งหมดเกี่ยวกับ Bitcoin เป็นสิ่งผิดกฎหมาย", 30 กรกฎาคม 2556 ("Bank of Thailand declared that all transactions with Bitcoin are illegal", July 30, 2013). Accessed May 17, 2016. <https://www.meconomics.net/content/577>.

navigant.com, Angotti, Alma. "Advantage Risk & Regulation", May 25, 2016. Accessed June 1, 2016. <http://www.navigant.com/insights/library/gic/2016/advantage-risk-and-regulation-spring-2016/>.

nytimes.com, The New York Times. "How Liberty Reserve's Virtual Currency Works", 2013. Accessed February 10, 2016. http://www.nytimes.com/interactive/2013/05/29/nyregion/how-liberty-reserves-virtual-currency-works.html?_r=0.

nytimes.com, Perlorth, Rashbaum, Santora. The New York Times, "Online Currency Exchange Accused of Laundering \$6 Billion", 2013. Accessed February 10, 2016. <http://www.nytimes.com/2013/05/29/nyregion/liberty-reserve-operators-accused-of-money-laundering.html>.

sec.or.th., The Securities and Exchange Commission, Thailand. "*FinTech Forum: FinTech Ecosystem*". Accessed Jul 16, 2016. <http://www.sec.or.th/EN/Pages/FinTech/fintech.aspx>.

theguardian.com, Olson, Parmy. "*The man behind Silk Road – the internet's biggest market for illegal drugs*", November 10, 2013. Accessed May 31, 2016. <https://www.theguardian.com/technology/2013/nov/10/silk-road-internet-market-illegal-drugs-ross-ulbricht>.

usatoday.com, Leger, Donna L., USA TODAY. "*How FBI brought down cyber-underworld site Silk Road*", 2013. Accessed June 1, 2016. <http://www.usatoday.com/story/news/nation/2013/10/21/fbi-cracks-silk-road/2984921/>

3.4 Others

3.4.1 English

Brown, Richard G., "*A simple explanation of bitcoin "sidechains"*", 2014. Accessed February 22, 2016. <http://gendal.me/2014/10/26/a-simple-explanation-of-bitcoin-sidechains/>.

Duhaime, Christine. "*What is Money Laundering? Duhaime's Financial Crime and Anti-Money Laundering Law*". March 7, 2014 (2014). Accessed January 12, 2016. <http://www.antimoneylaunderinglaw.com/aml-law-in-canada/what-is-money-laundering>

Federal Financial Institutions Examination Council, "*Bank Secrecy Act/Anti-Money Laundering InfoBase: Customer Due Diligence-Overview*", Accessed June 1, 2016. https://www.ffeic.gov/bsa_aml_infobase/pages_manual/OLM_013.htm.

- Federal Financial Institutions Examination Council, *"Bank Secrecy Act anti-money laundering examination manual appendix d: Statutory definition of financial institution"*. Accessed May 24, 2016. https://www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_104.htm.
- Federal Financial Institutions Examination Council. *"History of Anti-Money Laundering Laws"*. Accessed May 29, 2016. https://www.fincen.gov/news_room/aml_history.html.
- Federal Reserve Bank of Atlanta. *"Retail Payments Risk Forum Working Paper: Banking Bitcoin-Related Businesses: A Primer for Managing BSA/AML Risks"*, 2015.
- Greene, Olivia. *"Risk Advisory, Risks and Challenges Associated with Bitcoin Transaction Monitoring for AML"*, 2015. Accessed June 5, 2016. https://www.dhglp.com/Portals/4/ResourceMedia/publications/Risk-Advisory_Bitcoin.pdf
- Henning, Peter. *"For Bitcoin, Square Peg Meets Round Hole Under the Law"*, December 9, 2013. Accessed February 24, 2016. http://dealbook.nytimes.com/2013/12/09/for-bitcoin-square-peg-meets-round-hole-under-the-law/?_r=0
- King, Douglas. Federal Reserve Bank of Atlanta, *"Retail Payments Risk Forum Working Paper: Banking Bitcoin-Related Businesses: A Primer for Managing BSA/AML Risks"*, 2015.
- Langhirt, Joseph H., Plewa, David., and Greenberg, Michael. *"Bitcoin is property, not currency, IRS says – Notice leaves many open questions about convertible virtual currencies"*, Apr 3, 2014. Accessed May 24, 2016. <https://www.dlapiper.com/en/us/insights/publications/2014/04/bitcoin-is-property-not-currency/>

