UNODC
United Nations Office on Drugs and Crime

Basic Manual on the Detection And Investigation of the Laundering of Crime Proceeds Using Virtual Currencies

June 2014

This publication was produced with the financial support of the U.S. Department of State, Bureau for International Narcotics and Law Enforcement Affairs. Opinions, conclusions and recommendations expressed in the publication belong to the author(s) and do not necessarily reflect the view of the Department of State.

* * *

This publication has not been formally edited. Cover photo: Antoaneta Petrova.

1 Introduction

As a custodian of the UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, the UN Convention against Transnational Organized Crime and the UN Convention against Corruption, UNODC possesses significant comparative advantages for delivering assistance in the anti money-laundering and asset forfeiture areas. The UNODC mandate in these areas was strengthened by ECOSOC resolution 2004/29, which specifically states that UNODC should "continue its work against money-laundering, subject to the availability of extra budgetary resources and in cooperation with relevant regional and international organizations participating in activities designed to give effect to applicable international instruments and relevant standards for combating money-laundering, through the provision to Member States, upon request, of training, advisory assistance and long term technical assistance".

In 2012, at the request of the GUAM Secretariat, and with the financial support of the Bureau for International Law Enforcement and Narcotics Affairs of the US Department of State, the UNODC Regional Office for Central Asia launched the project "Strengthening capacities of the GUAM Member States to cooperate at the national and regional levels in combating money-laundering as well as in seizing and confiscating crime proceeds". The project seeks to promote a regional approach to counter money-laundering in the GUAM Member States (Georgia, Ukraine, Azerbaijan and Moldova) and, at the same time, to strengthen inter-agency cooperation of these States at the national levels.

The purpose of this manual, which has been drafted in the framework of the above mentioned project, is to provide practical information for investigators and prosecutors on the detection, investigation, prosecution and seizure of crime proceeds laundered through the use of virtual currencies.

2 Acknowledgements

The authors would like to thank all of those who provided input, advice and feedback on the content of the manual.

The manual has been drafted under the technical guidance of the UNODC Global Programme against Money Laundering, Proceeds of Crime and the Financing of Terrorism (GPML) and Global Programme on Cybercrime.

Expert contributions were provided by the UNODC consultants Messrs. David O'Reilly, Giorgi Jokhadze and Yevheniy Umanets.

Contributions were also provided by representatives from the GUAM states.

3 Table of Contents

Basic Manual on the Detection And Investigation of the Laundering of Crime Proceeds Using Virtual Currencies

Module 1
Introduction to Virtual Currencies

1 Summary

The purpose of this module is to provide a general overview of the history and concepts of electronic money and virtual currencies. The information contained in this module is important background material that forms the basis and context for the modules that follow.

To understand the genesis of virtual currencies, a brief history of virtual currencies is provided, including some of the most famous examples of virtual currencies and virtual currency exchanges. This is followed by definitions of the key terms that will be used throughout these modules, as well as relevant legal definitions. Providing clear definitions helps to refine the scope of the discussion, as well as preventing miscommunication and confusion. A description of some of the more common types of electronic money and virtual currencies is then provided, including a categorisation model for virtual currencies.

It is very important from an investigative point of view to understand the interfaces between electronic money, virtual currencies and the traditional financial system. Some of the most common interfaces are discussed and finally, the current state of legal regulation of virtual currencies is provided. Several case studies of virtual currencies are included, with particular attention paid to the Bitcoin network, considering its topical nature and the particular challenges raised by this technology.

2 Learning Objectives

By the end of this module you will:

- Know the key terms in the area of electronic money and virtual currencies.
- Be aware of the main types of electronic money and virtual currencies.
- Understand the interface between virtual currencies and the traditional financial system.
- Know the current state of legal regulation of electronic money and virtual currencies.
- Know what bitcoins are and how they work, as an example of a cryptocurrency.

3 History of Virtual Currencies

Virtual currencies are not a new concept, with multiple virtual currencies having come and gone over the past decade. This section provides a brief summary of some of the most famous virtual currencies and currency exchanges.

One of the first popular virtual currencies was E-Gold. First established in 1996[1], E-Gold allowed users to open an account with a value denominated in grams of gold (or other precious metals) and the ability to make instant transfers of value to other E-Gold accounts. It was reported that in 2005 E-Gold had 2.5 million account holders, performing daily transactions with a typical value of US$6.3 million. In 2007, E-Gold was indicted by a grand jury in the US, accusing the company of money-laundering, conspiracy and operating an unlicensed money transmitting business, ultimately leading to the shut down of E-Gold by the US courts[2, 3]. E-Gold spawned a range of imitators such as e-Bullion.com, Pecunix.com and others.

In 1998, WebMoney was established and continues to experience significant growth, with almost 25 million users at the time of writing[4]. The WebMoney system is based on providing its users with the ability to control individual property rights for valuables (assets) stored by other participants of the system (known as Guarantors)[5].

Liberty Reserve, established in 2006, and operating until 2013, allowed users to register and transfer money to other users with only a name, email address and date of birth. No efforts were made to verify the identities of its users. In 2013 the US Department of Justice charged Liberty Reserve with operating an unregistered money transmitter business and money-laundering for facilitating the movement of more than $6 billion in illicit proceeds[6].

---

[1] "Feds accuse E-Gold of helping cybercrooks", NBC News, May 2007. (Source: http://redtape.nbcnews.com/_news/2007/05/02/6346006-feds-accuse-e-gold-of-helping-cybercrooks)

[2] "Internet currency firm pleads guilty to money laundering", The Industry Standard, July 2008. (Source: http://web.archive.org/web/20090414185759/http://www.thestandard.com/news/2008/07/22/internet-currency-firm-pleads-guilty-money-laundering)

[3] http://en.wikipedia.org/wiki/E-gold

[4] http://www.wmtransfer.com/eng/about/statistics/index.shtml, WebMoney statistics retrieved April 2014.

[5] http://en.wikipedia.org/wiki/WebMoney

[6] "'Black Market Bank' Accused of Laundering $6B in Criminal Proceeds", ABC News, May 2013. (Source: http://abcnews.go.com/US/black-market-bank-accused-laundering-6b-criminal-proceeds/story?id=19275887)

Bitcoin is a decentralised, peer-to-peer payment network that is powered by its users with no central authority or middlemen. Satoshi Nakamoto published the first Bitcoin specification and proof of concept to a cryptography mailing list in 2009[7]. Since that time, the value of bitcoins has fluctuated wildly, ranging from approximately US$0.30 in 2011 to US$1135 in 2013[8]. The operation of the Bitcoin network is discussed in detail in the Bitcoin case study below.

[7] https://bitcoin.org/en/faq
[8] http://bitcoincharts.com/

4 Definition of Terms

The definition of terms is important to prevent duplication of effort and unintended confusion. This is particularly relevant in the area of virtual currencies where numerous related definitions exist for commonly used terms such as electronic money[9], virtual currency[10], [11], [12], [13], [14], [15] and cryptocurrency[16]. These definitions, sometimes overlapping or inconsistent, vary in both substance and focus. Indeed, whether virtual and electronic currencies meet the definition of a currency or should be considered as a commodity is also currently under debate[17], [18], [19].

For the purposes of this document, the definitions of terms and classification of virtual currencies proposed by the FATF will be used[20]. These definitions are provided in the following sections.

4.1 FATF Definitions

4.1.1 Virtual Currency

"A virtual currency is a digital representation of value that can be digitally traded and functions as (1) a medium of exchange; (2) a unit of account; and/or (3) a store of value, but does not have legal tender status in any jurisdiction."

[9] http://ec.europa.eu/internal_market/payments/emoney/index_en.htm
[10] http://en.wikipedia.org/wiki/Virtual_currency
[11] "Guidance: Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies", FinCEN Guidance note FIN-2013-G001, March 2013. (Source: http://www.fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html)
[12] "EBA warns consumers on virtual currencies", European Banking Authority, December 2013. (Source: http://www.eba.europa.eu/-/eba-warns-consumers-on-virtual-currencies)
[13] "Virtual Currency Schemes", European Central Bank, October 2012. (Source: http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf)
[14] "Virtual Economies and Currencies – Additional IRS Guidance Could Reduce Tax Compliance Risks", United States Government Accountability Office, May 2013. (Source: http://www.gao.gov/assets/660/654620.pdf)
[15] "Redefining Virtual Currency", Yankee Group, May 2013. (Source: http://info.tapjoy.com/wp-content/uploads/sites/4/2013/05/RedefiningVirtualCurrency_WhitePaper-1MAY2013-v1.pdf)
[16] http://www.investopedia.com/terms/c/cryptocurrency.asp
[17] "Bitcoin Judged Commodity in Finland After Failing Money Test", Bloomberg, Jan 2014. (Source: http://www.bloomberg.com/news/2014-01-19/bitcoin-becomes-commodity-in-finland-after-failing-currency-test.html)
[18] IRS Notice 2014-21. (Source: http://www.irs.gov/pub/irs-drop/n-14-21.pdf)
[19] "Bitcoin Turns Into Art as Sweden Rejects Creative Currency", Bloomberg, Jan 2014. (Source: http://www.bloomberg.com/news/2014-01-21/bitcoin-becomes-art-as-swedish-taxman-rejects-creative-currency.html)
[20] FATF Report "Virtual Currencies – Key Definitions And Potential AML/CFT Risks" FATF, June 2014. (Source: http://www.fatf-gafi.org/topics/methodsandtrends/documents/virtual-currency-definitions-aml-cft-risk.html)

For the purposes of this definition, a "digital representation" is a representation of something in the form of digital data. A physical object, such as a flash drive or a bitcoin, may contain a digital representation of virtual currency, but ultimately, the currency only functions as such if it is linked digitally, via the Internet, to the virtual currency system.

The critical point of note in the use of the term "digital representation" is the fact that it is the digital data itself that is the virtual currency, not the medium on which the digital data is stored. Digital representations of virtual currency can be moved, copied or transferred to another storage medium, but the value of the virtual currency remains inherent in the digital representation.

Virtual currency is distinguished from fiat currency (a.k.a. "real currency", "real money" or "national currency"), which is the coin and paper money of a country that is designated as its legal tender; circulates; and is customarily used and accepted as a medium of exchange in the issuing country.

