

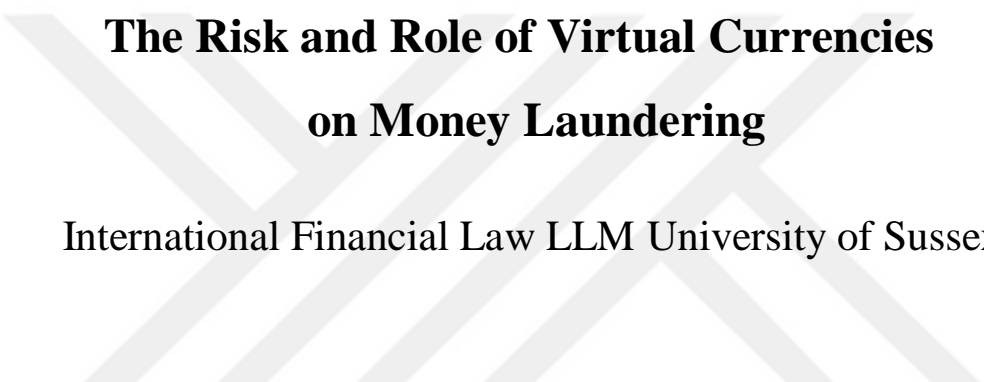
Candidate number: 212738

Title of dissertation: The Risk and Role of Virtual Currencies on Money Laundering

Word count: 9775

Date: 22 September 2020





**The Risk and Role of Virtual Currencies
on Money Laundering**

International Financial Law LLM University of Sussex

Abstract

In this study, the virtual money phenomenon, which has just entered into the economic system, is examined in detail, and its advantages and disadvantages are stated. The crime of money laundering, which has become a threat between states, has been explained with its stages and methods, and the role of virtual money in money laundering is described as one of these methods. It has been determined that cryptocurrencies, which have a wider usage area and higher circulation power than other virtual currencies, are widely used in money laundering crime. The study also examined Silk Road, Liberty Reserve and Western Express International cases, which are essential in this regard, and systematic and legal results were explained. The legal regulations on money laundering have been examined on the basis of the international regulatory institutions, the United Nations, the European Union, the International Monetary Fund and the Financial Action Task Force, and the UK's regulations on this issue have also been analysed in detail. As a conclusion, this dissertation emphasised the importance of international information sharing and legal cooperation in the use of virtual currencies as a tool for money laundering.

Acknowledgements

The completion of this dissertation could not have been possible without my family, friends and relatives. I am thankful for their big love, support and encouragement.

I also would like to express my sincere gratitude to my Supervisor Dr Pablo Iglesias-Rodriguez, for providing his valuable guidance, comments and suggestions throughout the year and the process of planning and writing this dissertation.

TABLE OF CONTENTS

INTRODUCTION.....7

CHAPTER I MONEY

1. Definition and Historical Development of Money.....9

1.1 E-money.....10

1.2 Digital Money.....11

1.3 Virtual Money.....12

1.4 CryptoCurrency..... 13

CHAPTER II MONEY LAUNDERING

2. Stages of Money Laundering.....13

2.1.1 Placement.....13

2.1.2 Separation.....14

2.1.3 Integration.....14

2.2 Methods of Money Laundering.....14

2.2.1 Physical Money Transportation14

2.2.2 Trade-Based Money Laundering14

2.2.3 Casinos and other gambling.....16

2.2.4 Virtual Currencies.....16

2.2.4.1 Linden Dollar.....16

2.2.4.2 Bitcoin.....19

2.2.4.3 Ripple.....22

CHAPTER III Case Studies

3.1 Silk Road.....25

3.2 Liberty Reserve.....26

3.3 Western Express International.....27

CHAPTER IV- The Steps Taken within the Scope of International Combat and Cooperation against Money Laundering Crime

4.1 Regulations of the United Nations (UN).....28

4.2 Regulations of the European Union (EU)29

4.3 Regulations of the Financial Action Task Force (FATF).....31
4.4 Regulations of International Monetary Fund (IMF).....33
4.5 Regulations of the UK.....35

CONCLUSION.....36

BIBLIOGRAPHY.....39



INTRODUCTION

As all commercial activities require trust, a third party is needed, besides the buyer and seller, to establish trust between these two parties. Today, there is a third party in almost all kinds of economic activities that take place except for face-to-face cash transactions. This third party can be a bank where an individual uses their credit card in online shopping, an intermediary institution that allows them to make transactions on the stock exchange, or the state that allows the purchase of a property and protects the property right. These intermediaries reduce uncertainty by auditing and recording the transaction between buyer and seller, and enable transactions for parties that have no reason to trust each other.¹

Financial systems are also built on a model based on trust, which must be constantly audited and controlled. The more effective the supervision and surveillance mechanisms are in the markets, the more effectively the markets function. In this context, governments have established supervisory and regulatory bodies for financial markets which aimed to provide confidence, stability, accuracy and confidentiality for the effective functioning of the markets.

It would not be wrong to say virtual currencies are the most significant financial technology that has emerged in recent years. The development of information technologies, the widespread use of internet and e-commerce have changed people's requests, needs and made intermediaries in the financial sector open to discussion in terms of service cost, speed and security while the popularity of virtual currencies has increased. Despite virtual currencies are not legally regulated entities and pose risks, they have become increasingly preferred due to the benefits they provide compared to traditional payment tools especially for users. Although virtual currencies make commercial transactions and money transfers faster and less costly, they have become the focus of money laundering crime with their anonymity, decentralised structure and their independent transactions from any state.

For those who earn their money illegally, money laundering is a necessary way to avoid criminal prosecution while spending or saving their unfair earnings. Although money

¹ Melih Sefa Yavuz, 'Ekonomide Dijital Dönüşüm: Blockchain Teknolojisi ve Uygulama Alanları Üzerine Bir İnceleme' [Digital Transformation In Economy:A Review of Blockchain Technology and Application Areas] (2019) 4(1) Research of Financial Economic and Social Studies (RFES) 15,16.

laundering is heavily mentioned with the financing of terrorism, as described in the dissertation, there is much more than the financing of terrorism within the scope of the crime.

Money laundering is the removal of money obtained from crime from their source through complex commercial and financial transactions and aims to include it into the economic system. With the increase of globalization and accessibility, virtual currencies have become an important factor in money laundering. In recent years, as an alternative to traditional ways, virtual currencies have started to be used remarkably in money laundering. Money can be transferred without any follow-up, supervision and intervention through virtual currencies in order to remove the money obtained from the crime from its source.

This situation has created a national and international alarm situation, and a new and specific area has emerged in the world of crimes. Old methods and perspectives cannot be applied to the crime of using virtual currencies in money laundering because it is a complex field with a constant flow of new information and requires technical knowledge. That is why studies in this field are important for the development of new perspectives. This dissertation provides information in four chapters regarding the most up-to-date legal and technical developments on this subject.

The first two chapters planned as a definition chapter and aim to give information about the characteristics of the concepts, which is why descriptive methodology is used in this part. In this way, the differences between e-money, virtual money, digital money, crypto currency and their working principles are specified, the steps and methods of money laundering crime are explained, the Linden dollar is examined as virtual money and Bitcoin and Ripple are examined as a crypto virtual money.

In the third part, the cases of money laundering using virtual currencies are examined with the decisions of Silk Road, Liberty Reserve and Western Express International, and it is explained how virtual money has become a crime tool and the consequences of money laundering crime are highlighted. The socio-legal approach is important at this point in terms of examining the effect of law in society through cases.

The fourth chapter includes the legal regulations on the subject. Legislation on this issue is examined specifically in the United Nations, European Union, Financial Action Task Force,

International Monetary Found and UK, and this section is based on understanding the rules surrounding the issue. The doctrinal approach is used in the fourth chapter because it aims to examine the rules in detail and the relationship between rules.

In the conclusion, alternative solutions are shared to explain how to prevent this crime. The law will examine both internal and external standards in common law countries with the normative approach which aims to go beyond the law and targets what the law should be.

This research aims to determine the function of virtual money among the tools used in money laundering with systemic risks and to examine the legal regulations and measures taken in this regard whether well suited or not. It also evaluates possible legal and practical ways to prevent this misuse.

Research Questions

What is the difference between e-money, digital money, virtual currency and crypto currency? How do virtual currencies become attractive as a decentralise currency? Are virtual currencies a curse or a miracle? Why do people prefer distributed ledger technology and blockchain systems over secure market controllers and brokers? What is the role of virtual currencies in money laundering? What is cyberlaundering? Is it possible to prevent money laundering with virtual currencies? Are there any measures taken to use virtual currencies in money laundering?

CHAPTER I

1- Definition and Historical Development of Money

In order for something to be considered as money, it must be a medium of exchange, unit of account and store of value.² The feature of being a medium of exchange is that money can be given to a seller by a buyer in return for a product/service purchase. The unit of account feature is that money can measure value since it is a standard numerical unit used to measure the market value of products, services and other transactions. Its feature of being a value storage tool is that it can be used as a means of saving money due to its constant movement over time. If the money that cannot be spent today is accumulated, the spending power is transferred to a later

²Michael B. Connoly, *'International Business Finance'* (2006) Taylor & Francis e-Library -Routledge, 1st Edn., 11.

time.³

When looking at the historical process of money, it can be seen that commodity money was first used through bartering which is possible when mutual needs are mutually appropriate and depend on a 'double coincidence of wants'. This is what one of the parties wants to give, when the other party wants to receive.⁴ Since it was not always possible for these requests to coincide, the collective memory system was adopted in small communities. Similar to credit, a person could receive goods and services from other group members and offset the value of those goods or services in another way and at another time. For this, collective memory served as a kind of ledger and it was stated that those who did not contribute could be sanctioned.⁵ However, as the groups increased in number, it became difficult to follow, and over time, common representative units such as shells, silver and gold coins began to be used in return for goods and services. These units showed that the gold or silver equivalent of the value written on it would be paid.⁶

With the development of the trade and banking sector, dematerialised banknote money has become widespread.⁷ With the advancements in technology, existing payment systems are unable to meet the requests and needs of the people and the widespread use of the internet, electronic money and virtual currencies are significant concerns today.

1.1 E-money

Electronic money first came onto the agenda in the European Union in 1993, was analysed by the central banks of the member countries, and a report was published on this subject in 1994. In this report, electronic money is broadly defined as a monetary value that can be stored in a technical device and that the developments regarding electronic money are welcomed.⁸

In the E-Money Regulations 2011, electronic money is defined as a monetary value that can be

³ Saifedean Ammous, 'Can Cryptocurrencies Fulfil the Functions of Money?' (2018) 70 *The Quarterly Review of Economics and Finance*, 38, 39.