- Nakamoto, Satoshi., *"Bitcoin: A Peer-to-Peer Electronic Cash System"*, (2009), Accessed June 5, 2016. <https://bitcoin.org/bitcoin.pdf>.
- Palmer, Daniel. *"BOT Suggests Bitcoin Not Illegal But Warns Against its Use"*, (2014), Accessed February 20, 2016. <http://www.coindesk.com/bank-thailand-says-bitcoin-illegal-warns-use/>.
- Ramirez, Michael. *"Jurisdiction update: Thailand — AML"*, July 2, 2013. Accessed April 2, 2016. http://www.tilleke.com/sites/default/files/2013_Jul_Complinet_AML_Thailand.pdf.
- Robbins, Seth. *"Liberty Reserve Case Exposes New Frontiers in Laundering Digital Cash"*, June 4, 2013. Accessed May 24, 2016. <http://www.insightcrime.org/news-analysis/liberty-reserve-case-exposes-new-frontiers-in-laundering-digital-cash>.
- Schoder, D., and Fischbach, K., *"Peer-to-peer prospects: Communications of the ACM"*. ACM, New York USA, Volume 46. Issue 2 (2003). 27–29
- Schoder, D., Fischbach, K., and Christian, S., *"Core Concepts in Peer-to-Peer Networking"*. University of Cologne, Germany, 2005.
- Securities and Exchange Commission v. Trendon T. Shavers, et al. The Complaint, (2014). Accessed June 7, 2016. <https://www.sec.gov/litigation/complaints/2013/comp-pr2013-132.pdf>.
- Smith, Bryan. *"A Close Look at the IRS' Bitcoin Guidance"*, 2014. Accessed May 29, 2016. <http://www.law360.com/articles/524285/a-close-look-at-the-irs-bitcoin-guidance>.
- The Financial Action Task Force, *"Guidance for A Risk-Based Approach Virtual Currencies"*, 2015.

The Financial Action Task Force, "*Methodology: Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT systems technical compliance assessment*", February 2013. Accessed January 13, 2016. <http://www.fatf-gafi.org/media/fatf/documents/methodology/FATF%20Methodology%2022%20Feb%202013.pdf>

The Financial Action Task Force, "*International Standards on Combating Money Laundering and The Financing of Terrorism*", The FATF Recommendations. February 2012. Last modified October 2015. Accessed January 13, 2016. http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf

The Financial Crimes Enforcement Network, "*FIN-2013-A001: Update on Tax Refund Fraud and Related Identity Theft*", 2013.

The Financial Crimes Enforcement Network, "*FIN-2013-G001: Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies*", 2013.

The Financial Action Task Force, "*What is Money Laundering?* ", Accessed January 10, 2016. <http://www.fatf-gafi.org/faq/moneylaundering/>.

United Nations, FATF-GAFI, "*FATF Recommendation 5: Customer due diligence and record-keeping*", May 2015. Accessed August 8, 2016. <http://www.un.org/en/sc/ctc/docs/bestpractices/fatf/40recs-moneylaundering/fatf-rec05.pdf>

United Nations Office on Drugs and Crime, "*Legislative framework: Criminalizing the laundering of proceeds of trafficking in persons*" Accessed March 3, 2016. https://www.unodc.org/documents/human-trafficking/Toolkit-files/08-58296_tool_3-5.pdf.

Watts, Jake Maxwell. *"Thailand's Bitcoin ban is not quite what it seems"*. July 31, 2013. Accessed February 20, 2016. <http://qz.com/110164/thailands-infamous-bitcoin-crackdown-is-not-quite-what-it-seems/>.

3.4.2 Thai

ข่าวหนังสือพิมพ์กรุงเทพฯธุรกิจ. 'ธนาคารแห่งประเทศไทยชี้แจง ระวัง Bitcoin เพราะห่วงแก๊งกำไลบาท', (31 กรกฎาคม 2556) (2556). (Bangkokbiznews. *'Bank of Thailand explanations that suspended Bitcoin because worried about the speculation of Thai Baht'*. (July 31, 2013) (2013))

ธนาคารแห่งประเทศไทย. 'ข่าว สปท. เรื่องข้อมูลเกี่ยวกับ Bitcoin และ หน่วยข้อมูลทางอิเล็กทรอนิกส์อื่นๆ ที่ลักษณะใกล้เคียง', ฉบับที่ 8/2557, (18 มีนาคม 2557) (2557). (Bank of Thailand. *'BOT news: the information about Bitcoin and other electronic data which similar to Bitcoin'*, no.8/2014, (March 18, 2014) (2014)).