4.1.2 Electronic Money/e-money

"It [virtual currency] is distinct from e-money, which is a digital representation of fiat currency used to electronically transfer value denominated in fiat currency. E-money is a digital transfer mechanism for fiat currency – i.e., it electronically transfers value that has legal tender status."

Virtual currencies are defined as not having legal tender status in any jurisdiction. It is possible, both hypothetically and practically, to create a digital representation of fiat currency. This is, by definition not virtual currency, so a different term, electronic money, is used to refer to digital representations of fiat currency.

4.1.3 Digital Currency

"Digital currency can mean a digital representation of either virtual currency (non-fiat) or e-money (fiat)..."

Unique challenges arise when a digital representation of value is used. Some are specific to virtual currencies and some are specific to electronic money. In the case of virtual currencies, for example, topics relating to the conversion of fiat currency to virtual currency arise. These are less of an issue for electronic money, which is already a direct representation of fiat currency.

However, it can sometimes be useful to refer to digital representations of value, irrespective of whether the value represents legal tender in a particular jurisdiction or not. For example, in either case the problem of "double spending" needs to be addressed. Double spending is a situation where a digital

representation of value is spent more than once. Obviously this is a serious problem in any value transfer system and is not dependent on whether the digital data represents fiat or non-fiat currency.

The term digital currency encompasses both of the above definitions, and provides a term by which it is possible to refer to digital representations of both fiat and non-fiat currencies.

5 Classifying Virtual Currencies

The classification of virtual currencies that follows is drawn from the work of the FATF[21]. They propose that virtual currencies be classified according to:

1. Whether they can be converted back and forth for fiat currency or not (Convertible or non-convertible).

2. Whether there is a single administrating authority for the virtual currency or not (centralised or distributed).

The definitions of these categories, and some further discussion can be found in the following sections. Other classifications are, of course, also possible[22].

5.1 Convertible vs. Non-convertible Virtual Currency

"Convertible (or open) virtual currency has an equivalent value in real currency and can be exchanged back-and-forth for real currency. Examples include: Bitcoin; e-Gold (defunct); Liberty Reserve (defunct); Second Life Linden Dollars; and WebMoney."

"Non-convertible (or closed) virtual currency is intended to be specific to a particular virtual domain or world, such as a Massively Multiplayer Online Role-Playing Game (MMORPG) or Amazon, and under the rules governing its use, cannot be exchanged for fiat currency. Examples include: Project Entropia Dollars[23]; Q Coins; and World of Warcraft Gold."

The first categorisation of virtual currencies is whether the virtual currency can be exchanged back-and-forth for fiat currency. A virtual currency that can be exchanged for fiat currency is called a "convertible" or "open" virtual currency. A virtual currency that cannot be exchanged for fiat currency is called a "non-convertible" or "closed" virtual currency.

As noted in the FATF report, even where a non-convertible currency is transferrable only within a specific virtual environment, it is possible that an unofficial, secondary black market may arise to exchange the "non-convertible"

[21] FATF Report "Virtual Currencies – Key Definitions And Potential AML/CFT Risks" FATF, June 2014. (Source: http://www.fatf-gafi.org/topics/methodsandtrends/documents/virtual-currency-definitions-aml-cft-risk.html)

[22] "Virtual Currency Schemes", European Central Bank, October 2012. (Source: http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf)

[23] Notwithstanding the definition provided above by the FATF, it should be noted that Project Entropia Dollars can, in fact, be exchanged for fiat currency and is therefore a convertible currency (http://account.entropiauniverse.com/account/withdrawals/).

virtual currency for fiat currency or another virtual currency[24]. Because of this, the categorisation of virtual currencies into convertible/non-convertible is of limited value as a primary distinguishing characteristic for law enforcement and investigative purposes. Instead, the categorisation of virtual currencies based on whether they are centralised or non-centralised is more applicable. This distinction is discussed in the next section.

5.2 Centralised vs. Non-centralised Virtual Currency

The second categorisation of virtual currencies is whether the virtual currency has a centralised administrating authority or not. A virtual currency with a central administrating authority is called a "centralised" virtual currency. A virtual currency with no central administrating authority is called a "decentralised" virtual currency.

All non-convertible virtual currencies are centralised. By definition they are issued by a central authority that establishes rules making them non-convertible. Convertible virtual currencies may be either centralised or decentralised.

"Centralized Virtual Currencies have a single administrating authority (administrator) – i.e., a third party that controls the system. An administrator issues the currency; establishes the rules for its use; maintains a central payment ledger; and has authority to redeem the currency (withdraw it from circulation). The exchange rate for a convertible currency may either be floating – i.e. determined by market supply and demand for the virtual currency – or pegged – i.e. fixed by the administrator at a set value measured in fiat currency or another real-world store of value, such as gold or a basket of currencies. Currently, the vast majority of virtual currency payment transactions involve centralized virtual currencies. Examples: E-gold (defunct); Liberty Reserve dollars/euros (defunct); Second Life "Linden dollars"; PerfectMoney; WebMoney "WM units"; and World of Warcraft gold."

A third party in the context of this categorisation is an individual or entity that is involved in a transaction but is not one of the principals and is not affiliated with the other two participants in the transaction – i.e. a third party functions as a neutral entity between the principals in a business or financial transaction.

"Decentralized Virtual Currencies (a.k.a. crypto-currencies) are distributed, open-source, math-based peer-to-peer virtual currencies that have no central administrating authority, and no central monitoring or oversight. Examples: Bitcoin; LiteCoin; and Ripple."

[24] "Virtual currency requires tough new regulations", China View, February 2012. (Source: http://news.xinhuanet.com/english/2007-02/12/content_5730970.htm)

The most topical example of a decentralised virtual currency is Bitcoin, although there are others. Decentralised virtual currencies typically operate on the basis of a peer-to-peer network through which transactions are managed. Information about transfers of ownership propagates through the network in such a way that after a short period of time, when the transactions are confirmed, the security and integrity of the value transfer is assured.

Case Study: Linden Dollars

Second Life is an online virtual world developed by Linden Lab[25]. Individuals interact with Second Life by installing a software application on their PC that allows them to connect to and explore the virtual world. Within the context of this virtual world there is an internal economy and an internal currency, known as the Linden dollar. Linden dollars can be used to buy, sell, rent or trade land, goods or services with other users.

By the categorisation described in Section 5, Linden dollars are a convertible, centralised virtual currency as discussed in the following sub-sections.

Convertible Virtual Currency

Linden dollars can be purchased both in the world of Second Life and also online at the Linden Exchange, LindX[26], or at other third-party currency exchanges.

Linden Dollars can be purchased at the Linden Exchange using a major credit card or PayPal[27]. Third party currency exchanges accept other forms of transfer such as bank transfers[28] or bitcoins[29, 30]. Linden dollars can be converted into other virtual currencies or fiat currencies by selling the Linden dollars at a currency exchange.

Centralised Virtual Currency

Linden Lab defines the terms of use for Linden dollars and acts as an administrating authority for the virtual currency. Linden Lab defines in their

[25] http://secondlife.com/whatis/
[26] http://community.secondlife.com/t5/English-Knowledge-Base/Buying-and-selling-Linden-dollars/ta-p/700107
[27] http://community.secondlife.com/t5/English-Knowledge-Base/Billing/ta-p/700037#Section_.3
[28] https://www.virwox.com/help.php
[29] http://www.crossworldsxchange.com/buy_L$_bitcoins.htm
[30] https://en.bitcoin.it/wiki/VirWoX

terms of service that dollars have no intrinsic value as a form of currency or other financial instrument and cannot be redeemed from Linden Lab[31]. There are also a number of notable cases where policy decisions by Linden Labs have had a significant effect on the value of Linden dollars[32].

Case Study: World of Warcraft Gold

World of Warcraft is a massively multiplayer online role-playing game (MMORPG) created by Blizzard Entertainment[33]. Players control a character within the game to explore the world, fight monsters, complete quests and so on. Players can purchase items within the game using virtual gold. Gold is earned within the game by completing quests and in various other ways.

By the categorisation described in Section 5, World of Warcraft Gold is a non-convertible, centralised virtual currency as discussed in the following sub-sections.

Non-convertible Virtual Currency

Due to the fact that World of Warcraft gold being sold by third parties is commonly stolen from compromised accounts or otherwise gained through means that breach acceptable usage policies, Blizzard Entertainment actively discourages users of World of Warcraft from purchasing gold from third parties[34], [35]. There are programmes of user awareness as well as sanctions for those found using third party gold. Sanctions for users purchasing gold from third parties can include being permanently banned from World of Warcraft[36].

Despite this, there continues to be an active unofficial, secondary trade in World of Warcraft gold[37]. As mentioned in Section 5.1, the fact that there is secondary trade in World of Warcraft gold means that it becomes, *de facto*, a convertible virtual currency even though it is non-convertible according to the definitions of the FATF.

[31] lindenlab.com/tos. In particular Sections 4.5 and 9.2.
[32] http://en.wikipedia.org/wiki/Economy_of_Second_Life#Acts_of_Linden
[33] http://us.battle.net/wow/en/
[34] http://eu.battle.net/wow/en/shop/anti-gold/
[35] http://us.battle.net/wow/en/blog/3768752
[36] http://us.battle.net/en/security/theft#gold
[37] http://www.wikihow.com/Safely-Buy-Gold-in-World-of-Warcraft

Centralised Virtual Currency

Blizzard Entertainment defines the terms of use for World of Warcraft gold and act as an administrating authority for the virtual currency[38]. In particular, by agreeing to the terms of use:

"You agree that you have no right or title in or to any such content, including without limitation the virtual goods or currency appearing or originating in the Game, or any other attributes associated with any Account. Blizzard does not recognize any purported transfers of virtual property executed outside of the Game, or the purported sale, gift or trade in the "real world" of anything that appears or originates in the Game. Accordingly, you may not sell in-game items or currency for "real" money, or exchange those items or currency for value outside the Game."[39]

[38] http://us.blizzard.com/en-us/company/legal/wow_tou.html
[39] http://us.blizzard.com/en-us/company/legal/wow_tou.html (Section 8)

6 Interface Between Virtual Currencies and Traditional Financial System

For the purposes of this manual, it is important to understand the interface between virtual currencies and the traditional financial system.