⁴ Hanna Halaburda, 'Digital Currencies: Beyond Bitcoin' (2016) 103(3) *Digiworld Economic Journal* 77,79.

⁵ Ibid.

⁶ Dror Goldberg, 'Famous Myths of Fiat Money' (2005) 37(5) *Journal of Money, Credit and Banking* 957,961.

⁷ Ibid.

⁸ Report on Electronic Money, European Central Bank (*European Central Bank*, 1998)
<<https://www.ecb.europa.eu/pub/pdf/other/emoneyen.pdf>> accessed at: 03.08.2020.

stored electronically and can be claimed against its issuer.⁹ In simple terms, e-money is an electronic representation of fiat money. Therefore, factors such as the determination of the value of money by the monetary policies executed by the central bank and its issuance by the central bank are valid for e-money.¹⁰

One advantage of using electronic money is that it increases the rate of online shopping. In addition, anonymous electronic money can be used to do anonymous shopping. This may increase the rate of online shopping and help to gain more information about the shopping habits of consumers.¹¹ While shopping online, users are most concerned about their credit card information being stolen.

Currency refers to a generally accepted form of money in the shape of coins or banknotes issued by a government that is used in trade for the exchange of goods and services. In this sense, electronic money is produced by the private sector and lacks coercive power. The ability of electronic money to terminate debt depends on the agreement between the parties to do so.¹² It enables the parties to fulfil their monetary obligations within the framework of a contractual relationship by transferring electronic money.¹³ A certain amount of issued electronic money is deposited. For this reason, the creditor takes into account the amount of electronic money accumulated in the contractual relationship. With the transfer of electronic money in the state of savings, the monetary obligations in the contract are fulfilled.¹⁴

1.2 Digital Money

The amounts seen in bank accounts are a digital representation and substitute for paper money.¹⁵ Digital currency products based on smart cards reduce the demand for banknote currency. In this way, money can be stored and transferred electronically without the need for physical contact. Software-based digital currency products, on the other hand, also affect

⁹ The E-Money Regulations 2011, Sec 2

¹⁰ Katharine Kemp and Ross P Buckley, 'Resolution Powers over E-Money Providers' (2017) 40 UNSWLJ 1539, 1546.

¹¹ A. Michael Fromkin, 'Flood Control on the Information Ocean: Living With Anonymity, Digital Cash, and Distributed Databases' (1996) 15 Pittsburgh Journal of Law and Commerce 395, 400.

¹² Nobuhiko Sugiura, 'Electric Money and the Law: Legal Realities and Future Challenges' (2009) 18(3) Pacific Rim Law & Policy Journal Association 511, 515.

¹³ Ibid.

¹⁴ Ibid 516.

¹⁵ Aleksander Berentsen, 'Monetary Policy Implications of Digital Money' (1998) 51 KYKLOS 89, 91.

transaction deposit demand due to the reduced transaction costs and learning spreads, facilitating and reducing the cost of transferring value between different account types, banks and countries.¹⁶

Some opinions consider these coins only as of the online monitoring of the money in deposit and that there is no separate concept called ‘digital money’.¹⁷ In the case *Armstrong DLW GmbH v Winnington Networks Ltd.*, EU carbon credits recorded in electronic form registers were considered to be available ‘only in electronic form’, and stated that they had no separate qualifications.¹⁸

1.3 Virtual Money

Virtual money is a type of electronic money as well as a type of unregulated digital money. Virtual money and electronic money are both in digital form.¹⁹ However, there are differences between them. In electronic money, the unit of account is traditional and legal in circulated currencies such as the Pound Sterling, Euro and the Dollar. However, virtual currencies are currencies such as Bitcoin, Linden Dollars and Ripple were invented later and have no legal circulation. Electronic money is accepted by anyone other than the issuer. Virtual currencies are accepted within a specific virtual community. Electronic money is regulated legally, whereas virtual currencies have no legal regulation. There are legally regulated electronic money institutions that issue electronic money, while virtual money is issued by private individuals who are not in the financial field. The supply of electronic money is fixed. In virtual currency, the supply of money is not fixed and depends on the issuer. The par value of electronic money is guaranteed, while in virtual currency it is not guaranteed. Electronic money is under control, while virtual money is not. Risk in electronic money can be operational in terms of credit and circulation capability in virtual currency.²⁰

¹⁶ Ibid 93.

¹⁷ Kelvin F.K. Low and Ernie Teo, ‘Chapter 10-Legal Risks of Owning Cryptocurrencies’ *Handbook of Blockchain: Digital Finance and Inclusion (Cryptocurrency, FinTech, InsurTech and Regulation)* (Nikki Levy, 2017) 229.

¹⁸ [2012] EWHC 10 (Ch) (11 January 2012) as cited in: Kelvin F.K. Low and Ernie Teo, ‘Legal Risks of Owning Cryptocurrencies’ *Handbook of Blockchain: Digital Finance and Inclusion (Cryptocurrency, FinTech, InsurTech and Regulation)* (Nikki Levy, 2017) 230.

¹⁹ Sarah Rotman, ‘Bitcoin versus Electronic Money’ (2014) CGAP Report No: 88164 1.

²⁰ Beate Sauer, ‘Virtual Currencies, the Money Market, and Monetary Policy’ (2016) 22 *Int Adv Econ Res* 117, 126.

1.4 Cryptocurrency

Crypto coins, seen as an alternative to the classical banking system, allow round the clock and instant money transfer transactions. Crypto currencies are alternative currency, they are digital and also virtual money at the same time. Although cyripto currencies are systems that work with similar principles, they vary among themselves. The vast majority of crypto currencies work with the logic of Bitcoin, very few cryptocurrencies differ in terms of technical features and bring a different approach.²¹ Although hundreds of cryptocurrency types are available as of today, it should not be ignored that there have been many unsuccessful attempts. Bitcoin, Ethereum and Ripple are the top three coins by market capitalisation.²²

Ethereum is built on the blockchain system similar to Bitcoin, but Ripple is different from these two cryptocurrencies in that it is a money transfer network created for banks and payment systems. Although the Ethereum system is similar to the Bitcoin system, Ripple has followed a different path and the Bitcoin and Ripple systems will be analysed in detail in the next chapter.

CHAPTER II

2-Money Laundering

Activities such as smuggling, extortion, blackmail, drug and human trafficking constitute a large part of the proceeds from crime and these revenues is dirty money. Money laundering is defined as the action taken to hide the source of these illegal revenues obtained from crime and to remove them from their source as much as possible with certain processes, in order to include these revenues in the financial system.²³

2.1 Stages of Money Laundering

2.1.1 Placement

²¹ European Central Bank, 'Virtual Currency Schemes – A Further Analysis' (2015)

<<https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf>> accessed at:10.08.2020.

²²CoinMarketCap 'Top 100 Coins by Market Capitalization' (CoinMarketApp, 2020) <<https://coinmarketcap.com/coins/>> accessed at:10.08.2020.

²³ Fabian Maximilian Teichmann, 'Recent Trends in Money Laundering' (2020) 73 Crime Law Soc Change 237, 240.

The fact that the earnings from crime are usually in the form of large amounts of money makes it difficult to use these revenues as a payment tool through the financial system or to transfer them to different persons or organisations. Therefore, revenues have to go through the first stage of the laundering process, which is the placement stage, also called the inclusion of funds into the financial system.²⁴ Placement is performed in two ways, these being by primary and secondary deposit. Primary deposit is the division of the income obtained from crime and its transfer to different sources directly, while the secondary deposit is the indirect inclusion of money in the economic system due to transactions made on behalf of natural or legal third parties.²⁵ The placement stage aims for the crime revenue to be leaked into the system.

2.1.2 Separation (Layering)

The purpose of the separation phase is to remove the funds, which were included in the system during the placement phase, from their source by going through multiple transfers and transactions.²⁶ Electronic payment systems and changing jurisdiction with inefficient cooperation of criminal prosecution facilitate this process. Especially with the help of tools that allow rapid fund transfer, it becomes impossible to track, find and capture these funds.²⁷ Thus, the capital transfer is legitimised through the pricing and unreal billing of fictional goods or services such as real estate, art or antiques and consulting firms.²⁸ In this way, it aims to break the link between crime and revenue during the separation phase.

2.1.3 Integration

The integration stage is the stage where the crime proceeds return to the source. After the funds are included in the financial system and make their tracking difficult through complex transactions, they are then brought back to the source with a legal outlook.²⁹ The integration phase is the culmination of a successful money laundering process.

2.2 Methods of Money Laundering

²⁴ Ibid 239.

²⁵ Friederich Schneider & Ursula Windischbauer, 'Money Laundering: Some Facts' (2008) 26 Eur J Law Econ, 387, 395.

²⁶ Ibid 396.

²⁷ Ibid.

²⁸ Teichmann Fabian Maximilian, J. 'Twelve Methods of Money Laundering' (2017) 20(2) Journal of Money Laundering Control 130, 134.

²⁹ See (28).

2.2.1 Physical Money Transportation

In cases where the funds in cash form are not able to be integrated into the financial system, it may be possible to transfer these funds to another country physically.³⁰ In order to prevent money laundering through physical money transfers, strict measures are implemented in the countries' customs and restrictions have been placed on carrying cash above an amount determined by law. This regulation created the smurfing (structuring) system, which allows the funds to be divided into small amounts and included in the financial system. However, series of precautions have been taken to prevent physical money transportation including educated dogs, x-ray machines, statistical analyses of data and restriction on the provision of HD notes such as the 500 Euro banknote.³¹

2.2.2 Trade-Based Money Laundering

Trade-based money laundering is the inclusion of money in the financial system by showing the source of the income obtained from crime as though it were obtained from legal trade. Front and/or shell firms used for this purpose try to include the funds in the financial system by creating fictitious exports and sales.³² Although these companies have specific fields of activity and addresses in official documents, the situation in question just for appearances. Establishing these firms in off-shore regions which do not engage in any commercial or manufacturing activities and where banking laws are weak and confidentiality obligations are not strong, is one of the common methods preferred by money launderers.³³

Buying and reselling high-value goods with money from crime, making fictitious purchases, billing more or less at the time of purchase, and creating fake employment (black salaries) are also trade-based money laundering methods like shell companies.³⁴

2.2.3 Casinos and other gambling

³⁰ FATF, 'Money Laundering Through the Physical Transportation of Cash' (*www.fatf-gafi.org*, 2015) 8
< <https://www.fatf-gafi.org/media/fatf/documents/reports/money-laundering-through-transportation-cash.pdf> > accessed at:20.08.2020.

³¹ Ibid 88.

³² FATF, 'APG Typology Report on Trade Based Money Laundering' (*www.fatf-gafi.org*, 2012) 36
<https://www.fatf-gafi.org/media/fatf/documents/reports/Trade_Based_ML_APGReport.pdf > accessed at:30.08.2020.