ธนาคารแห่งประเทศไทย. 'ธุรกิจปัจจัยชำระเงินต่างประเทศ'. (Bank of Thailand., *'Types of Foreign Exchange Licenses'*). Accessed May 17, 2016. <https://www.bot.or.th/Thai/FinancialMarkets/ForeignExchangeRegulations/ForeignMeansOfPaymentBusinesses/Pages/default.aspx>

เนติบัณฑิตยสภา ในพระบรมราชูปถัมภ์. 'ลักษณะของสัญญา การแบ่งประเภทของสัญญา และการก่อให้เกิดสัญญา', 2555. (The Thai Bar under The Royal Patronage. *'Feature of contract, Classification of contract and Causing of contract'*, 2012). Accessed March 4, 2016. <https://www.thethaibar.or.th/thaibarweb/fileadmin/DAM/2555/PDF/Lecture/LectureTerm1/20/1.pdf>.

มติคณะรัฐมนตรี. 'มาตรการป้องกันปราบปรามการฟอกเงิน และการต่อต้านการสนับสนุนทางการเงินแก่การก่อการร้าย เรื่อง นโยบายการปฏิบัติตามหลักเกณฑ์การรู้จักลูกค้า/การตรวจสอบเพื่อทราบข้อเท็จจริงเกี่ยวกับลูกค้าของสถาบันการเงิน และหน่วยธุรกิจ หรือผู้ประกอบการวิชาชีพที่ไม่ใช่สถาบันการเงิน', 27 กุมภาพันธ์, 2550. (The resolution of the Cabinet. *'Anti-Money Laundering and Combating the Financing of*

Terrorism: AML/CFT on the KYC / CDD policies for financial institution and business or non-financial business', February 27, 2007). Accessed April 18, 2016. http://www.amlo.go.th/amlofarm/farm/web/index.php?option=com_content&view=article&id=863&Itemid=880.

รุ่งเรืองสภากุล, วรณทณี. 'การรู้จักลูกค้า (KYC) และการพิสูจน์ทราบลูกค้า (CDD) ตอนจบ', 2552.

(Ruugruangsapasakul, Wantanee. '*Know Your Customer (KYC) and Customer Due Diligence (CDD) the final chapter*', 2009). Accessed April 18, 2016. <https://www.gotoknow.org/posts/288336>.

แสงเนตรสว่าง, สรรเพชญ. สำนักงานป้องกันและปราบปรามการฟอกเงิน, 'การป้องกันปราบปรามการฟอกเงินและการต่อต้านการสนับสนุนทางการเงินแก่การก่อการร้าย', 22 กรกฎาคม 2557. (Sangnatesawang, Sunpetch. Anti-Money Laundering Office, '*Anti-Money Laundering and Combating the Financing of Terrorism*', July 22, 2014). Accessed April 20, 2016. http://www.tlaa.org/2012/images/activities/pdf/info_file_1_2014_07_22_110605.pdf.

สำนักงานป้องกันและปราบปรามการฟอกเงิน (ปปง.). 'มาตรการป้องกันปราบปรามการฟอกเงิน และการต่อต้านการสนับสนุนทางการเงินแก่การก่อการร้าย เรื่อง นโยบายการปฏิบัติตามหลักเกณฑ์การรู้จักลูกค้า/การตรวจสอบเพื่อทราบข้อเท็จจริงเกี่ยวกับลูกค้า ของสถาบันการเงิน และหน่วยธุรกิจ หรือผู้ประกอบการวิชาชีพที่ไม่ใช่สถาบันการเงิน', 2553. (Anti-Money Laundering Office (AMLO). '*Anti-Money Laundering Measures and Combating the Financing of Terrorism policy guidelines Know Your Customer / Customer Due Diligence of Financial Institutions and Designated Non-Financial Businesses and Professions, DNFBP*', 2010). Accessed April 6, 2016. [http://www.amlo.go.th/amlofarm/farm/information/files/1\(3\).pdf](http://www.amlo.go.th/amlofarm/farm/information/files/1(3).pdf).

4. Other Materials

Mazzant, Amos L. United States Magistrate Judge, Case No.4:13-CV-416, 'Memorandum Opinion Regarding the Court's Subject Matter Jurisdiction', 2013.

Pamplin, Berkley A., 'Virtual Currencies and The Implications for U.S. Anti-Money Laundering Regulations'. Master of Science in Economic Crime Management, Utica College, 2014.

Peng, Starry. 'BITCOIN: Cryptography, Economics, and the Future.' School of Engineering and Applied Science, University of Pennsylvania, December 2013.



BIOGRAPHY

Name	Mr. Pratyapa Apaiyanukorn
Date of Birth	January 24, 1988
Educational Attainment	Year 2010 : Bachelor of Law, 2 nd Class Honors. Thammasat University, Thailand Year 2011 : Thai Barrister at Law
Work Position	State Officer
Work Experiences	August 2013 – Present : Officer at Enforcement Department, The Securities and Exchange Commission, Thailand September 2011 – May 2013 : Legal Officer at Litigation Department, Toyota Leasing (Thailand) Co., Ltd