As mentioned above, secondary markets for non-convertible virtual currencies exist. The primary source of non-convertible currencies is the central administrating authority for the particular virtual currency in question. Secondary markets for non-convertible currencies, such as online auction sites, may accept a wide range of funding sources, including convertible virtual currencies.

The purpose of this section, however, is to focus on the ways in which primary trade in convertible virtual currencies is funded. In other words, the ways in which it is possible to convert between virtual currencies and fiat currencies, goods, services or other representations of value.

6.1 Virtual Currency Exchanges

Convertible virtual currencies are commonly traded on virtual currency exchanges, with different exchanges available for trading different virtual currencies. A mix of fixed fee and percentage commission pricing structures are used by the virtual currency exchange for their exchange services. Additional fees may be charged for depositing and/or withdrawing funds from the virtual exchange account. The range of available funding sources and withdrawal destinations for virtual currency exchanges vary but some examples include:

- Other virtual currencies[40], [41], [42].
- Bank transfer[43], [44], [45]
- Money remittance provider[46]
- Payment card[47]
- Cash[48], [49]
- PayPal[50]

[40] https://firstmetaexchange.com/home
[41] https://www.virwox.com/?stage=1
[42] http://howtobuybitcoins.info/
[43] https://www.bitstamp.net/help/how-to-buy/
[44] http://portal.bitcoinschile.cl/
[45] https://www.bitcoin.de/en/faq/which-payment-methods-are-available/18.html
[46] https://www.coinmama.com/
[47] http://btc-dealer.com/
[48] http://www.tradebitcoin.com/
[49] https://localbitcoins.com/
[50] https://www.virwox.com/?stage=1

Other novel models exist, where the currency exchange does not necessarily support the back-and-forth trade of currency but facilitates the purchase of virtual currency through non-traditional means. One example of such a system is the purchase of bitcoins by SMS[51].

Considering the relatively unregulated nature of this market, a risk exists that virtual currency exchanges do not properly identify the source of cash or third party funding used to purchase virtual currencies[52]. In the recent past, several countries have announced plans to regulate virtual currency intermediaries, such as currency exchanges, to combat the risks of money-laundering associated with them[53], [54], [55].

6.2 Financial Institutions

As mentioned above in Section 6.1, a bank account can act as a funding source for purchasing virtual currency or as a destination for exchanging virtual currencies for fiat currency. As such, all of the typical regulatory and supervisory measures that are in place relating to the use of bank accounts would be applicable. However, as highlighted elsewhere, the use of money mules to facilitate laundering of crime proceeds using various techniques on the Internet, including virtual currencies, can present challenges[56], [57].

Virtual currency exchanges themselves will also interface with the financial system to hold and/or transfer fiat currency. The legal and regulatory implications of this fact continue to evolve[58], [59], [60].

---

[51] http://sms.btc-sm.com/

[52] FATF Report "Virtual Currencies – Key Definitions And Potential AML/CFT Risks" FATF, June 2014. (Source: http://www.fatf-gafi.org/topics/methodsandtrends/documents/virtual-currency-definitions-aml-cft-risk.html), p. 9.

[53] "Singapore to regulate virtual currency exchanges", BBC News, March 2014. (Source: http://www.bbc.co.uk/news/business-26556523)

[54] "New York regulator plans 'regulated' Bitcoin exchanges", BBC News, March 2014. (Source: http://www.bbc.co.uk/news/technology-26538378)

[55] "Convertible Virtual Currency (Like Bitcoin) is Subject to US Money-Laundering Rules", Digital Passing, March 2013. (Source: http://www.digitalpassing.com/2013/03/22/convertible-virtual-currency-bitcoin-money-laundering-rules/)

[56] "Criminal money flows on the Internet: methods, trends and multi-stakeholder counteraction.", Council of Europe Global Project on Cybercrime and MONEYVAL, March 2012. (Source: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/reports-presentations/MONEYVAL_2012_6_Reptyp_flows_en.pdf)

[57] "Money Laundering Using New Payment Methods", FAFT-GAFI, October 2010. (Source: http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20using%20New%20Payment%20Methods.pdf)

[58] "Jaman's Mizuho in US, Canada suits over Mt. Gox bitcoin losses", Reuters, March 2014. (Source: http://www.reuters.com/article/2014/03/16/us-bitcoin-mtgox-mizuho-

6.3 Cash/ATMs

The use of cash has always been attractive in the laundering of crime proceeds. Therefore, the interface between virtual currencies and cash warrants particular attention.

The awareness and popularity of virtual currencies has substantially increased in recent years, particularly with the advent of Bitcoin. Following on from this growing popularity, novel business models have emerged in the case of Bitcoin that offer possibilities were not historically available with other virtual currencies. For example, Bitcoin ATMs are available in a number of countries[61]. Such ATMs allow buying and selling of bitcoins for cash[62], [63].

Additionally, virtual currency exchanges exist to facilitate people meeting face-to-face to exchange virtual currencies for cash[64], [65].

6.4 Payment Cards

Globally, payment cards, in particular debit and pre-paid cards have grown at double-digit percentage rates nearly every year in the last decade[66]. Prepaid cards can act an alternative to a variety of traditional banking products and services, such as debit or credit cards or travellers cheques[67]. This may include features such as not only making payments but also receiving payments from third parties, cross-border remittances, and so on.

Prepaid cards can be designed to provide absolute anonymity. In fact, some prepaid card issuers attract customers with anonymous prepaid cards with no or high loading and transaction limits[68].

---

idUSBREA2E01V20140316)

[59] "MtGox class-action suits in US and Canada allege fraud, drag in Japan's Mizuho Bank", arstechnica, March 2014. (Source: http://arstechnica.com/tech-policy/2014/03/mtgox-class-action-suits-in-us-and-canada-allege-fraud-drag-in-japans-mizuho-bank/)

[60] "China Banks Financial Companies from Bitcoin Transactions", Bloomberg News, December 2013. (Source: http://www.bloomberg.com/news/2013-12-05/china-s-pboc-bans-financial-companies-from-bitcoin-transactions.html)

[61] http://bitcoinatmmap.com/

[62] https://bitcoinatm.com/

[63] https://robocoinkiosk.com/

[64] http://www.tradebitcoin.com/

[65] https://localbitcoins.com/

[66] "Expanding Opportunities in Debit and Pre-paid Card Products", Euromonitor International, February 2013. (Source: http://www.euromonitor.com/expanding-opportunities-in-debit-and-pre-paid-card-products/report)

[67] "Report on New Payment Methods", FATF-GAFI, 2006. (Source: http://www.fatf-gafi.org/media/fatf/documents/reports/Report%20on%20New%20Payment%20Methods.pdf)

[68] "Money Laundering Using New Payment Methods", FATF-GAFI, October 2010. (Source: http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20using%20New%20Payment%20Methods

6.5 Money Remittance Providers

Previous work studying criminal money flows on the Internet has indicated that the use of money remittance providers is the most common technique for laundering criminal money derived from cybercrime[69]. As the overwhelming majority of wire transfers through money remittance providers are paid out in cash, this service enables the introduction of criminal proceeds into the financial system. Further, the sheer volume of legitimate cash transactions provides excellent camouflage for money-laundering activity in the placement stage. Often the money services are part of a more complex scheme where at least one cash operation is involved, involving at least one money mule.

A commonly reported typology involving money remittance providers proceeds as follows:

1. Fake job advertisements are sent via spam, applicants being recruited by telephone or by other non-face-to-face procedures. Often jobs are related to financial issues or advertised as “work at home”.

2. Money transferred into the bank account of the recruited mule. The mule is required to withdraw the amount in cash and send it to a specific beneficiary by money remittance provider. The mule receives a commission for performing this service.

3. Money remittance providers are used to move the cash to its recipient.

In the context of the current discussion, there is no reason why cash could not be transferred into the account of a mule (step 2 above) via a virtual currency.

6.6 Merchants Accepting Virtual Currencies

Another side effect of the increasing popularity of bitcoins is that an increasing numbers of merchants are accepting payments in virtual currencies, most notably with bitcoins[70, 71, 72]. Bitcoins are an attractive option for merchants for the following reasons[73]:

.pdf)

[69] Paragraph 139, “Criminal money flows on the Internet: methods, trends and multi-stakeholder counteraction.”, Council of Europe Global Project on Cybercrime and MONEYVAL, March 2012. (Source: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/reports-presentations/MONEYVAL_2012_6_Reptyp_flows_en.pdf)

[70] https://bitpay.com/directory#/

[71] https://spendbitcoins.com/places/

[72] http://www.coindesk.com/information/what-can-you-buy-with-bitcoins/

[73] https://www.bitcoin247.com/en/merchants

1. Once confirmed, Bitcoin transactions are irreversible therefore there is no possibility of chargebacks or other fraud losses that can occur when using payment cards.

2. The fees associated with processing bitcoins are lower than payment card acquiring fees.

As well as merchants accepting bitcoins, there is a growing ecosystem of merchant services that are available to assist small businesses to configure and accept bitcoin payments[74].

[74] https://en.bitcoin.it/wiki/How_to_accept_Bitcoin,_for_small_businesses

7 Legal Regulation

This section of the manual will attempt to address the issues of currently applicable regulations of virtual currency, both in the national and international contexts.

7.1 International Regulations and Standards

As an introductory note, it is fair to assume that, in the current state of affairs, no set of specific rules or standards that are globally applicable yet exists in relation to virtual currency as a form of digital currency. The relative novelty of the phenomenon, as well as a fairly recent rise to any substantial levels and relatively little impact, has so far not called for a comprehensive legal regulation of virtual currencies.

Yet, it would be illogical to assume that virtual currencies operate in a complete legal vacuum. Even in the absence of a set framework of legal regulations in this area, one has to be aware of the general context in which electronic money and virtual currency is being used, that is, the rapid development of e-commerce, and, in particular, the efforts of global, regional and national players in order to facilitate innovation and efficiency of financial transactions that are, without doubt, one of the core enablers of successful e-commerce systems. Besides, some aspects related to the potential use of virtual currencies for money-laundering purposes, as well as cybercrime offences it is usually connected with (in cases of illegal activities involving virtual currencies), need to be kept in mind.