³³ FATF, 'Professional Money Laundering' (*www.fatf-gafi.org*, 2018) 30
<<http://www.fatf-gafi.org/media/fatf/documents/Professional-Money-Laundering.pdf>> accessed at:31.08.2020.

³⁴ Ibid 37.

The most important factor for money launderers is the use of casinos, as these venues are cash-intensive. Cash-weighted casinos are authorised to perform many financial transactions such as opening loans, extending the loan terms, safe-leasing services and check turnovers.³⁵

By creating the impression that the money has been won through gambling, it is also possible to remove the dirty money from its source by gambling. In this case, a large amount of money can be added into the system within a few hours.³⁶

2.2.4 Virtual Currencies

The use of virtual currencies in money laundering has become one of the most preferred methods in recent years. The confidentiality of identity information and not being under the supervision of any authority makes the system open to many forms of illegal financial transfers. Especially in deep web and dark web transactions, the use of virtual money is preferred for money laundering and terrorist financing.

2.2.4.1 Linden Dollar

The use of virtual currencies as a money laundering crime tool has started primarily through online games. The game called Second Life is one of the first and popular examples of this. Second Life is a platform-based environment whose economy is based on the purchase and sale of products such as clothes, experiences and commodities.³⁷ Linden dollars (L\$) were produced and developed by Linden Research Inc in 2003 for Second Life and its virtual community started using its own currency in 2006 through their online characters which called 'avatar'.

Economic activities in the Second Life game are solely related to the trading of virtual goods and services. All transactions take place entirely within the infrastructure developed by Linden Labs and there is no real-world counterpart like Bitcoin. However, it is possible for the characters of the game to turn the virtual money earned during the game into reality.³⁸ Second

³⁵ Jeffrey Simser, 'Money Laundering: Emerging Threats and Trends' (2012) 16 (1) *Journal of Money Laundering Control* 41,47.

³⁶ *Ibid.*

³⁷ Clare Chambers-Jones, 'Money Laundering in a Virtual World' (2018) in C. King, C. Walker and J. Gurulé (eds.) *The Palgrave Handbook of Criminal and Terrorism Financing Law* (Palgrave Macmillan, 2018) 174

³⁸ Robert Stokes, 'Virtual money laundering: the case of Bitcoin and the Linden dollar' (2012) 21(3) *Information and Communications Technology Law* 221, 227.

Life has two membership levels, basic and premium. Premium members pay a certain monthly amount and experience a more advanced game than basic members. Basic members, on the other hand, experience a free though limited game. Premium members also get a 300 Linden dollar stipend weekly.³⁹ Besides, anyone who wants to buy Linden dollars must use a credit card or have a PayPal account. The money earned in Linden dollars can then be converted into US dollars at the currency exchange office in the game and transferred to a real-life bank account via PayPal.⁴⁰ Linden dollars can be earned by trading LindeX virtual currency exchange or virtual products. One US dollar is approximately 320 Linden dollars, and this number can change daily.⁴¹

Although Second Life is located in a virtual environment, some transactions can pose real problems and players may need to be protected as consumers in this market. Linden Dollars are supplied by Linden Labs. It has been criticised that if the company offers a Linden Dollar at any random time, it would create an excess of money and the currency would likely lose value at any time.⁴²

Due to the fact that the simulation banks in the game give high interest on Linden dollars purchased with real money, many players have converted their real money to Linden dollars and deposited their virtual money in these virtual banks. Upon the 2007 bankruptcy of Ginko Financial, a bank in the game, Second Life players who had accounts in this bank lost approximately 750,000 dollars in real money.⁴³ After that, Linden Labs asked Second Life users to prove that they were authorised by financial institutions to earn interest or income from investments. Banks that did not prove this were closed in the game.⁴⁴

Since the Linden dollar was not recognised as a virtual currency by the Financial Crime Enforcement Network (FinCen) until 2013, it provided an excellent background for terrorists, organised crime and even normal business owners to transfer money to undetected parties,

³⁹ Ibid 224.

⁴⁰ Ibid.

⁴¹ CurrencyRate '1 USD US Dollar to LD Linden Dollar' <<https://usd.currencyrate.today/ld>> accessed at: 01.09.2020.

⁴² European Central Bank 'Virtual Currency Schemes' (2012) 1, 30

<<https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>> accessed at:01.09.2020.

⁴³ Ibid 31.

⁴⁴ Ibid.

especially during this period.⁴⁵ It is possible to do this even with 15-20 virtual characters created in the game. The money can be transferred to a single source by distributing the crime revenue to these accounts using the smurfing method and this revenue can be laundered by purchasing real estate from a co-conspirator, which is just one of the bogus identities involved.⁴⁶ By collecting all of the money into a single account, the seller moves the money away from their source and reaches them again.

According to the rules of the Second Life game, Linden Labs is not obliged to compensate for Linden dollars lost in the game database. They are exempt from recovering damages caused by any operational problem that may occur in the game.⁴⁷ In Second Life, players are also vulnerable to fraud. In the game, it is unclear who the other player really is with whom one player is cooperating, and how far the money can be traced back to a particular player in any money flow.⁴⁸ The lack of legal regulation and knowledge when opening an account for this game provides the ideal environment for criminals, terrorists, fraudsters and those who want to launder money to participate in this game.

In a report by the US Treasury Department Office FinCen dated March 18, 2013, the definition of virtual money and fiat money was made, and the concepts of ‘user’, ‘exchanger’ and ‘administrator’ were explained within the scope of convertible money. According to the report, the user is a person who buys virtual currency to purchase goods and services and the exchanger is the person who sells products and services through virtual currency while the party that puts virtual money into circulation and withdraws it from circulation is the administrator. In this way Linden Labs, as the Linden dollar exchanger and administrator, has also become subject to taxation and the guidance aimed to facilitate the control.⁴⁹

Linden dollars, which have been subject to tax applications since 2013, is required to provide personal information such as a full name and address, date of birth and US social security

⁴⁵ James Elliott, ‘Help – Somebody Robbed my Second Life Avatar!’ (2008) 1(1) Virtual Worlds Research: Past, Present and Future 1, 5.

⁴⁶ Ibid.

⁴⁷ See (44) 32.

⁴⁸ Ibid.

⁴⁹ FinCen ‘Application of FinCEN’s Regulations to Persons Administering, Exchanging or Using Virtual Currencies’ (2013) <<https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf>> accessed at:03.09.2020.

number, or passport and photo ID to the Linden Labs subsidiary Tilia as of 2019, with a focus on preventing money laundering.⁵⁰

2.2.4.2 Bitcoin (BTC)

Cryptocurrencies entered the financial world as a phenomenon when a Japanese programmer, alias Satoshi Nakamoto, created Bitcoin in 2009.⁵¹ The constant increase in the transaction volume of Bitcoin and the volatility of its value against the US dollar played an active role in attracting attention in the financial markets.⁵² Although there are many types of virtual currencies as of today, Bitcoin, was the first crypto money and example of a crypto virtual currency in the technological sense, and thus is the best known and most-used virtual currency since its inception.

The currency's smallest unit of value is equal to one 100 millionth of a Bitcoin (0.00000001 BTC) which called 'satoshi' and inspired by Satoshi Nakamoto and produced by mining.⁵³ Anyone can become a Bitcoin miner and produce Bitcoins by running their software with specialised hardware. Bitcoin mining is the process of creating a new block for the Bitcoin blockchain, requiring a great deal of energy consumption, processing power and an extremely fast internet connection as possible.⁵⁴

Bitcoins are mined using a mathematical method which is an intense computer application that solves difficult problems within the Bitcoin network. In today's monetary system, when the supply of money in circulation increases, inflation risk arises and the value of money falls. That is why, the mathematical operations are becoming increasingly difficult as the Bitcoins to be produced and designed are limited to 21 million to prevent this risk. In today's monetary system, when the supply of money in circulation increases, inflation risk arises and the value of money falls. According to researches, the rate of Bitcoin production is halved every four

⁵⁰Juha Saairinen 'Virtual world Second Life to enforce anti-money laundering regs' <<https://www.itnews.com.au/news/virtual-world-second-life-to-enforce-anti-money-laundering-regs-527558>> accessed at: 03.09.2020.

⁵¹ Tony Klein, Hien Pham Thu, Thomas Walther 'Bitcoin is not the New Gold – A comparison of volatility, correlation, and portfolio performance' (2018) 59 International Review of Financial Analysis 105

⁵² Halaburda (n 6) 84.

⁵³ Malcolm Campbell-Verduyn, (Ed.) 'Bitcoin and Beyond' (2018) RIPE Series in Global Political Economy London: Routledge, 133.

⁵⁴ Florian Tschorsch and Björn Scheuermann, 'Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies' (2016) 18 (3) IEEE Communications, Surveys & Tutorials 2084, 2087.

years.⁵⁵

Miners need to prove to the network that they verify their transactions using an algorithm; which is called proof of work. Each new block must contain proof of work to be accepted by the rest of the network. According to the proof of work system, when the block content is inferred with the number found by the miners, the result should be lower than the difficulty target of the network.⁵⁶ It is barely possible for malicious people to manipulate the data due to the use of a private/public key encryption method.⁵⁷

Every transaction made with Bitcoin is recorded on a blockchain that acts as a general registry. The blockchain contains the information for all transfers made in the Bitcoin network and makes it possible for all users in the network to access the information. The blockchain is carried out using a method of sequencing each transaction one after another, which is then approved by the users included in the network. Thus, each transaction that participates in the blockchain is stored as a single file and is accessible to anyone who wants.⁵⁸

A Bitcoin transaction spreads across the Bitcoin network in a concise time, measured in seconds, but takes time to be approved by other users. Subjecting Bitcoins to any transaction by a user become valid by digitally signing the transaction. Other users on the network immediately deny an operation that is not valid. Nobody can spend Bitcoins that they do not own, but there is a risk that the same Bitcoins will be subjected to other transactions within the time taken to confirm the transaction.⁵⁹ Since the confirmation of the transaction takes time, although the information of a transaction is spread to the whole network in a short time. This risk is called 'double spending'. At least six different end-to-end transactions are expected to be approved to eliminate the double-spending risk. This risk has been overcome by the blockchain method.⁶⁰

The Bitcoin wallet is used to store money. The difference from a regular wallet is that instead of storing cards or bonds, the Bitcoin wallet keeps Bitcoin private keys. Unlike the Bitcoin

⁵⁵ See (11).

⁵⁶ Tschorsch et al (n 56) 2091.

⁵⁷ Ibid 2117.

⁵⁸ Aurelio F. Bariviera, Maria Jose Basgall, Waldo Hasperue 'Some Stylized Facts of the Bitcoin Market' (2017) 484 *Physica A Statistical Mechanics and its Applications* 82, 83.

⁵⁹ See (18) 236.

⁶⁰ Ibid 242.

network, the Bitcoin wallet can be only controlled by its owner that is why the security of users' private keys is of great importance.⁶¹

Bitcoin is a peer-to-peer electronic money transfer system, which means that the central authority does not follow money transfer transactions and the Bitcoins received in purchases are sent directly to the another Bitcoin wallet.⁶² Transactions are anonymous with using pseudonyms, and occur between Bitcoin addresses which are digital aliases.⁶³ All Bitcoin transfer transactions occur publicly and are constantly in the network. In this way, anyone is able to see the amount of Bitcoin transfer transactions belonging to any Bitcoin address. However, the identity of the Bitcoin user who owns that address is hidden and the buyer and seller can not be fully tracked.⁶⁴

Transactions are transparent, fast and global. Since the first Bitcoin offering in 2009, all transactions have been publicly visible. Transactions in nominal physical money have no memory, although Bitcoin transaction memory is kept in blockchain databases, which act as a global ledger.⁶⁵ Transactions made are instantly reported to the Bitcoin network around the World and transactions can not be undone. No authority, state, individual, computer programmer, or even those who designed the system, can change or undo a transaction that has been approved by one of the miners, accepted by the others, and written on the blockchain.⁶⁶ No permission is required from any person or organisation to make a transaction and no one can prevent the transaction from being made.

It is possible to convert Bitcoin to real currencies, but it can only happen if someone wants to buy Bitcoins. In other words, if there are people who want to enter the system and buy Bitcoins, it would be possible to convert Bitcoin to real money. This means that if anybody want to exit the system completely, this may not be possible due to a lack of liquidity.⁶⁷

Unlike real currencies, Bitcoin is not affected by the economic situation of any country, as it is not affiliated with any country's central bank. In addition, since it is not known to whom it belongs nor is it monitored by a central authority, it is not possible to encounter a threat such

⁶¹ 'How does bitcoin work?' <<https://bitcoin.org/en/how-it-works>> accessed at:03.09.2020.

⁶² Rotman (n 21) 2.

⁶³ Tschorsch et al (n 56) 2103.

⁶⁴ Tschorsch (n 56) 2109.

⁶⁵ Ibid 2086.

⁶⁶ Ibid 2084.

⁶⁷ See (44) 27.

as a freezing or seizing of accounts opened with Bitcoin.⁶⁸ Traditional financial systems make audits easier because the currencies used in these financial systems have a central control mechanism. There is no central registry for in Bitcoin and other cryptocurrencies, so there is no authority to prevent and supervise the abuse of the system.⁶⁹ According to SEC v. In the Shavers, an online Bitcoin forum was promised 7% interest per week to investors. However, Bitcoins bought by new investors were used for the payments to existing investors and for the personal expenses of those who organised the investment by making conversion to US dollars.⁷⁰

In blockchain technology, transactions are verified through a consensus mechanism and recorded in the chain. This process is possible when more than half of the participants verify the data to be recorded on the network. Due to a security issue called '51% Attack', malicious individuals may delete, modify, or stop the network's operation if they hijack more than half of the accounts of participants on the network.⁷¹ This situation raises concerns about the security of private / permitted networks, which are expected to be more limited in terms of the number of participants.

The ability to open accounts anonymously with pseudonyms and the deficiencies in the field of identification make it attractive to use this system with malicious intent by launderers and people who want to finance terrorism. During the account opening process, it is not possible to determine for whom and for what purposes the transactions are performed with the use of alphanumerically generated customer numbers. The unique key generated for each transaction provides privacy to its users.⁷² But this privacy can be a disadvantage in terms of detecting suspicious transactions. All of this raises concerns about Bitcoin's legal status and whether it is safe or likely to be used for illegal purposes.

2.2.4.3 Ripple (XRP)

Ripple, one of the most well-known and most used virtual currencies, has managed to differentiate itself from Bitcoin by using Bitcoin infrastructure. Inspired by the idea of Bitcoin,

⁶⁸ Tschorsch (n 56) 2085.

⁶⁹ Bariviera et al (n 60) 83.

⁷⁰ Case No. 4:13-CV-416 <https://edisciplinas.usp.br/pluginfile.php/2836197/mod_resource/content/1/SEC-v-Shavers-No-4-13-CV-416-E-D-Tex-Sept-18-2014.pdf> accessed at:04.09.2020.

⁷¹ Yavuz (1) 27.

⁷² Bariviera et al. (n 60) 84.

programmers developed Ripple in May 2011, where transactions were verified by a consensus process between users, not by mining activities as in the Bitcoin system.⁷³ Unlike the Bitcoin system, all currencies in Ripple are pre-created by the system's developers.⁷⁴ Since it is not a process like mining, Ripple consumes less electrical energy.

Ripple has an algorithm that creates reliable subnets within the system.⁷⁵ In this way, it does not require all participants in the system to be in synchronised communication as it is in other virtual currencies using Bitcoin technology, and the transaction processes are faster than the others.

As an alternative to systems that require synchronisation like Bitcoin, the Ripple Protocol Consensus Algorithm introduces a new method called the Unique Node List (UNL).⁷⁶ Each node in the Ripple system has this list of servers that it queries during the consensus process. Unlike the approval of each participant in the Bitcoin system, each participant in the consensus process only takes into account only the other members in their UNL. Therefore, the UNL of any participant consists of servers that the participant trusts will not defraud the system collectively. It is anticipated that these servers will not send false information to the network in a coordinated manner.⁷⁷

The Ripple system is built on an open protocol that allows payments between different systems and networks, and is built to be compatible with the existing infrastructure used by banks. As of September 2016, Ripple announced the establishment of the first interbank group to work with distributed financial technology for global payments. Bank of America Merrill Lynch, Santander, UniCredit, Standard Chartered, Westpac Banking Corporation and Royal Bank of Canada are founding members of GPSG.⁷⁸ This group will oversee the establishment and maintenance of Ripple payment transaction rules, official standards of transactions and is

⁷³David Schwartz, Noah Youngs, Arthur Britto, 'The Ripple Protocol Consensus Algorithm' (2018) <https://ripple.com/files/ripple_consensus_whitepaper.pdf> accessed at:04.09.2020

⁷³ Bariviera et al. (n 60) 84.

⁷⁴ Beat Weber, 'Competing for legitimacy: A typology of virtual currencies' (2016) Preliminary draft prepared for the 2nd International Workshop on P2P Financial Systems 10 accessed at:01.09.2020. <https://www.p2pfsys.com/wp-content/uploads/2017/04/paper_11-min.pdf>

⁷⁵ Ammous (n 2) 45.

⁷⁶ Sufian Hameed & Sameet Farooq, 'The Art of Crypto Currencies: A Comprehensive Analysis of Popular Crypto Currencies' (2016) 7(12) International Journal of Advanced Computer Science and Applications (IJACSA) 426, 429.

⁷⁷ Schwartz et al (n 72) 3.

⁷⁸ Marcus Treacher, 'Announcing Ripple's Global Payments Steering Group' (2016) <<https://ripple.com/insights/announcing-ripples-global-payments-steering-group/>> accessed at:04.09.2020.

engaged in the development of their payment capacity applications. It is distributed through business development agreements, initiatives given to liquidity providers and sales to institutional buyers who are considering investing in XRP.⁷⁹ Finally, money transfer costs between banks included in the Ripple network are very low compared to other digital currencies. In 2018, the money transfer transaction fee in the Ripple network was \$ 0.0011 on average, while these fees were \$ 3.5 in Bitcoin and \$ 0.30 in Ethereum.⁸⁰

3. Case Studies

What we call the Internet can be roughly divided into three layers: the surface web, the deep web, and the dark web.⁸¹ The surface web is the ‘world wide web’ that everyone uses. The deep web is a large pool of information that contains content that cannot be indexed by search engines such as Google, and that search engines do not have direct access to their databases.⁸² Michael Bergman, who was the first to introduce the term ‘deep web’ and is one of the leading authorities in this regard, found that the deep web is 450-550 times bigger than the world wide web. In addition, Bergman stated that the deep web is the area where information grows the fastest on the internet.⁸³ The dark Web is specified as an area in which illegal activities are carried out within the deep web.⁸⁴

The Onion Router (Tor) emerged in 2002 as a joint project entirely between the US Naval Research Laboratory and the non-profit Free Haven Project.⁸⁵ The main purpose of the project is to create a distributed, anonymous and encrypted network to be used by those who need it. In other words, Tor's purpose is to create a network platform that will keep the transmitted data anonymous.⁸⁶ Log in to the deep and dark web is possible with a Tor connection.⁸⁷

⁷⁹ Ibid.

⁸⁰ Yavuz (1) 21

⁸¹ Debiel Santos, ‘What the Dark Web Is and Isn’t’ (2017)

< <https://www.smartdatacollective.com/what-dark-web-and-isn-t/> > accessed at:04.09.2020.

⁸² Vincenzo Ciancaglini, Marco Balduzzi, Robert McArdle, and Martin Rösler, ‘Below the Surface: Exploring the Deep Web’ (2015) Trend Micro 1, 5.

⁸³ Michael Bergman, ‘White Paper: The Deep Web: Surfacing Hidden Value’ (2001) 7(1) The Journal of Electronic Publishing <<https://quod.lib.umich.edu/jjep/3336451.0007.104?view=text;rgn=main>> accessed at: 04.09.2020.

⁸⁴ Ciancaglini et al. (n 80) 6.

⁸⁵ Tor, ‘About, History’ <<https://www.torproject.org/about/history/>> accessed at: 04.09.2020.

⁸⁶ Brett Hawkins, ‘Under the Ocean of the Internet- The Deep Web’ (2016) SANS Institute Information Security Reading Room 1, 9.

⁸⁷ Santos (n 79) 1.

3.1 Silk Road

The dark web drew all the attention with the arrest of Ross William Ulbricht who is the founder of the Silk Road website. The Silk Road which was the first successful anonymous marketplace on the dark web, was launched in 2011 and designed as a platform where sellers and buyers can shop anonymously over the internet like an Amazon web site.⁸⁸

It was revealed that Ulbricht used two different ways to anonymise the operations on the Silk Road he had established. Firstly, it used the Tor network to anonymise its customers, and secondly, it carried out all illegal transactions with Bitcoin.⁸⁹ Users bought and sold drugs and illicit goods anonymously with the help of Silk Road. Law enforcement started secret drug purchases through Silk Road in December 2011. An operation was initiated in 2013 with an undercover agent who agreed to sell drugs and also commit murder. According to the FBI's claim, 144.000 Bitcoins worth \$28.5 million were found when Ulbricht's computer was seized and he was arrested.⁹⁰

The Silk Road case was pointed out by the FATF to show that bitcoins can be used for criminal as well as legal instruments.⁹¹ It is stated that, hundreds of millions of dollars obtained from crime were laundered according to the bitcoin value on the seizure dates of Silk Road through similar illegal transactions.⁹² One of the challenges with virtual currencies is that the entire transaction process does not require the involvement of a traditional bank at any stage and that is why the follow-up was carried out by the FBI. Another consequence of this case is that there is now a new type of crime on the Internet that requires a different skill and a different investigation process than traditional crimes.⁹³

⁸⁸ Hawkins (n 84) 13.