7.1.1 E-commerce Regulatory Framework and its Application to Virtual Currencies

Although there is no uniform definition of e-commerce, it is largely understood as any form of business transaction between individuals and entities that use electronic communications technology in place of physical exchange of goods or services.[75] The rise and continued growth of e-commerce is largely attributed to the development of the Internet as a medium for communication between customers and businesses; in recent figures, e-commerce amounts to almost 5% of global sales.[76]

[75] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, Article 2 (f) (Source: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:en:HTML); UNCITRAL Model Law on Electronic Commerce, Art. 1(b) (Source: https://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model.html.).

[76] BizReport, "Global ecommerce sales top U.S.$1 trillion" (Source: http://www.bizreport.com/2013/08/global-ecommerce-sales-top-us1-trillion.html)

The reference point for e-commerce regulations is the Model Law on Electronic Commerce of 1996, developed and adopted by the United Nations Commission on International Trade Law (UNCITRAL).[77] Although not an international treaty proper - in the classic sense of public international law – this document has been used extensively to provide guidance to developing national legislations concerning facilitation of e-commerce and is, in essence, an international standard for e-commerce regulation. The UNCITRAL Secretariat keeps track of nations that have adopted and put into force the legislation on e-commerce; as of writing, such laws have been promulgated by 54 states.[78]

The UNCITRAL Model Law on Electronic Commerce lays down a number of concepts that are instrumental in understanding the current legal debate with regard to virtual currencies. One of such concepts is the principle of **technological neutrality**,[79] or *media neutrality* in terms put forward by the Model Law.[80] Translating this in terms of virtual currencies, the technologies used for transactions by virtual currencies can be used for both legitimate and illegal purposes, and the core technology is not considered illegal *per se* due to the potential of its criminal use. This argument is particularly relevant in the debates surrounding potential prohibition of virtual currencies as legitimate financial instruments, which would result in denial to the legitimate use of technology. These concerns are not dissimilar in nature to jurisprudence involving decentralized peer-to-peer sharing of copyrighted materials and technical means used for these purposes;[81] most of the case law confirms technological neutrality concept by upholding the legitimate uses of the technology in question, and shifting responsibility for illicit uses to the end users.

Although the immediate purpose of the UNCITRAL Model Law on E-Commerce may be to harmonize the e-commerce regulations, its overall goal is, in essence, to promote development of e-commerce and to create an environment conducive to its growth. In this context, virtual currencies pose an interesting dilemma. On one hand, the use of virtual currency is consistent with the overall goal of facilitating electronic commerce by offering yet another method of

[77] https://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model.html.
[78] https://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model_status.html.
[79] Explanatory Report to the United Nations Convention on the Use of Electronic Communications in International Contracts, available at: http://www.uncitral.org/pdf/english/texts/electcom/06-57452_Ebook.pdf.
[80] UNCITRAL Model Law on Electronic Commerce (with Guide to Enactment), (Source: https://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf.)
[81] A&M Records, Inc. v. Napster, Inc. (Source: http://onlinelaw.wustl.edu/case-study-am-records-inc-v-napster-inc/); MGM Studios, Inc. v. Grokster, Ltd. (Source: http://en.wikipedia.org/wiki/MGM_Studios,_Inc._v._Grokster,_Ltd.), Pirate Bay (Source: http://en.wikipedia.org/wiki/The_Pirate_Bay_trial), BitTorrent systems (Source: http://en.wikipedia.org/wiki/Legal_issues_with_BitTorrent).

financial transactions that may be beneficial for the development of electronic trade; on the other, threats and challenges posed by the highly speculative nature of crypto-currencies and cybercrime threats against the currencies themselves may represent a discouraging factor for electronic commerce, as illustrated by recent high-profile case of Mt. Gox[82].

One of the most relevant aspects of e-commerce regulations in terms of virtual currencies is **consumer protection**, that is, the set of rules protecting the rights of customers entitling them to a reasonable standard of goods and services received, and protecting them from unfair and unjust business practices. For example, the EC Directive on Electronic Commerce[83] specifically notes the high level of consumer protection as an essential concept contributing to the free movement of information society services.[84] Given the wide range of issues covered by modern consumer rights and consumer protection legislation, it is rather apparent that some of the features of crypto-currencies, such as Bitcoin, with the finality of financial transaction and without the possibility for returns would certainly be questionable from the consumer protection point of view.[85] Perhaps an even more relevant example is the ongoing and active convergence between cybercrime and data protection communities: consumer protection organizations are quickly becoming major partners in detecting and reporting cybercrime,[86] and can thus be an equally important source of information for investigations related to illegal use of virtual currencies.

At the same time, various legal texts concerning electronic payments and electronic money have arguably less relevance in the context of virtual currencies. The problem is that either international or regional regulatory instruments addressing e-money and e-payments[87] follow largely the logic that such payments and funds are being processed through established financial mechanisms, by regular financial institutions that deal with fiat money; while virtual currencies, whether centralized or decentralized, operate, as a matter of fact, beyond the realm of these institutions and mechanisms, with the important

[82] http://en.wikipedia.org/wiki/Mt._Gox#Bankruptcy_and_shutdown.
[83] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, (Source:http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32000L0031&from=EN.
[84] P. Directive on injunctions for the protection of consumers' interests (Source: http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:31998L0027)
[85] Right of withdrawal under the Directive 2011/83/EU on Consumer Rights (Source: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32011L0083&rid=1)
[86] http://www.ftc.gov/enforcement/consumer-sentinel-network.
[87] UNCITRAL Model Law on International Credit Transfers (Source: https://www.uncitral.org/pdf/english/texts/payments/transfers/ml-credittrans.pdf); Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions (Source: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009L0110&from=EN)

exception of interactions taking place during exchange into fiat currencies and vice versa. While certain analogies can undeniably be drawn from a purely legal standpoint, the dissimilarities in processing transactions and, above all, the large disparity in terms of applicable regulation hold little value in terms of legal analysis and practical application in this particular respect.

7.1.2 Money-laundering Regulations and Virtual Currencies

Money-laundering denotes the process by which criminals disguise the original ownership and control of the proceeds of criminal conduct by making such proceeds appear to have derived from a legitimate source. Though criminal money may be successfully laundered without the assistance of the financial sector, the reality is that hundreds of billions of dollars of criminally derived money is laundered through financial institutions annually.[88] The nature of the products and services offered by the financial services industry (managing, controlling and possessing money and property belonging to others) means that it is vulnerable to abuse by money launderers.

There is an extensive body of international instruments and standards addressing money-laundering, pioneered by the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances of 1988, which is the first international legal instrument that has defined the elements of offences of laundering of the proceeds of crime provided by this Convention.[89] This approach is further upheld by the United Nations Convention on Transnational Organized Crime of 2003[90] and the United Nations Convention against Corruption of 2005,[91] which further develop the notions of laundering of the proceeds of crime, and establish specific requirements and procedures for combating these. The International Convention for the Suppression of the Financing of Terrorism takes a more specialized approach by specifically requiring mechanisms for identification, detection and freezing or seizure of instrumentalities and proceeds from terrorist financing crimes.[92]

The overview of modern instruments for combating money-laundering would not be complete without noting the Financial Action Task Force (FATF), an

[88] International Compliance Association, "What is Money Laundering?", (Source: http://www.int-comp.org/what-is-money-laundering).
[89] Article 5 of the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (Source: http://www.unodc.org/pdf/convention_1988_en.pdf)
[90] Article 6 and 7 of the United Nations Convention against Transnational Organized Crime (Source: http://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf)
[91] Article 23, 52, 54 and 57 of the United Nations Convention against Corruption (Source: http://www.unodc.org/documents/treaties/UNCAC/Publications/Convention/08-50026_E.pdf)
[92] Article 8 of the International Convention for the Suppression of the Financing of Terrorism (Source: http://www.un.org/law/cod/finterr.htm).

inter-governmental body established and tasked with setting standards and promoting effective implementation of legal, regulatory and operational measures for combating money-laundering, terrorist financing and other related threats to the integrity of the international financial system[93] Its Recommendations[94], that encompass topics such as money-laundering, terrorist financing, and the financing of the proliferation of weapons of mass destruction, are, in essence, enforceable standards subject to compliance monitoring mechanisms employed by the FATF itself.

Given the purpose of this manual and the nature of decentralized virtual currencies, it is rather apparent that the use of virtual currencies attracts legitimate concerns of its use as a means to undertake money-laundering or, in general, criminal money flows on the Internet. Nevertheless, it has to be understood that money-laundering aspects of virtual currencies are focused to a lesser extent on technology (which can be still relevant for the reasons of increased secrecy and difficult traceability, as well as reliance on cryptography), but rather relate to the lack of applicable regulation and powers of supervisory authorities with regard to virtual currency transactions. Since transactions involving virtual currency are, in fact, removed from established, and thus thoroughly regulated, traditional financial institutions, virtual currencies pose a certain appeal to those who wish to engage in money-laundering. Some specific types of virtual currency based on anonymity and cryptography, such as Bitcoin, would have an "added value" of being extremely hard to trace and decode in terms of transactions between users of such systems. Therefore, a relevant focus in terms of money-laundering is not on virtual currency itself, but on a rather closely related framework of international standards that address, in one way or another, the threats that are connected with the criminal use of virtual currencies for laundering of proceeds of crime.

7.2 Criminal Offences Associated with Virtual Currencies

Virtual currencies, by their very nature, may be related to a range of criminal offences. Whilst the focus of this Manual is on money laundering offences involving virtual currency, it is important to briefly set out the broader context within which such offences may be encountered. This includes as concerns the relationship of offences involving virtual currencies to cybercrime offences.

In the first instance, and as noted above, virtual currencies may engage a number of regulatory provisions. Breach of such regulations may be accompanied, in some cases, by criminal sanctions. Thus, the possession or operation of a virtual currency *per se*, in some jurisdictions may constitute a

[93] http://www.fatf-gafi.org/pages/aboutus/.
[94] http://www.fatf-gafi.org/topics/fatfrecommendations/documents/internationalstandardsoncombatingmoneylaunderingandthefinancingofterrorismproliferation-thefatfrecommendations.html.

criminal offence, such as illegal possession of an unlicensed currency, or operation of an unlicensed money exchange business.

As a form of value, virtual currencies may themselves also form the object of a criminal offence. Possible offences include, for example, the theft of sums of virtual currency, or the fraudulent obtaining of virtual currency. Such acts may or may not also include conversion to real currency as part of the offence.

In addition, virtual currencies may form part of the *modus operandi* of a separate offence, such as when used for the purchase of illicit goods, such as weapons, drugs or child abuse material, as well as for the payment of services that may be regulated or criminalized in certain countries, such as online gambling. In this sense, virtual currencies may form *instrumentalities* of crime. In addition, virtual currencies may be provided or collected with the intention that they should be used in full or in part in order to carry out an offence constituting an act established in accordance with the universal legal instruments against terrorism, or otherwise intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities of a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or international organization to do or abstain from doing any act (terrorist financing offences).

Finally, as is the focus of this manual, the criminal offence of money laundering is committed where virtual currencies are used for the conversion or transfer of property, knowing that such property constitutes proceeds of crime, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an offence or offences to evade the legal consequences of his actions, or for the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of property, knowing that such property is proceeds of crime.

In light of the electronic nature of virtual currencies, in almost all of these possible offence types, a close relationship with ‘cybercrime’ offences may exist. The term ‘cybercrime’ itself is not amenable to a single definition, and is likely best considered as a collection of acts or conduct, rather than one single act. Cybercrime is commonly understood as a concept that denotes offences against computer data and systems, namely offences against confidentiality, integrity and availability of data and systems, as well as offences committed by means of computer data and systems and content-related offences, such as computer-related fraud, copyright or trademark offences, or sending and controlling sending of SPAM. In the latter case, the “traditional” offences, such as forgery or production, distribution, or possession of child pornography, gain different quality and impact if committed through the use of computer systems, since the

technology enables and facilitates commission and/or cover-up of such offences, wider distribution of such effects, and aggravated impact on victims, often across different jurisdictions.[95] Overall, however, a distinction may be made by 'core' cybercrime offences, related to acts directed against computer information systems or data, and a broader category of cybercrime offences committed by means of computer systems or data.

The last decade has seen significant developments in the promulgation of international and regional instruments aimed at countering cybercrime. These include binding and nonbinding instruments. The genesis, legal status, geographic scope, substantive focus, and mechanisms of such instruments vary significantly. Examples of regional treaties are, for instance, the Council of Europe Convention on Cybercrime, the Commonwealth of Independent States (CIS) Agreement on Cooperation in Combating Offences related to Computer Information, the Shanghai Cooperation Organization Agreement on Cooperation in the Field of International Information Security, or the League of Arab States Convention on Combating Information Technology Offences.[96] All of the GUAM Member States are Member States of the Council of Europe, and also became Parties to the Council of Europe Convention on Cybercrime., .[97] They regularly undergo compliance monitoring with the Council of Europe Cybercrime Committee (T-CY).

With respect to criminal offences involving virtual currencies, 'core' cybercrime offences (such as illegal access to a computer system) may be *ancillary* to offences such as theft of virtual currency. Breaking into a personal wallet through 'hacking', with a view to stealing bitcoins can be qualified as theft for example, where cybercrime is an auxiliary offence, facilitating the commission of the former. Illegal access offences may also be linked with money laundering offences involving virtual currency, such as when accounts of third parties are used without the consent of that person for transactions.

Broader forms of cybercrime, such as computer-related fraud, may constitute the primary offence for which virtual currency is the object, such as when

[95] UNODC Comprehensive Study on Cybercrime (Draft, 2013), prepared by UNODC for the consideration of the open-ended intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime, according to the methodology agreed on by the expert group (hereinafter referred to as UNODC Comprehensive Study on Cybercrime), pp. 11 et. seqq.

[96] Council of Europe Convention on Cybercrime (2001); Commonwealth of Independent States (CIS) Agreement on Cooperation in Combating Offences related to Computer Information (2001); Shanghai Cooperation Organization Agreement on Cooperation in the Field of International Information Security (2009); League of Arab States Convention on Combating Information Technology Offences (2010). For an overview of binding and non-binding instruments, see also UNODC Comprehensive Study on Cybercrime, pp. 63 et seqq.

[97] List of State Parties available at: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG.

virtual currency is obtained through deception. Finally, content-related and other forms of cybercrime, such as computer-related possession or distribution of child abuse material or sale of illicit drugs online, may constitute either a predicate offence for money laundering via virtual currencies (in the case of sale of such material), or the primary offence for which virtual currencies are an instrumentality (in the case of purchase of such material). Indeed, the case of Silk Road could be no better example of the potential use of crypto-currencies for trade in illegal materials.[98] In short, the possible interactions between cybercrime offences, 'traditional' offences, and virtual currencies are multiple and potentially complex.

Importantly, however, a number of features of criminal acts usually considered as 'cybercrime' show similar features, from the investigative perspective, as criminal acts involving virtual currencies. Cybercrime, for example, perhaps more than any other form of crime, is often committed as a transnational offence, spanning several jurisdictions and leading to problems both in investigation of and legal assistance in such matters. Secondly, illegal use, interception or interference with computer systems or data is often difficult to track and thus reporting levels of cybercrime remain a major problem. Third, as with all crimes, cybercrimes leave traces of evidence, and most of such evidence is in electronic format – that is, electronic evidence; there are numerous legal and technical difficulties in securing and examining such evidence, especially in a timely manner. These and other features of cybercrime, that are very often predicate or auxiliary offences to the criminal use of virtual currencies, often require a more advanced understanding of both regulators and criminal justice personnel in successfully addressing the challenges posed by both.

7.3 National Regulatory Frameworks

In contrast to the international context, the issue of regulating the use of virtual currencies has been addressed domestically to a certain level in several jurisdictions, mostly in terms of applicable reporting and registration, taxation, and potential misuse for money-laundering. However, it seems that the current attempts at regulating virtual currencies are still at the preliminary stage, testing various approaches to regulation and anticipating the growth of virtual currency transactions, as well as being mindful of the advances in technology. Hence the widely varying approaches to regulating the status and rules applicable to virtual currencies.

Due to its increasing reliance on e-commerce, the **United States of America** has so far been strongly engaged in the virtual currency debate. The approach currently employed by its policy makers and regulators is to allow virtual currencies to operate under the condition that specific regulations are

[98] USA Today, "How FBI brought down cyber-underworld site Silk Road" (Source: http://www.usatoday.com/story/news/nation/2013/10/21/fbi-cracks-silk-road/2984921/)

applicable to certain players in virtual currencies services. Along these lines, in March 2013, the Financial Crimes Enforcement Network (FinCEN) issued interpretive guidance FIN-2013-G001,[99] clarifying the application of US regulations to certain categories of virtual currency services (exchangers, administrators and so on) in terms of obligations for money services businesses ("MSBs"), who must comply with registration, record-keeping, and other financial requirements. The March 2013 guidance draws clear lines between, on one hand, users of virtual currency (not deemed as MSBs and thus excluded from registration and recording requirements) and administrators and exchangers on the other, who are covered by definition of MSBs since their actions constitute "money transmitter" services. Additionally, the Internal Revenue Service (IRS) has issued Notice 2014-21[100] in response to several questions as to the status of virtual currencies in the United States for taxation purposes. It notes that the virtual currencies must be treated as a commodity and thus taxable in terms of income that may be generated by sale of such commodities.

The **United Kingdom** has taken a similar approach to the market of virtual currencies (decentralized crypto-currencies in particular), as provided by the HM Revenue & Customs Brief 09/14 on "Tax treatment of activities involving Bitcoin and other similar cryptocurrencies".[101] Recognizing the evolving nature of decentralized crypto-currencies, whilst not explicitly recognizing the bitcoin as a full-fledged currency, the brief effectively treats bitcoin like any other form of payment for tax purposes, for both individual (VAT treatment, which differs by the categories of users, such as miners or exchangers) and corporate taxation regime (especially in terms of income and capital gains taxes derived from trade in bitcoins).

China has taken a different approach to regulating the virtual currency market, through banning the use of Bitcoin and other crypto-currencies by financial and payment institutions. In December 2013, The People's Bank of China and Five Associated Ministries issued a Notice on "Prevention of Risks Associated with Bitcoin",[102] making public their position that Bitcoin is not money, cannot be used to exchange legal tender for foreign currency, pay a mortgage, pay a legal settlement, make investments, or provide insurance. However, the prohibition is not absolute, since virtual currencies can still be used as a trade commodity on the Internet at the risk of the users. Nevertheless, Bitcoin-commerce websites

[99] http://fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html.
[100] http://www.irs.gov/pub/irs-drop/n-14-21.pdf?utm_source=3.31.2014+Tax+Alert&utm_campaign=3.31.14+Tax+Alert&utm_medium=email.
[101] http://www.hmrc.gov.uk/briefs/vat/brief0914.htm.
[102] BTC China, "The People's Bank of China and Five Associated Ministries Notice: "Prevention of Risks Associated with Bitcoin" (unofficial translation)", (Source: https://vip.btcchina.com/page/bocnotice2013).

must file with the telecommunications regulatory agencies in accordance with the country's anti-money-laundering law.

Another different, albeit similarly cautious approach has been employed by the authorities of **Canada**, who have taken a position that Bitcoin is not a legal tender in the country. However, unlike the approach employed by China, Canadian authorities have left open a possibility to revise the issue based on developments in the future. In taking a closer look at Bitcoin and other virtual currencies, factors such as financial stability, highly speculative nature as well as "convenience and ease of use, price, reliability, safety, and effective redress mechanisms" for Canadian citizens were taken into account.[103] At the same time, one of the first Automated Teller Machines (ATM) that allows for exchange of virtual currency into Canadian dollar, or vice versa, was installed in Vancouver in October 2013.[104] There are numerous exchange facilities and other ways to trade in bitcoins in Canada, which are indicative of rising popularity of crypto-currencies in the country.