⁸⁹ Ibid 14.

⁹⁰ Andy Greenberg, 'FBI Says It's Seized \$28.5 Million In Bitcoins From Ross Ulbricht, Alleged Owner Of Silk Road' (2013) <<https://www.forbes.com/sites/andygreenberg/2013/10/25/fbi-says-its-seized-20-million-in-bitcoins-from-ross-ulbricht-alleged-owner-of-silk-road/#2f4ff5ec2765>> accessed at: 05.09.2020.

⁹¹ FATF, 'Virtual Currencies Key Definitions and Potential AML/CFT Risks' (2014) <<https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>> accessed at:05.09.2020.

⁹² Ibid.

⁹³ Mohammad Ahmad Naheem, 'Exploring the links between AML, digital currencies and blockchain technology' (2019) 22 (3) Journal of Money Laundering Control 515,520.

The discovery by the FBI of this illegal activity being carried out on the internet has increased the curiosity of the whole world and has revealed the need to examine the deep web and the dark web, in many areas.

3.2 Liberty Reserve

The Liberty Reserve (LR) case is touted as the world's most massive money-laundering operation. In Federal prosecutors arrested Arthur Budovsky, founder of the Costa Rica-based Liberty Reserve, the international organisation of money laundering and unlicensed money transfers on May 2013 for money laundering.⁹⁴

Unlike the Silk Road, the LR case involved a type of bank structure that effectively converted fiat dollars into its own virtual currency called Liberty dollars. According to the LR system, customers convert their money into LR dollars and transactions can be made anonymously with other LR accounts for an additional fee and also the money can then be converted from LR dollars to fiat currencies. The funds can then be converted from LR dollars to fiat currencies.⁹⁵ Due to this anonymity, Liberty Reserve has been the preferred as a bank of the criminal underworld by laundering over \$ 6 billion between 2006 and 2013.

It has been stated that over a period of seven years, LR has laundered billions of dollars in money laundering and almost all of the LR activities are due to criminal activities.⁹⁶ According to US officials, credit card fraudsters, identity card thieves, hackers, child pornography businesses and drug dealers are the first to use this route. After the capture of Arthur Budovsky, the websites and accounts associated with the company were closed and a total of \$25 billion was withdrawn from circulation and founder he was sentenced to 20 years imprisonment.⁹⁷ The U.S. Department of the Treasury has identified Liberty Reserve as the primary financial institution for money laundering under Section 311 of the U.S. Patriot Act.⁹⁸

⁹⁴ Jay B. Sykes and Nicole Vanatko, 'Virtual Currencies and Money Laundering: Legal Background, Enforcement Actions, and Legislative Proposals' (2019) Congressional Research Service Report, 1,9 <<https://fas.org/sgp/crs/misc/R45664.pdf> > accessed at:01.09.2020.

⁹⁵ Ibid.

⁹⁶ See (91).

⁹⁷ US Department of Justice, 'Liberty Reserve Founder Sentenced to 20 Years For Laundering Hundreds of Millions of Dollars' (2016) <<https://www.justice.gov/opa/pr/liberty-reserve-founder-sentenced-20-years-laundering-hundreds-millions-dollars> > accessed at: 05.09.2020.

⁹⁸ See (89).

After this case, it was decided that unlicensed exchanges such as Liberty Reserve will not be used by banks within the scope of anti-money laundering (AML) application.⁹⁹ It is a critical case in terms of having beneficial ownership information about customers and creating an AML framework to report suspicious transactions and accepting that virtual currencies are regulatory transactions.¹⁰⁰

3.3 Western Express International

The eight-year investigation of Western Express International, an internet-based cybercriminal group, resulted in the conviction of 16 members for global identity theft and cyber fraud.¹⁰¹ Cybercrime group members communicated through ‘card creation’ web sites that smuggle stolen credit cards and personal identity information. It is intended to evade law enforcement and regulatory agencies through fake IDs, anonymous messaging, email, and virtual currency accounts.¹⁰²

Merchants sold nearly 100,000 stolen credit cards and personal identification information online and received payments through e-Gold and Web Money. Buyers, on the other hand, earned criminal proceeds of approximately US \$5 million with additional crimes such as illegal possession of stolen goods and fraud.¹⁰³

Western Express International is a Manhattan-based New York company that operates as a virtual currency exchange and money changer to coordinate internet payment methods used by the criminals and launder their revenues.¹⁰⁴ The money carrier laundered the illegal revenues of the cybercriminal group and earned more than \$35 million through various accounts.¹⁰⁵

In this file, it has been seen that the internet usage habits of criminal enterprises may be fundamentally different from traditional organized criminals, and it has been realized that unlike other files, the processes of using the initiative, decision-making and legal investigation have become difficult at this point.

⁹⁹ Ibid.

¹⁰⁰ See (91).

¹⁰¹ See (89) 12.

¹⁰² Ibid.

¹⁰³ Ibid.

¹⁰⁴ Naheem (n 91) 522.

¹⁰⁵ See (99).

CHAPTER III

4-The Steps are Taken within the Scope of International Combat and Cooperation against Money Laundering Crime with Cryptocurrencies

4.1 Regulations of the United Nations (UN)

International efforts to prevent money laundering are aimed at preventing the financing of terrorism and the criminal economy created by illegal revenues by criminal or terrorist organisations or criminal individuals. That is why the United Nations Office of Drugs and Crime (UNODC) was established to carry out the Global Programme against Money-Laundering, Proceeds of Crime and the Financing of Terrorism.¹⁰⁶

The 1988 United Nations Convention Against the Trafficking of Narcotic Drugs and Psychotropic Substances is the first international convention to criminalise money laundering.¹⁰⁷ The Global Program against Money Laundering (GPML) was created in 1997 in response to an authorisation arising from the 1988 Convention. This programme includes the need to regulate the financial activities of member states and to take legal and administrative precautions to facilitate the detection, investigation and prosecution of money laundering.¹⁰⁸

The UN Convention against Transnational Organized Crime, adopted by the UN General Assembly in Palermo, Italy in 2000, requires member states to agree on the definition of crime in the fight against money laundering and the financing of terrorism, thus eliminating the situation that crime in one country is not a crime in another. It aimed to remove. Also, it emphasised the importance of the legal and operational unity of the countries by referring to the 40 recommendations published by the FATF on this issue.¹⁰⁹

¹⁰⁶UNODC ‘UNODC on Money-Laundering and Countering the Financing of Terrorism-GPML Mandate’ <<https://www.unodc.org/documents/money-laundering/GPML-Mandate.pdf>> accessed at: 05.09.2020.

¹⁰⁷ Ibid.

¹⁰⁸UNODC, ‘Global Programme against Money Laundering’ <<https://www.unodc.org/pdf/gpml.pdf>> accessed at:05.09.2020.

¹⁰⁹ UNODC ‘United Nations Convention against Transnational Organized Crime and the Protocols Thereto’ <<https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html#Fulltext>> accessed at:05.09.2020.

The International Convention on the Suppression of the Financing of Terrorism came into force in April 2002, encouraging the member states to take measures to protect their financial systems from misuse by persons planning or engaging in terrorist activities.¹¹⁰

In 2009 UNODC published in collaboration with the Commonwealth Secretariat and the IMF, the Provisions of the Common Law Legal Systems Model Legislative Provisions on Money Laundering, Terrorism Financing, Preventive Measures and Proceeds of Crime model law and updated it in 2016.¹¹¹ Within the scope of this model law, money is defined in detail, and virtual money is described as a type of money with the feature of the medium of exchange.¹¹² In the process of updating the provisions of the model law, the FATF Guide on Virtual Currencies was published, and it was stated that the model law adopted these provisions and FATF's recommendations.¹¹³

UNODC started a training in 2017 to combat organised crime where cryptocurrency is being used. With this training, UNDOC emphasised the necessity of the member countries to adapt their efforts and capacities in accordance with the new types of crime emerging.¹¹⁴

4.2 Regulations of the European Union (EU)

The 'Directive on the Prevention of the Use of the Financial System for Money Laundering', numbered 91/308/EEC, which is the first binding regulation made to prevent the use of the financial system by launderers, entered into force on 10 June 1991 and it informed member states that their local legislation should regulate money laundering as a criminal offence.¹¹⁵ With the revision of the FATF recommendations in 1996, the directive 91/308 /EEC was

¹¹⁰ UNODC 'UN Instruments and Other Relevant International Standards on Money-Laundering and Terrorist Financing' <<https://www.unodc.org/unodc/en/money-laundering/Instruments-Standards.html?ref=menuside#UN-Conventions>> accessed at:06.09.2020.

¹¹¹ UNODC Commonwealth Sekretariat, 'Common Law Legal Systems Model Legislative Provisions on Money Laundering, Terrorism Financing, Preventive Measures and Proceeds of Crime' (2016) <https://www.imolin.org/pdf/Common_Law_Model_provisions_on_AMLCFT_and_Recovery_of_Procees_of_Crime.pdf> accessed at:06.09.2020.

¹¹² Ibid 4.

¹¹³ See (110).

¹¹⁴ UNODC, 'UNODC Launches Training to Tackle Cryptocurrency-Enabled Organized Crime' (2017) <<https://www.unodc.org/unodc/en/frontpage/2017/May/unodc-launches-training-to-tackle-money-laundering-and-bitcoin-banking-fraud.html>> accessed at: 07.09.2020.