Perhaps a middle ground in these different examples has been established by **Singapore**. Whilst not restricting virtual currencies as an eligible medium for transactions in its financial system, Singapore plans to tighten the requirements for Bitcoin exchanges and vending machines to ensure user identification and transparency at all times.[105]

Case Study : Bitcoin

Bitcoin is a decentralised, peer-to-peer payment network that is powered by its users with no central authority or middlemen. Satoshi Nakamoto published the first Bitcoin specification and proof of concept to a cryptography mailing list in 2009[106]. Fundamentally, the purpose and operation of the Bitcoin network is concerned with the management and sharing of a public ledger, known as the "block chain". This ledger contains

[103] Canada Revenue Agency, "What you should know about digital currency" (Source: http://www.cra-arc.gc.ca/nwsrm/fctshts/2013/m11/fs131105-eng.html).
[104] Mashable, "World's First Bitcoin ATM Opens In Vancouver, Canada" (Source: http://mashable.com/2013/10/30/bitcoin-atm-2/)
[105] Monetary Authority of Singapore, "MAS to Regulate Virtual Currency Intermediaries for Money Laundering and Terrorist Financing Risks" (Source: http://www.mas.gov.sg/news-and-publications/press-releases/2014/mas-to-regulate-virtual-currency-intermediaries-for-money-laundering-and-terrorist-financing-risks.aspx)
[106] https://bitcoin.org/en/faq

every transaction ever performed and is used to verify the validity of every transaction[107]. The integrity and chronological order of the transactions in the ledger are enforced by cryptography.

By the categorisation described in Section 5, bitcoin(s) are a convertible, decentralised virtual currency, also commonly known as a cryptocurrency. Bitcoins introduce some novel technical features that make investigations into the laundering of crime proceeds particularly challenging, therefore it is worthwhile to expend some effort understanding how Bitcoin works.

On this basis, it is useful to consider the functionality of the Bitcoin network in terms of the issues that need to be addressed for it to act reliably as a decentralised virtual currency.

Transferring bitcoins

The first, and perhaps most obvious question, is how do users of the Bitcoin network transfer bitcoins to one another.

Each user in the Bitcoin network has one, or more, Bitcoin addresses. A user can create as many Bitcoin addresses as they want, even a separate addresses for every single transaction if they want[108].

The addresses serves as a unique identifying value that is used to represent ownership of a particular bitcoin[109,110]. For Person A to send money to Person B, they broadcast a message to the Bitcoin network containing the sender address, the recipient address (their "receiving address") and the amount to transfer. Every node in the Bitcoin network that receives this message will update their copy of the ledger and then pass along the transaction message to other nodes[111].

What stops an attacker, say Person C, broadcasting a message to the network transferring bitcoins from Person A's address to Person C (or another person), thus stealing Person A's bitcoins? This eventuality is prevented because the authenticity of transaction messages is assured using the cryptographic technique of digital signatures[112]. In order to create a valid transaction message transferring bitcoins from Person A's address, the

[107] https://bitcoin.org/en/how-it-works
[108] In some commonly available Bitcoin software, the user's identity is represented as a single "wallet" containing multiple "receiving addresses".
[109] Strictly speaking, each address is a public/private key pair. The "receiving address" is the public key. The private key is kept secret and used to digitally sign transactions, thus verifying the authenticity of the transaction.
[110] See http://en.wikipedia.org/wiki/Public-key_cryptography for general information on public key cryptography.
[111] http://www.imponderablethings.com/2013/07/how-bitcoin-works-under-hood.html
[112] http://en.wikipedia.org/wiki/Digital_signature

person generating the message must have the password associated with the address[113].

Two questions now arise:

1. How does Person B know that Person A actually owns the bitcoins that are being transferred?
2. How does Person B know that Person A hasn't already transferred the bitcoins to someone else?

These questions will be answered in the next two sections.

Proving Ownership of bitcoins

In order to construct a valid transaction message to transfer bitcoins, the sender of the bitcoins must prove that they are the current owner.

Consider a situation where Person A is sending, for example, ten bitcoins to Person B. Person A must include in the transaction message references to previous transactions where they received more than the required ten bitcoins. These are referred to as the "inputs" to the transaction[114].

Recall that each user of the Bitcoin network maintains a copy of the ledger ("block chain") that contains the history of all previous transactions. Person B can then verify that the bitcoins referenced in Person A's transaction message indeed belong to Person A.

To simplify this process, there is a rule that transactions must balance. In other words, the number of bitcoins in the inputs to the transaction must match the number of bitcoins in the outputs.

This is best understood with a concrete example. Consider the transaction where Person A wants to send ten bitcoins to Person B. The list of inputs and outputs shown in Table 1 will help to illustrate the balancing issue.

[113] Strictly speaking, the person must have the private key associated with the public key that represents the sender's address. Recall that each address is a public/private key pair. The "receiving address" is the public key and the corresponding private key is used to digitally sign transactions that transfer value from the sender's "receiving address".

[114] The recipient(s) of the Bitcoins are referred to as the "outputs" of the transaction.

Inputs		*Outputs*	
Transaction ID	**Amount**	**Wallet ID**	**Amount**
123	1	Person B	10
456	3	Person A	2
999	4		
888	4		

Table 1: Sample list of transaction inputs and outputs

On the "inputs" side of the transaction there is a list of four transactions that will contain the "receiving address" of Person A. These are Person A's proof that they own a total of 12 bitcoins. Person B can look up these transaction IDs in the block chain and verify that the recipient address in each case was Person A's address. Person B will also verify that these transactions have not been used as the input to some other transaction, in other words that the bitcoins have not already been spent.

On the "outputs" side of the transaction there is the ten bitcoins that Person A wants to send to Person B. Person A transfers the remaining two bitcoins back to their own address. This final output entry means that the total number of bitcoins in the "inputs" equals the total number of bitcoins in the "outputs" and the transaction is therefore balanced.

Preventing Double Spending

The final piece of the puzzle is the prevention of double spending. This is a big issue in a peer-to-peer networks[115], like the Bitcoin network, because there is no guarantee that the order in which transactions are received by any particular node in the network represents the order in which they were created.

In practical terms, what prevents Person A creating a transaction message sending bitcoins to Person B and simultaneously creating a second transaction message to send bitcoins to someone else, hence double spending the same bitcoins? It is certainly possible that some nodes within the Bitcoin network would receive the second transaction first. When the second transaction arrived at these nodes some later time, it would be considered invalid because it reuses inputs that have already been used in

[115] By contrast with a client-server model, peer-to-peer networks have no central point and the peers distribute information through the network. General information on peer-to-peer networks can be found at http://en.wikipedia.org/wiki/Peer-to-peer.

another transaction.

The key technological advance of the Bitcoin network is the technique by which this issue is resolved[116].

Transactions are assembled into groups, known as blocks, and the blocks are linked together to form the block chain. Transactions within a block are considered to have happened at the same time. The blocks are ordered by virtue of the fact that each block refers to the previous block in the chain.

Transactions that are not already in a block are called unconfirmed transactions. Any node in the network can collect a set of unconfirmed transactions, assemble them into a block and propose them as the next block in the chain. The proposed block must contain the solution to a complex mathematical problem that is computationally difficult to calculate[117]. The Bitcoin network dynamically adjusts the difficulty of the mathematical problem so that a new block is added to the chain on average once every ten minutes.

Although it is unlikely, it may occasionally happen that multiple nodes in the Bitcoin network may propose blocks at around the same time. In this case the block chain temporarily branches as different nodes in the network append different blocks to the block chain.

This situation is resolved when the next block is added to the chain. The new block will, as mentioned previously, contain a reference to the previous block in the chain. It will be therefore be appended to one of the two possible branches in the block chain. At this point, one of the two branches is longer. The rule of the Bitcoin network is that nodes must switch to the longest available branch. The result is that very quickly the block chain will stabilise and all nodes will agree on all blocks that are a few back from the end of the chain.

It is therefore considered safer to wait for a period of time before, for example, shipping any goods based on a transfer of bitcoins. Each block takes approximately ten minutes to compute on average, so waiting for six blocks would mean waiting about an hour.

[116] Numerous excellent summaries of this process exist on the Internet. For example https://en.bitcoin.it/wiki/Block_chain and http://www.youtube.com/watch?v=Lx9zgZCMqXE.

[117] Strictly speaking, the node creating the block tries adding a large number of different numeric values to the block until it finds a value such that the cryptographic hash of the block is below a certain threshold value.

Bitcoin Mining

The process of building blocks and appending them to the block chain as described above is known as mining. Whoever solves the block and appends it to the block chain receives a reward of 25 bitcoins. Every four years the block reward is cut in half until eventually no more bitcoins will be released. A total of 21 million bitcoins will be created.

In addition to the bitcoin reward, miners also receive a transaction fee that can optionally be included with transactions. Currently the main reward for mining is the bitcoins themselves but over time transaction fees will become the incentive for mining.

Most mining is performed not by individuals but rather by organised groups of miners, known as mining pools. The reward for computing blocks is divided amongst the members of the pool in proportion to the amount of computational effort each member provided to the pool.

Self Assessment

Question 1: Using the definitions adopted by the FATF, define the terms "virtual currency", "electronic money" and "digital currency", explaining clearly the difference between each term.

Question 2: Describe the characteristics that differentiate a convertible virtual currency from a non-convertible virtual currency. Provide an example from each category.

Question 3: Describe the characteristics that differentiate a centralised virtual currency from a decentralised virtual currency. Provide an example from each category.

Question 4: When considering virtual currencies it is important to be aware of the interface between virtual currencies and the traditional financial system. In this context, discuss the role virtual currency exchanges play. Focus in particular on the range of possible funding sources from which virtual currencies can be acquired.

Question 5: Aside from virtual currency exchanges, give three examples of interfaces between the traditional financial system and virtual currencies that are relevant to the issue of laundering crime proceeds through the use of virtual currencies.

Question 6: Explain the reasons why some virtual currencies might be an attractive payment method for legitimate merchants.

Question 7: Explain what is meant by the term cryptocurrency.

Question 8: Describe the operation of the Bitcoin network paying particular attention to the purpose of "mining".

Question 9: Explain how the Bitcoin network prevents "double spending" of bitcoins.

Question 10: Explain how a user of the Bitcoin network proves ownership of a certain amount of bitcoins to another user.

Question 11: Describe the correlation between principles of technological neutrality and the use of virtual currencies for illegal purposes.

Question 12: Describe the possible "appeal" of virtual crypto-currencies for money-laundering purposes.

Question 13: What is the difference between cybercrime offences against confidentiality, integrity and availability of computer/systems data, and content-related cybercrime offences?

Question 14: Mention at least two countries that have banned or restricted

the use of bitcoins, and elaborate on the reasons for such decisions.

Basic Manual on the Detection And Investigation of the Laundering of Crime Proceeds Using Virtual Currencies

Module 2
The Challenges Presented by Virtual Currencies

1 Summary

When considering the laundering of crime proceeds, virtual currencies present a range of particular challenges. The purpose of this module is to describe these challenges.

Firstly, the reasons why virtual currencies can present difficulties to the detection and investigation of laundering of crime proceeds will be examined. This is followed by an examination of the typologies by which virtual currencies are used to launder crime proceeds. Finally, some relevant trends are also highlighted.

2 Learning Objectives

By reading this module you will:

- Understand the threats presented by virtual currencies.
- Be aware of the typologies used to facilitate laundering by virtual currencies.
- Know the challenges to detection of laundering through virtual currencies.
- Be aware of the challenges that can exist at a national level to the investigation of laundering through virtual currencies.
- Be aware of the challenges that can exist at an international level to the investigation of laundering through virtual currencies.
- Be aware of relevant trends in the area of virtual currencies and their use for laundering crime proceeds.

3 Threats Presented by Virtual Currencies

This section intends to answer the following question: what is it about the nature of virtual currencies that makes them difficult to investigate in cases of laundering of crime proceeds? To answer this, the following sections describe some of the unique challenges to investigations posed by the use of virtual currencies to launder crime proceeds.

3.1 Fast, Irreversible Transactions

A number of factors relating to the speed and reversibility of virtual currency transactions are notable from the point of view of laundering crime proceeds.

The speed of transactions that are possible with new payment methods[1], [2] has been highlighted as a risk factor in previous work. In particular, funds can be withdrawn or converted much more quickly than through more traditional channels. The implication of the possible transaction speed is increased complexity of monitoring and additional difficulty freezing funds. New payment methods, in this context, include virtual currencies.

The extent to which transactions can be reversed depends on the virtual currency in question. Bitcoin transactions, for example, once confirmed cannot be reversed[3]. They can, however, be refunded by the person receiving the funds. This, of course, is not a reversal of the transaction, rather a transaction by the recipient transferring the funds back to the original sender. Centralised virtual currencies, on the other hand, are generally operated within the context of the terms of service of the administrating authority[4]. In the vast majority of centralised virtual currency systems, the administrating authorities will advertise the fact that transactions made in the virtual currency system cannot be reversed. However, the administrating authority typically has ultimate authority to act as they see fit, including, presumably, reversing virtual currency transactions if they were to choose to do so.

Several forms of transaction are possible, and therefore need to be considered. In the following sub-sections, the behaviour of virtual currencies in each of these scenarios will be considered in terms of speed and reversibility. The three categories of transactions that will be discussed are:

---

[1] In this context, new payment methods (NPMs) are defined as prepaid cards, mobile payments and Internet payment services. Internet payment services are defined as including digital/electronic currencies

[2] Paragraph 43, "Money Laundering Using New Payment Methods", FATF-GAFI, October 2010. (Source: http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20using%20New%20Payment%20Methods.pdf)

[3] https://bitcoin.org/en/you-need-to-know

[4] For example, http://lindenlab.com/tos.

1. Transferring from fiat currency to virtual currency (or vice versa)
2. Converting from one virtual currency to another
3. Transferring virtual currency from one account to another

3.1.1 Transferring from fiat currency to virtual currency

Generally speaking, transfers of fiat currency to virtual currency are performed in one of two ways:

- Some centralised virtual currencies can be purchased from or sold directly to the administrating authority[5]. In these cases, the terminology of purchasing/selling is sometimes referred to as depositing/withdrawing.
- Other centralised virtual currencies, and decentralised virtual currencies are typically acquired through the use of a virtual currency exchange.

As mentioned in Module 1, many possible funding sources can be used to acquire virtual currencies, including bank transfer, money remittance provider, payment card, cash and Internet payment services, such as PayPal. The clearing cycles (including speed and reversibility of transfers) varies by funding source and a full discussion is beyond the scope of this course.

3.1.2 Converting from one virtual currency to another

From the perspective of virtual currency exchanges, conversion from one virtual currency to another is a special case of buying/selling virtual currency. Using a virtual currency as a funding source to purchase other virtual currencies is supported by some currency exchanges[6], [7], [8].

In most cases, delays in transferring virtual currency are fraud prevention measures implemented by the virtual currency exchanges. These delays are often applied to new accounts or funding sources and are relaxed or removed after multiple transactions have been performed and the customer has built up a transaction history.

Depending on the particular virtual currencies concerned, and the nature of the transaction, instant transfers of virtual currency are possible. For example, it is possible to purchase Second Life Linden Dollars and have them instantly credited to your account[9].

[5] http://account.entropiauniverse.com/account/deposits/
[6] https://firstmetaexchange.com/home
[7] https://www.virwox.com/?stage=1
[8] http://howtobuybitcoins.info/
[9] The virwox exchange will instantly credit Linden Dollars to the specified virtual identity (avatar).

3.1.3 Transferring virtual currency from one account to another

The details of transferring virtual currency value from one account to another, of course depends on which virtual currency is being discussed. The speed of transaction confirmation varies depending on the particular virtual currency, but is generally in the range from instantaneous transfer to a delay of the order of minutes[10],[11].

For example, as mentioned above, decentralised virtual currency transactions (e.g. Bitcoin), once confirmed, are irreversible. The advantage of this for a legitimate user is that there is no possibility of having the transaction reversed ("charged back") due to fraud. From the criminal point of view, the non-reversible nature of the transaction means that there is no clearing cycle, or other opportunities within the payment system to recover the funds.

For these very same reasons (speed and irreversible transactions), Bitcoins have become an attractive payment method on the criminal underground[12], [13], [14].

Transfers of virtual currency between accounts in the case of centralised virtual currencies are also typically instantaneous. However, it is possible, in principle at least, for the administrating authority to reverse the transaction at some point in the future.

3.2 Anonymity by Design

This is a threat presented primarily by decentralised virtual currencies in particular. Some of these virtual currencies have been designed specifically to provide transactional anonymity. The canonical example of a decentralised virtual currency is Bitcoin, so they will be used as an example of the threat of transactional anonymity[15].

Recall that a publicly accessible ledger of all transactions is maintained by the Bitcoin network. Transactions are confirmed and added to this ledger through the Bitcoin mining process. Recall further that bitcoin ownership is represented by associating a particular amount of bitcoins with a particular address. The

[10] 10 minute transaction confirmation for Bitcoins (see Module 1)
[11] 2.5 minute transaction confirmation for LiteCoin (https://litecoin.org/)
[12] "Mind your wallet: why the underworld loves bitcoin", Reuters, March 2014. (Source: http://www.reuters.com/article/2014/03/14/us-bitcoin-criminals-insight-idUSBREA2D09820140314)
[13] "FBI Fears Bitcoin's Popularity with Criminals", Wired, September 2012. (Source: http://www.wired.com/2012/05/fbi-fears-bitcoin/)
[14] "What Bitcoins can buy you in the criminal underground", Cybercrime Review, May 2012. (Source: http://www.cybercrimereview.com/2012/05/what-bitcoins-can-buy-you-in-criminal.html)
[15] See Module 1 for a description of how Bitcoins work.

purpose of transactions in the Bitcoin network is to transfer ownership of a certain amount of bitcoins from one address to another. Each transaction, therefore, contains information about the source address, destination address and the amount of the transaction.

However, apart from the record of transactions that take place involving two particular Bitcoin addresses, there is no way to associate an address with any other address in the Bitcoin network. There is also no way within the Bitcoin network to associate an address with a real world identity. Indeed, a transaction where a single individual controls both the sender address and the destination address are indistinguishable from one where different people control the two addresses.

The implication of the anonymity offered by these decentralised virtual currencies is that even though it is not difficult to follow the flow of value being transferred through the Bitcoin network, understanding how this flow reflects transfers of real-world value between different parties is particularly challenging.

It may be possible, in some very limited circumstances, to associate transactions to or from a particular Bitcoin address with a particular IP address. However, traffic anonymising technologies can be used to make this more difficult[16].

By contrast, it is entirely possible that the administrating authority of centralised virtual currencies will retain information about virtual currency transactions, such as the funding source, the virtual currency account to which funds were transferred, records of transfers of virtual currency between accounts or conversion of virtual currency into fiat currency. This is particularly true in cases where the administrating authority is either directly exchanging fiat currency for virtual currency or brokering such exchanges. In most cases, however, the controls that virtual currency administrating authorities put in place are primarily fraud prevention measures, rather than anti-money-laundering measures. This issue will be discussed further in the next section.

3.3 Inadequate Transaction Records

As mentioned in the previous section, it is possible that the administrating authority of centralised virtual currencies will retain information about transactions. This may include information such as contact details for customers, funding sources, records of transfers of fiat currency into virtual currency, records of transfers of virtual currency value between accounts, records of transfers of virtual currency into fiat currency or other virtual currencies.

[16] https://www.torproject.org/

However, the absence of a regulatory obligation on administrators of virtual currencies, as part of a comprehensive regulatory framework for virtual currencies, means that the administrating authorities and currency exchanges dealing in virtual currencies may not keep records that would typically be retained by traditional financial institutions.

Indeed, there have been instances in the past where virtual currency exchanges have not required any form of real-world identification of their customers. For example, Liberty Reserve, which was shut down by the US Department of Justice in May 2013, ostensibly required basic identifying information. However, it did not validate identities. Users routinely established accounts under false names, including blatantly criminal names ("Russia Hackers", "Hacker Account", "Joe Bogus") and blatantly false addresses ("123 Fake Main Street, Completely Made Up City, New York"). Liberty Reserve further required users to make deposits and withdrawals through particular third-party exchangers, generally either unlicensed or in parts of the world with weak money-laundering oversight or regulation regimes. By avoiding direct deposits and withdrawals from users, Liberty Reserve managed to not collect information about them through banking transactions or other funding activity[17].

Even in cases where there is not deliberate efforts made to make transactions anonymous in this way, the lack of a regulatory requirement to retain records means that the administrating authorities and exchanges may not keep information that would be vital to an investigation. In particular, information on funding sources, transaction records and customer due diligence records may only be retained for as long as the information is required commercially, if it is gathered at all. Retention periods may therefore not be adequate for investigative purposes, particularly cross-jurisdictional investigations.

Additionally, given the lack of regulation, there may be no obligation on the administrating authorities/virtual currency exchanges to report suspicious transactions.