¹¹⁵ Niels Vandezande, 'Virtual currencies under EU Anti-Money Laundering Law' (2017) 33 Computer Law & Security Review 341,343.

regulated, and the Directive 2001/97/EC was adopted on 19 November 2001. The main purpose of this regulation is to ensure full compliance with FATF recommendations.¹¹⁶

Directive 2005/60/EEC, also known as the third directive, entered into force on 26 October 2005 in order to comply with the nine special recommendations issued by FATF and to introduce measures against financing of terrorism and the previous regulations were repealed.¹¹⁷ In order to achieve more effective results in the fight against money laundering and financing of terrorism, 2015/849 ‘Anti-Money Laundering EU Directive No. 4’ was published in 2015. Within the scope of the Directive, new regulations were introduced to prevent money laundering and terrorist financing with the standards introduced in subjects such as detailed due diligence, risk-based approach, continuous monitoring of transactions and determination of the real beneficiary.¹¹⁸ In the first four regulations, virtual currencies and cryptocurrencies are not included.¹¹⁹

The Fifth Money Laundering Directive (5AMLD) entered into force in January 2020, aiming to strengthen the European Union's ongoing AML/CFT policies.¹²⁰ Unlike other regulations, 5AMLD contains important provisions, especially for virtual currencies. The definition of crypto money has been made and cryptocurrencies and cryptocurrency exchanges are considered as ‘obliged entities’, and it was accepted that they are subject to the AML/CFT provisions which specified in 4AMLD like other entities and actions.¹²¹ This includes an obligation to conduct customer due diligence (CDD) and submit suspicious activity reports (SAR). 5AMLD imposes reporting obligations by the Financial Intelligence Units (FIU) to obtain the addresses and identities of the owners of the virtual currency and in doing so to combat the anonymity associated with the use of the cryptocurrency.¹²² Under 5AMLD, cryptocurrency exchangers and wallet providers must now be registered with the authorities in their location like FCA.

4.3 Regulations of The Financial Action Task Force (FATF)

¹¹⁶ Ibid 344.

¹¹⁷ Ibid 347.

¹¹⁸ Ibid 348.

¹¹⁹ Ibid 349.

¹²⁰ 5th Anti Money Laundering Directive (5AMLD) 2018/843 <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018L0843>> accessed at:07.09.2020.

¹²¹ 5AMLD Sec 8.

¹²² 5AMLD Sec 9.

FATF was established by the G-7 countries within the OECD in 1989, with the aim of ensuring international cooperation to prevent money laundering and financing of terrorism.¹²³ Although it operates within the OECD, the FATF, which acts independently, has not been established for an unlimited period because it is an ‘action force’, and it required a specific decision of their Ministers for the work to continue. Thirty years after its creation, FATF Ministers adopted a new, open-ended mandate for the FATF in April 2019.¹²⁴ The implementation of the global anti-money laundering (AML) regime is mostly governed by the FATF. Due to the fact that it does not strictly enforce UN conventions on AML, the FATF has become the centre for the monitoring and review of countries and the implementation of recommendations.¹²⁵

Due to initiatives to strengthen the financial system against the risk of money laundering, FATF has published 40 recommendations in 1990 through this direction and made recommendations regarding the measures that can be taken within the scope of AML / CFT.¹²⁶

FATF 40 recommendations are mainly aimed at protecting the financial system against money laundering risks. As a result of the 40 Recommendations implemented in 1990, new methods and technological developments emerging in money laundering methods, it was revised in 1996 and additional measures were recommended, and with the September 11 attacks, the regulations for the financing of terrorism came to the agenda with the initiatives of the USA. In the FATF 40 recommendations, explanations regarding money laundering and financing of terrorism, precautions and co-operative suggestions were given. In 2001, 8 special recommendations were added to 40 to combat the financing of terrorism, and finally, with the revision made in 2003, these recommendations were implemented as 40 + 9 Recommendations issued by the FATF were accepted as the standard.¹²⁷ In particular, the UN has given serious support to the adoption of these resolutions by the member states and to develop their national

¹²³Anja P. Jakobi, ‘Governing Illicit Finance in Transnational Security Spaces: the FATF and Anti-Money Laundering’ (2018) 69 *Crime Law Soc Change* 173,176.

¹²⁴ FATF, ‘What do we do’ (2019) <<https://www.fatf-gafi.org/about/whatwedo/>> accessed at 07.09.2020

¹²⁵ Jakobi (n 121) 184.

¹²⁶FATF, ‘40 Recommendations’ (2004) <<https://www.fatf-gafi.org/publications/fatfrecommendations/documents/the40recommendationspublishedoctober2004.html>> accessed at: 07.09.2020.

¹²⁷ FATF, ‘IX Special Recommendations’ (2001) <<https://www.fatf-gafi.org/publications/fatfrecommendations/documents/ixspecialrecommendations.html>> accessed at: 07.09.2020.

legislation in this direction. FATF 40 + 9 recommendations are milestones in AML / CFT combat.

In the FATF supplementary recommendations, specific issues are emphasised. The first of the nine special recommendations issued by FATF involve the recognition and implementation of UN resolutions. The second recommendation acknowledges the purpose of financing terrorism as the premise of money laundering. The third recommendation includes the freezing and seizure of funds used for this purpose. The fourth recommendation recommends the detection of suspicious transactions and their reporting with international cooperation. The fifth recommendation aims to ensure that the judicial processes after determination continue with also international cooperation.¹²⁸ Recommendation number six deals with alternative remittance methods and according to the recommendation, countries should supervise bank and non-bank financial institutions and ensure control of money transfers. As per recommendation number seven, instead of anonymity, money transfers and track information such as name, address and the account number should be examined. Recommendation number eight aims to prevent money laundering and fraud, under the name NGO and number nine draws the attention of countries to the transfer of money or securities as a currency exchange by cash-carrying couriers from one country to another for money laundering purposes.¹²⁹ The sixth and seventh articles of these recommendations are incompatible with the peer-to-peer structure of virtual currencies and the freedom of anonymous transactions. Virtual currencies are also not subject to a central or state control, which makes it challenging to identify transfers made in this direction.

FATF issued a ‘Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services’ report in 2013 on new payment products and services (NPSS) and general information was given about the new online technology that has become widespread and the risks it carries.¹³⁰ In ‘Virtual Currencies: Key Definitions and Potential AML / CFT Risks’ Report issued by FATF in 2014, with the anonymity in virtual currency trading, limited identification and non-verification of participants, division of transactions into various countries, lack of control and a central oversight body combined with their global

¹²⁸ Ibid 2

¹²⁹ Ibid 3.

¹³⁰ FATF, ‘Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services Report’ (2013) <<https://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf>> accessed at: 08.09.2020.

access, it has been determined to virtual currencies pose a risk in money laundering and terrorist financing.¹³¹ In 2015, the FATF published the ‘Guidance for a Risk-Based Approach - Virtual Currencies’ Report, emphasising the role of cryptocurrencies in money laundering.¹³² In this report, the 2013 NPSS Report was referred, and the role of virtual currencies in money laundering was highlighted for the reasons stated in the previous report. Especially the global anonymity and lack of control, provided by virtual currencies, make it attractive for money laundering and the leading cases on this issue were examined in the report.

Increasing usage areas of virtual money, emerging new cases and risk dimension required changes in FATF 40 recommendations. Recommendations were revised in February 2018 (Recommendation 2) and June 2019 (Recommendation 15), and definitions of ‘virtual asset’ and ‘virtual asset service provider’ were added to the Recommendation 15.¹³³

Finally, ‘Guidance for a Risk-Based Approach: Virtual Assets and Virtual Asset Service Providers’ Report and ‘International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation’ Guidance was issued in 2019. These regulations will help countries and virtual asset service providers understand their anti-money laundering and counter-terrorism financing obligations and effectively enforce FATF requirements and with the latest regulations, serious attention has been drawn to virtual currencies.

4.4 Regulations of International Monetary Fund (IMF)

The International Monetary Fund (IMF) was established in 1945, to follow global financial markets, increase cooperation, ensure financial stability and promote economic growth. In addition, it carries out various activities in order to provide the stable progress of financial markets and to prevent abuses, money laundering and financing of terrorism in member countries.¹³⁴ In addition to the regulations made to combat money laundering, regulations were

¹³¹ FATF, ‘Virtual Currencies: Key Definitions and Potential AML / CFT Risks Report’ (2014) <<https://www.fatf-gafi.org/documents/documents/virtual-currency-definitions-aml-cft-risk.html>> reached at: 08.09.2020.

¹³² FATF, ‘Guidance for a Risk Based Approach - Virtual Currencies Report’ (2015) <<https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf>> accessed at: 08.09.2020.

¹³³FATF, ‘International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation Recommendations’ (2019) < <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html>> accessed at: 08.09.2020.

¹³⁴ IMF, ‘The IMF at a Glance’ <<https://www.imf.org/en/About>> accessed at: 08.09.2020.

put into effect because of the September 11 attacks, including the financing of terrorism. In this context, 40 + 9 Recommendations published by FATF in July 2002 were accepted as international standards by the IMF.¹³⁵

In order to develop programs on money and terrorism financing within the framework of financial integrity, the IMF agreed in 2002 to make this field a regular part of the activities and the World Bank decided to cooperate in this field.¹³⁶ Within the scope of joint pilot studies, it was decided to carry out studies to improve the institutional capacity by improving the dialogue, developing methodology in the assessment of the fight against international money laundering and terrorism financing, and intensifying the training activities.¹³⁷

In January 2016, a comprehensive IMF Staff Discussion Note on the role of virtual currencies in money laundering was published, and it was stated that the international nature of virtual currencies made risk tracking difficult.¹³⁸ As experience is gained in this field, it is aimed to develop international standards and practices, provide guidance on the most appropriate regulatory responses and thus promote harmony between jurisdictions.¹³⁹

In the speech delivered by IMF Managing Director Christine Lagarde at the FATF Plenary Meeting, the satisfaction of the FATF and IMF cooperation on money laundering was emphasised and it was stated that financial technology (FinTech) should be used wisely in terms of money laundering and terrorist financing.¹⁴⁰ It has been noted that the distributed ledger system owned by virtual currencies as a FinTech asset, is more powerful against cyber attacks due to keeping transaction records and copies. It was also stated in this speech that AML / CFT assistance was provided to 120 countries by the IMF.

¹³⁵ IMF, 'Revisions to the Financial Action Task Force (FATF) Standard—Information Note to the Executive Board' (2012)

<<https://www.imf.org/en/Publications/Policy-Papers/Issues/2016/12/31/Revisions-to-the-Financial-Action-Task-Force-FATF-Standard-Information-Note-to-the-PP4683>> accessed at: 09.09.2020.

¹³⁶ IMF, 'Anti-Money Laundering and Combating the Financing of Terrorism: Review of the Quality and Consistency of Assessment Reports and the Effectiveness of Coordination' (2006) 55
<<https://www.imf.org/external/np/pp/eng/2006/041806r.pdf>> accessed at: 09.09.2020.

¹³⁷ Ibid 9

¹³⁸ IMF, 'Virtual Currencies and Beyond: Initial Considerations IMF Staff Discussion Note' (2016)
<<https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf>> accessed at: 09.09.2020.

¹³⁹ Ibid.

¹⁴⁰ Christine Lagarde, 'Working Together to Fight Money Laundering & Terrorist Financing' (2017)
<<https://www.imf.org/en/News/Articles/2017/06/21/sp062217-working-together-to-fight-money-laundering-terrorist-financing>> accessed at: 10.09.2020.

Regulation of Crypto Assets FinTech Note was published by IMF in December 2019, drawing attention to crypto-asset risks. It has been stated that the anonymity in virtual currencies makes it difficult to monitor the virtual currencies as a crypto crime tool and it makes cooperation difficult due to the unequal tracking methods between the jurisdictions of these entities, which fall under different regulations globally.¹⁴¹ Although the financial sector regulators have taken a position on cryptocurrencies, regulations and practices differ between countries due to the lack of a single global legal standard in this regard.¹⁴² The FinTech Notes encourages the determination of a worldwide standard for the detection and sanctions of the said cryptocurrencies in money laundering.

4.5 Regulations of the UK

The Crypto-assets Taskforce, consisting of HM Treasury, the Financial Conduct Authority and the Bank of England, was established in 2018 due to the increasing use and tracking of virtual currencies.¹⁴³ Representatives of crypto-assets and distributed accounting and ledger technology firms, banks, industrial service firms and academicians attended the roundtable meeting held in the same year, and the Final Report was prepared at the end of this meeting. In the report, Task Force found that while virtual currency activity in the UK has increased in recent years, the overall size of the UK market represents a small percentage of the overall global crypto asset market and all three institutions supported that this market should be developed in a controlled manner. The Task Force raises the need to provide firms with extra clarity on where current crypto asset activities are regulated and investigate whether unregulated activities need to be regulated in the future.¹⁴⁴ The report states that smart contracts using distributed ledger technology (DLT) can pose a challenge in terms of civil law and the General Data Protection Regulation (GDPR). Since the erasure right in GDPR is not in DLT transactions, it is recommended to develop specific DLT solutions that comply with GDPR requirements and also to comply with the Data Protection Act 2018.¹⁴⁵

¹⁴¹ Cristina Cuervo, Anastasiia Morozova, and Nobuyasu Sugimoto, 'Regulation of Crypto Assets- FinTech Notes - International Monetary Fund' (2019) 19/03 LCC HG1710.C84, 1, 6.

¹⁴² Ibid 16.

¹⁴³ HM Treasury, 'Cryptoassets Taskforce: Final Report' (2018)

<https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752070/cryptoassets_taskforce_final_report_final_web.pdf > accessed at:10.09.2020.

¹⁴⁴ Ibid 16.

¹⁴⁵ Ibid 28.

In the Guidance on ‘Crypto-assets Consultation Paper’ published in January 2019, FCA also aims for market participants to understand whether the crypto assets they use are within regulatory limits. With the guide, market participants are alerted to the problems and they know what rules or regulations they are subject to.¹⁴⁶

On January 10, 2020, the UK's money laundering laws were regulated, and with this amendment, EU's Fifth Money Laundering Directive (5MLD) and FATF's 40+9 Principles were applied to domestic law with ‘The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations of 2017’. This amendment also includes money laundering with crypto assets.¹⁴⁷

In UK laws, the concept of ‘crypto-asset’ is used to cover all virtual money and is defined as ‘a cryptographically secured digital representation of value or contractual rights that uses a form of distributed ledger technology (DLT) and can be transferred, stored or traded electronically’.¹⁴⁸

The UK left the European Union as of January 31 2020 and the Withdrawal Agreement (EUWA) signed with the EU envisages a process that extends to 31.12.2020. At the end of the interim period, EUWA ensures that the EU Financial Services Legislation applicable at the time has been incorporated into UK domestic law.¹⁴⁹

CONCLUSION

In recent years, cybercrime has made a significant leap forward as the main threat to the security of states, and the amount of money laundered by partnerships between organized crime and cybercrime has reached an unpredictable volume. In this way, criminals pay cybercriminals to divert proceeds of crime from their source, and cyber criminals gain new financial benefits

¹⁴⁶ FCA, ‘Guidance on Crypto Assets-Consultation Paper’ (2019) 4
<<https://www.fca.org.uk/publication/consultation/cp19-03.pdf>> accessed at: 10.09.2020.

¹⁴⁷ HM Revenue & Customs, ‘Money Laundering and Terrorist Financing (Amendment) Regulations 2019’ (2020) <<https://www.gov.uk/government/publications/money-laundering-and-terrorist-financing-amendment-regulations-2019/money-laundering-and-terrorist-financing-amendment-regulations-2019>> accessed at: 10.09.2020

¹⁴⁸ Laura Douglas, ‘United Kingdom’ in Michael S Sackheim and Nathan A. Howell (eds) *The Virtual Currency Regulation Law Review* (3rd Edn, Tom Barnes, 2020) 344.

¹⁴⁹ *Ibid* 323.

by combining their criminal activities with major crime cartels and it also offers criminals the opportunity to money laundering on their own, without the need for such cooperation.

In terms of virtual currencies such as Linden Dollars, which are used only in the purchase and sale of virtual goods and services, there is a need for regulations in terms of the protection of consumers instead of leaving virtual currency users to their fate and the law to be applied in virtual environments where these currencies are used. Because, as in the Second Life example, there is not only a game but a market where very serious monetary sums are in question. Therefore, as in real life, the need to protect consumers, money laundering, fraud crimes may be in question.

Cryptocurrencies have rapidly become prominent among virtual currencies, whose usage area is increasingly widespread and market value is increasing, offer the advantage of fast and low-cost anonymous transfer service. Due to its decentralized nature, transactions cannot be recorded and it is also impossible to track and trace transactions performed with alpha-numeric codes. Therefore, launderers, drug dealers, arms smugglers and terrorist-financing groups, who care about privacy and avoid pursuing by legal authorities, prefer the cryptocurrency market.

The other main factor in the use of cryptocurrencies in money laundering is that they are outside the legal regulations and controls imposed on the traditional financial system. It would be a more constructive approach to integrate and control this market into the financial system instead of struggling with these currencies due to the potential risks that these currencies carry.

Due to the widespread use of cryptocurrencies, no country has the power to ban cryptocurrencies. Even if its use and access are prohibited by law, it will not be possible in action to block access to websites that offer cryptocurrency trading with special tools such as Deep Web and VPN. In this context, determining the boundaries of institutions that mediate cryptocurrency trading by law and introducing a licensing model for these institutions in the capital markets may be important steps.

Regulatory financial institutions employ qualified personnel who can fulfil the requirements of the business in order to establish the necessary tools and control these transactions to distinguish between normal customer behaviour and suspicious transactions. Since the institutions that mediate cryptocurrency trading are not subject to central legal regulations and supervision, it is not possible to regularly and systematically monitor the transactions carried

out through these institutions. This situation prevents the detection and reporting of suspicious transactions.

Legal regulations to be made in this area can allow the crypto money market to be taken under control and to reduce the risks of money laundering. Detection of many crimes is not possible due to the different legal regulations of the countries. In order to ensure cooperation in this field, the directives and recommendations of the regulatory institutions should be integrated into the domestic law of the states and implemented meticulously. As the international regulatory bodies have stated, cooperation is the most important key in combating this crime.



BIBLIOGRAPHY

Articles

Ammous S, 'Can Cryptocurrencies Fulfil the Functions of Money?' (2018) 70 The Quarterly Review of Economics and Finance

Bariviera AF, Basgall MJ, Hasperue W, 'Some Stylized Facts of the Bitcoin Market' (2017) 484 Physica A

Berentsen A, 'Monetary Policy Implications of Digital Money' (1998) 51 KYKLOS

Ciancaglini V, Balduzzi M, McArdle R, and Rösler M, 'Below the Surface: Exploring the Deep Web' (2015) Trend Micro

Cuervo C, Morozova A, and Sugimoto N, 'Regulation of Crypto Assets- FinTech Notes (International Monetary Fund)' (2019) International Monetary Fund, LCC HG1710.C84

Elliott J, 'Help – Somebody Robbed my Second Life Avatar!' (2008) 1(1) Virtual Worlds Research: Past, Present & Future

Fromkin A, 'Flood Control on the Information Ocean: Living With Anonymity, Digital Cash, and Distributed Databases' (1996) 15 Pittsburgh Journal of Law and Commerce

Goldberg D, Famous Myths of 'Fiat Money' (2005) 37(5) Journal of Money, Credit and Banking

Halaburda H, 'Digital Currencies: Beyond Bitcoin' (2016) 103(3) Digiworld Economic Journal

Hameed S and Farooq S, 'The Art of Crypto Currencies: A Comprehensive Analysis of Popular Crypto Currencies' (2016) 7(12) International Journal of Advanced Computer Science and Applications (IJACSA)

Hawkins B, 'Under the Ocean of the Internet - The Deep Web' (2016) SANS Institute

Information Security Reading Room

Jakobi AP, 'Governing Illicit Finance in Transnational Security Spaces: the FATF and Anti-Money Laundering' (2018) 69 Crime Law Soc Change <https://doi.org/10.1007/s10611-017-9750-y>

Kemp K and Buckley RP, 'Resolution Powers over E-Money Providers' (2017) 40 UNSWLJ

Klein T, Thu H, Walther T, 'Bitcoin is not the New Gold – A Comparison of Volatility, Correlation, and Portfolio Performance' (2018) 59 International Review of Financial Analysis

Naheem M, 'Exploring the Links Between AML, Digital Currencies and Blockchain Technology' (2019) 22 (3) Journal of Money Laundering Control

Rotman S, 'Bitcoin versus Electronic Money' (2014) CGAP Report No: 88164, 1-4

Sauer B, 'Virtual Currencies, the Money Market, and Monetary Policy' (2016) 22 Int Adv Econ Res DOI: 10.1007/s11294-016-9576-x

Schneider F & Windischbauer U, 'Money Laundering: Some Facts' (2008) 26 Eur J Law Econ DOI 10.1007/s10657-008-9070-x 387–404

Simser J, 'Money Laundering: Emerging Threats and Trends' (2012) 16(1) Journal of Money Laundering Control

Sugiura N, 'Electric Money and the Law: Legal Realities and Future Challenges' (2009) 18(3) Pacific Rim Law & Policy Journal Association

Stokes R, 'Virtual Money Laundering: the Case of Bitcoin and the Linden Dollar' (2012) 21(3) Information & Communications Technology Law Journal DOI: 10.1080/13600834.2012.744225

Teichmann FMJ, 'Twelve Methods of Money Laundering' (2017) 20(2) Journal of Money Laundering Control

Teichmann, FMJ, 'Recent Trends in Money Laundering' (2020) 73 Crime Law Soc Change, <https://doi-org.ezproxy.sussex.ac.uk/10.1007/s10611-019-09859-0>

Tschorsch F & Scheuermann B, 'Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies' (2016) 18(3) IEEE Communications, Surveys & Tutorials

Weber B, 'Competing for Legitimacy: A Typology of Virtual Currencies' (2016) Preliminary draft prepared for the 2nd International Workshop on P2P Financial Systems

Vandezande N, 'Virtual currencies under EU Anti-Money Laundering Law' (2017) 33 Computer Law & Security Review

Yavuz MS, 'Ekonomide Dijital Dönüşüm: Blockchain Teknolojisi ve Uygulama Alanları Üzerine Bir İnceleme' [Digital Transformation In Economy: A Review of Blockchain Technology and Application Areas] (2019) 4(1) Research of Financial Economic and Social Studies (RFES)

Books

Campbell-Verduyn, M. (Ed.) *'Bitcoin and Beyond: Cryptocurrencies, Blockchains, and Global Governance'* RIPE Series in Global Political Economy (2018) ISBN 978-1-315-21190-9, Routledge, Taylor & Francis Group, London <https://doi-org.ezproxy.sussex.ac.uk/10.4324/9781315211909>

Chuen DLK and Deng R, (Eds.) *'Handbook of Blockchain'* Digital Finance and Inclusion (Cryptocurrency, FinTech, InsurTech and Regulation) (2017) ISBN:978-0-12-810441-5 <https://doi.org/10.1016/C2015-0-04334-9>

Connolly M, *'International Business Finance'* Taylor & Francis e-Library -Routledge (2006)

Douglas L, 'United Kingdom' in Michael S Sackheim and Nathan A Howell (eds) *The Virtual Currency Regulation Law Review* (3rd Edn, Tom Barnes, 2020)

Jones C, King C, Walker C, & Gurulé J (Eds.) 'Money Laundering in a Virtual World' *The Palgrave Handbook of Criminal and Terrorism Financing Law* (Palgrave Macmillan, 2018) https://doi.org/10.1007/978-3-319-64498-1_8

Low KFK and Teo E, 'Chapter 10-Legal Risks of Owning Cryptocurrencies' *Handbook of Blockchain: Digital Finance and Inclusion (Cryptocurrency, FinTech, InsurTech and Regulation)* (Nikki Levy, 2017))

Web Sites

European Central Bank 'Report on Electronic Money' (1998)

<<https://www.ecb.europa.eu/pub/pdf/other/emoneyen.pdf>> accessed at: 03.08.2020

European Central Bank, 'Virtual Currency Schemes – a Further Analysis' (2015)

<<https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf>> accessed at:10.08.2020

'Top 100 Coins by Market Capitalization' <<https://coinmarketcap.com/coins/>>

accessed at: 10.08.2020

FATF, 'Money Laundering Through the Physical Transportation of Cash' (2015)

<<https://www.fatf-gafi.org/media/fatf/documents/reports/money-laundering-through-transportation-cash.pdf>> accessed at: 20.08.2020

FATF 'APG Typology Report on Trade Based Money Laundering' (2012)

<https://www.fatfgafi.org/media/fatf/documents/reports/Trade_Based_ML_APGReport.pdf> accessed at: 30.08.2020

'Professional Money Laundering FATF Report' (2018)

<<http://www.fatf-gafi.org/media/fatf/documents/ProfessionalMoneyLaundering.pdf>>

accessed at: 31.08.2020

Currency Rate: USD to LDN <<https://usd.currencyrate.today/ld>> accessed at:

01.09.2020

Sykes JB and Vanatko N, 'Virtual Currencies and Money Laundering: Legal Background, Enforcement Actions, and Legislative Proposals' (2019) Congressional Research Service Report <<https://fas.org/sgp/crs/misc/R45664.pdf>> accessed at:

01.09.2020

European Central Bank 'Virtual Currency Schemes' (2012)

<<https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>>

accessed at: 01.09.2020

FinCen 'Application of FinCEN's Regulations to Persons Administering, Exchanging or Using Virtual Currencies' (2013)

<<https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf>> accessed at:

03.09.2020

Sarinen J, 'Virtual World Second Life to Enforce Anti-Money Laundering Regs' (2019) <<https://www.itnews.com.au/news/virtual-world-second-life-to-enforce-anti-money-laundering-regs-527558>>

accessed at: 03.09.2020

Bitcoin, 'How does Bitcoin Work?' <<https://bitcoin.org/en/how-it-works>> accessed at:

03.09.2020

Schwartz D, Youngs N, Britto A, 'The Ripple Protocol Consensus Algorithm' (2018)

<https://ripple.com/files/ripple_consensus_whitepaper.pdf> accessed at: 04.09.2020

Santos D, 'What the Dark Web Is and Isn't' (2017)

<<https://www.smartdatacollective.com/what-dark-web-and-isn-t/>> accessed at:

04.09.2020

Treacher M, 'Announcing Ripple's Global Payments Steering Group' (2016)
<<https://ripple.com/insights/announcing-ripples-global-payments-steering-group/>>
accessed at: 04.09.2020

Bergman M, 'White Paper: The Deep Web: Surfacing Hidden Value' (2001) 7(1) The Journal of Electronic Publishing
<<https://quod.lib.umich.edu/jjep/3336451.0007.104?view=text;rgn=main>> accessed at: 04.09.2020

Tor, 'About: History' <<https://www.torproject.org/about/history/>> accessed at: 04.09.2020

Greenberg A, 'FBI Says It's Seized \$28.5 Million In Bitcoins From Ross Ulbricht, Alleged Owner Of Silk Road' (2013)
<<https://www.forbes.com/sites/andygreenberg/2013/10/25/fbi-says-its-seized-20-million-in-bitcoins-from-ross-ulbricht-alleged-owner-of-silk-road/#2f4ff5ec2765>>
accessed at: 05.09.2020

US Department of Justice, 'Liberty Reserve Founder Sentenced to 20 Years For Laundering Hundreds of Millions of Dollars' (2016)
<<https://www.justice.gov/opa/pr/liberty-reserve-founder-sentenced-20-years-laundering-hundreds-millions-dollars>> accessed at: 05.09.2020

FATF 'Virtual Currencies: Key Definitions and Potential AML/CFT Risks' (2014)
<<https://www.fatf-gafi.org/documents/documents/virtual-currency-definitions-aml-cft-risk.html>> accessed at: 05.09.2020

UNODC, 'UNODC on Money-Laundering and Countering the Financing of Terrorism-GPML Mandate' <<https://www.unodc.org/documents/money-laundering/GPML-Mandate.pdf>> accessed at: 05.09.2020

UNODC, 'Global Programme Against Money Laundering' <<https://www.unodc.org/pdf/gpml.pdf>> accessed at: 05.09.2020

‘United Nations Convention against Transnational Organized Crime and the Protocols Thereto’ <<https://www.unodc.org/unodc/en/organizedcrime/intro/UNTOC.html#Fulltext>> accessed at: 05.09.2020

‘UN Instruments and Other Relevant International Standards on Money-Laundering and Terrorist Financing’ <<https://www.unodc.org/unodc/en/money-laundering/Instruments-Standards.html?ref=menuseide#UN-Conventions>> accessed at: 06.09.2020

UN Commonwealth Secretariat, ‘Common Law Legal Systems Model Legislative Provisions on Money Laundering, Terrorism Financing, Preventive Measures and Proceeds of Crime’ (2016) <https://www.imolin.org/pdf/Common_Law_Model_provisions_on_AMLCFT_and_Recovery_of_Proceeds_of_Crime.pdf> accessed at: 06.09.2020

‘UNODC Launches Training to Tackle Cryptocurrency-Enabled Organized Crime’ (2017) <<https://www.unodc.org/unodc/en/frontpage/2017/May/unodc-launches-training-to-tackle-money-laundering-and-bitcoin-banking-fraud.html>> accessed at: 07.09.2020

EU, 5th Anti Money Laundering Directive (5AMLD) 2018/843 <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018L0843>> accessed at: 07.09.2020

FATF, ‘What do we do?’ (2019) <<https://www.fatf-gafi.org/about/whatwedo/>> accessed at: 07.09.2020

FATF, ‘40 Recommendations’ (2004) <<https://www.fatfgafi.org/publications/fatfrecommendations/documents/the40recommendationspublishedoctober2004.html>> accessed at: 07.09.2020

FATF, ‘IX Special Recommendations’ (2001) <<https://www.fatf->

[gafi.org/publications/fatfrecommendations/documents/ixspecialrecommendations.html](https://www.fatf-gafi.org/publications/fatfrecommendations/documents/ixspecialrecommendations.html)> accessed at: 07.09.2020

FATF, 'Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services Report' (2013) <<https://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf>> accessed at: 08.09.2020

FATF, 'Guidance for a Risk Based Approach - Virtual Currencies Report' (2015) <<https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf>> accessed at: 08.09.2020

FATF, 'International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation Recommendations' (2019) <<https://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html>> accessed at: 08.09.2020

IMF, 'The IMF at a Glance' <<https://www.imf.org/en/About>> accessed at: 08.09.2020

IMF, 'Revisions to the Financial Action Task Force (FATF) Standard—Information Note to the Executive Board' (2012) <<https://www.imf.org/en/Publications/Policy-Papers/Issues/2016/12/31/Revisions-to-the-Financial-Action-Task-Force-FATF-Standard-Information-Note-to-the-PP4683>> accessed at: 09.09.2020

IMF, 'Anti-Money Laundering and Combating the Financing of Terrorism: Review of the Quality and Consistency of Assessment Reports and the Effectiveness of Coordination' (2006) <<https://www.imf.org/external/np/pp/eng/2006/041806r.pdf>> accessed at: 09.09.2020

IMF, 'Virtual Currencies and Beyond:Initial Considerations IMF Staff Discussion Note' (2016) <<https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf>> accessed at: 09.09.2020

Christine Lagarde, 'Working Together to Fight Money Laundering & Terrorist Financing' (2017) <<https://www.imf.org/en/News/Articles/2017/06/21/sp062217->

[working-together-to-fight-money-laundering-terrorist-financing](#)> accessed at:
10.09.2020

HM Treasury, 'Cryptoassets Taskforce: Final Report' (2018)
<https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752070/cryptoassets_taskforce_final_report_final_web.pdf> accessed
at:10.09.2020

FCA, 'Guidance on Crypto Assets-Consultation Paper' (2019) 4
<<https://www.fca.org.uk/publication/consultation/cp19-03.pdf>> accessed at:
10.09.2020

HM Revenue & Customs, 'Money Laundering and Terrorist Financing (Amendment) Regulations 2019' (2020)< <https://www.gov.uk/government/publications/money-laundering-and-terrorist-financing-amendment-regulations-2019/money-laundering-and-terrorist-financing-amendment-regulations-2019>> accessed at:10.09.2020