3.4 Identifying that Virtual Currencies Have Been Used

The relative obscurity of virtual currencies (relative to cash, payment cards or even other forms of online payment) may present a challenge to identifying that virtual currencies have been used to launder funds.

Knowing that suspects may have used virtual currencies to launder crime proceeds requires awareness on the part of the investigating authorities of the

[17] "Manhattan U.S. Attorney Announces Charges Against Liberty Reserve, One of World's Largest Digital Currency Companies, And Seven Of Its Principals And Employees For Allegedly Running A $6 Billion Money Laundering Scheme", US Department of Justice, May 2013. (Source: http://www.justice.gov/usao/nys/pressreleases/May13/LibertyReservePR.php?print=1)

capabilities of virtual currencies, as well as the technical capacity to gather the required evidence. The investigative tools, such as red flags/indicators can be of assistance in helping to identify the use of virtual currencies.

Further, an appropriate legal basis for the detection of laundering funds through virtual currencies must also be available.

3.5 Complex/Obfuscated Transaction Patterns

The dissociation of virtual currency accounts from real-world identities, combined with the ability for an individual to create an arbitrary number of accounts enables the development of novel, complex layering transaction patterns.

Consider, for example, the fact that any Bitcoin user can create any number of addresses that they want. Transactions between two addresses, both of which are controlled by the same individual are indistinguishable from transactions where different individuals control the two addresses. Therefore, it is possible in principle for someone to create, for example, 100,000 Bitcoin transactions between addresses they control before converting the bitcoins into another form. Reassembling such a chain of transactions, particularly if it needs to be done manually, would be at least very time consuming, if not impossible. Such a technique may form part of a complex laundering technique involving multiple individuals, virtual currencies and so on.

As well as the primary trade in virtual currencies that takes place with administrating authorities or virtual currencies exchanges, secondary trade in virtual currencies, such as the use of online auction sites or other trading forums, also creates opportunities for increasing the complexity of transaction patterns.

3.6 No Funding Limits

In the case of centralised virtual currencies, the administrating authorities may introduce funding limits, but these are typically a fraud management measure[18]. Similarly, virtual currency exchanges may have funding limits for newly established accounts but again these are typically for the purposes of fraud management.

Arbitrary amounts of money can be transferred without limit or oversight using decentralised virtual currencies. With Bitcoin, for example, the amount of a transaction makes no difference to the technique used to execute the transaction. As long as the holder of a certain Bitcoin address can prove

[18] https://secondlife.com/my/lindex/describe-limits.php (Requires logging in with a Second Life account).

ownership of a certain number of bitcoins, they can transfer all of that value to one or more other Bitcoin addresses, irrespective of the amount of bitcoins involved.

4 Typologies

Having discussed in the previous section the threats that virtual currencies present to detection and investigation of laundering crime proceeds, this section examines some of the techniques used by criminals to exploit these threats. Two important typology studies have been carried out that have gathered case studies and typology reports from FIUs in various jurisdictions. These are:

1. "Money Laundering Using New Payment Methods", published by the FATF in October 2010[19] (Referenced to below as FATF-NPM).
2. "Criminal money flows on the Internet: methods, trends and multi-stakeholder counteraction", published by the Council of Europe Global Project on Cybercrime and MONEYVAL in March 2012[20] (Referenced below as COE-CMF).

This section is an analysis of these two sources, focussing on the typologies discussed therein. The case studies provided in this section are primarily drawn from these two documents.

4.1 The Use of Virtual Currencies

The definitions of digital/electronic currency used in the COE-CMF report differ from the ones being used here. The definition of digital/electronic currency used there is:

"Digital or electronic currencies refer to a value exchange system that operates electronically. Electronic currency is encrypted code representing the value attacked to the certain "account", just as regular banknotes are a piece of paper carrying certain characteristics that transform it in a symbol of value."[21]

Even though this definition is different to the ones being used in this study, it is clear that the phenomenon being referred to is the same one. Therefore, to a first approximation, we can say that "Digital/electronic currency" in COE-CMF refers to "digital currency" as per the definitions in Module 1. Recall that "Digital currency", as defined in Module 1, is a term that encompasses both "virtual currencies" and "electronic money".

---

[19] "Money Laundering Using New Payment Methods", FATF-GAFI, October 2010. (Source: http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20using%20New%20Payment%20Methods.pdf)

[20] "Criminal money flows on the Internet: methods, trends and multi-stakeholder counteraction.", Council of Europe Global Project on Cybercrime and MONEYVAL, March 2012. (Source: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/reports-presentations/MONEYVAL_2012_6_Reptyp_flows_en.pdf)

[21] COE-CMF, Section 3.1.7, Paragraph 181.

As mentioned in Section 3 above, the fast, irreversible and anonymous nature of virtual currencies make them an attractive laundering technique for criminals. This was highlighted as follows:

"Cyber criminals and money launderers tend to use systems such as digital or electronic currency which afford varying degrees of anonymity depending upon the issuer, and typically afford them instant clearing and little or no chance of reversed charges. Some of the systems historically used by the criminal underground include, but are not limited to, e-Gold, WebMoney.ru, Liberty Dollar, Pecunix, Liberty Reserve, Fethard and E-Bullion."[22]

The same point is made in FATF-NPM as follows:

"Anonymity, high negotiability and utility of funds as well as global access to cash through ATMs are some of the major factors that can add to the attractiveness of NPMs for money launderers. Anonymity can be reached either "directly" by making use of truly anonymous products (i.e., without any customer identification) or "indirectly" by abusing personalised products (i.e., circumvention of verification measures by using fake or stolen identities, or using strawmen or nominees etc.)."[23]

New Payment Methods (NPMs) are defined as prepaid cards, mobile payments and Internet payment services. Internet payment services are defined as including digital/electronic currencies[24]. Once again, it is clear from this document that the phenomenon being referred to is the same as the one defined by the term "virtual currency" in this study.

Notwithstanding any differences in terminology that may be present, multiple case studies involving the use of virtual currencies to launder crime proceeds are provided in the two referenced typology studies. These will be discussed in the following sections.

4.2 Administrating Authorities and Currency Exchangers

Virtual currency administrators and exchanges are regulated to varying degrees in different jurisdictions. Considering the inherently international nature of virtual currencies, this presents a challenge from the perspective of detection and investigation of crime proceeds. This issue is highlighted at several locations in COE-CMF. For example:

[22] Reported by the USA in COE-CMF (Paragraph 186).
[23] FATF-NPM, Executive Summary, Paragraph 5
[24] FATF-NPM, Section 2.2, Paragraphs 43-45.

"Numerous responding jurisdictions indicated that Internet based payment service providers are insufficiently regulated and supervised with regards to AML/CFT obligations. Weak or non-existent regulatory controls in the operating environment is a key risk factor for both institutions and jurisdictions, coupled with non-existent or inadequate sanctioning regimes.

One of the difficulties in licensing and supervising those entities resides in the fact that often the jurisdiction of registration is different from the jurisdiction of operation. In some cases even the lack of specific legal provisions directed to such payment services suppliers could be an issue."[25]

Another typology highlighted in FATF-NPM related to the administrating authorities and currency exchangers is the issue of complicit providers or their employees.

"A number of submitted cases feature prepaid card and IPS[26] *providers or their employees, which are controlled by criminals and wilfully or recklessly assisting money laundering and terrorist financing activities. In such cases, market entry restrictions such as fit and proper tests have failed or are not applicable to the respective entity under that jurisdiction."*[27]

A case study of a complicit currency exchange was also cited. This case study is reproduced below.

Finally, COE-CMF draws specific attention to the fact that virtual currency exchanges, particularly those that offer the service of converting from one virtual currency to another, are a particular risk:

"The easy conversion to various virtual currencies and accounts by so-called "exchangers" offers an effective opportunity to criminals to conceal illegal funds."[28]

In summary, the following bullet points highlight the typologies associated with virtual currency administrating authorities and currency exchanges:

1. Legally or commercially structuring the administrating authority or currency exchange to exploit poor regulatory regimes.
2. Service providers or their employees being complicit in the laundering.
3. Converting between virtual currencies at a virtual currency exchange.

[25] COE-CMF, Section 2.4.3, Paragraphs 118-119. Also see Section 2.4.4.
[26] Internet Payment Service
[27] FATF-NPM, Section 4.3, Paragraph 130.
[28] COE-CMF, Paragraph 187 (Reported by Germany)

Case Study: Complicit Providers or Their Employees

"Case 33: Money laundering through a digital precious metals provider.

In 2008, an Internet-based digital currency business, and its three principal directors and owners, pleaded guilty to criminal charges relating to money laundering and the operation of an illegal money transmitting business.

Several characteristics of the digital currency business operation made it attractive to users engaged in criminal activity, such as not requiring users to provide their true identity, or any specific identity. The digital currency business operation continued to allow accounts to be opened without verification of user identity, despite knowing that the business was being used for criminal activity, including child exploitation, investment scams, credit card fraud, money laundering and identity theft. In addition, the digital currency business assigned employees with no prior relevant experience to monitor hundreds of thousands of accounts for criminal activity. They also participated in designing a system that expressly encouraged users whose criminal activity had been discovered to transfer their criminal proceeds among other accounts of said digital currency business. Unlike other IPS providers, the digital currency business operation did not include any statement in its user agreement prohibiting the use of its services for criminal activity.

Source: United States."[29]

4.3 Third Party Funding

Both FATF-NPM and COE-CMF discuss the fact that the availability of person-to-person transfers as a funding source for virtual currency purchases may allow complicit third parties to fund virtual currency accounts for the purposes of laundering crime proceeds.

COE-CMF has a lengthy discussion on the use of money mules to facilitate laundering of crime proceeds on the Internet. The use of money mules is summarised as follows:

"Mules receive in the bank accounts funds from, for example, a compromised online bank accounts [sic] and can either forward the funds to other accounts or withdraw the funds as cash and subsequently using another means such as a money transmission system or digital currency. The mule keeps a commission as part of the transaction."[30]

[29] FATF-NPM, Page 45.
[30] COE-CMF, Section 3.1.5, Paragraph 168.

Note that COE-CMF highlights in particular the fact that funds being handled by the mule may be used as a funding source for virtual currency.

The third parties may either be willing participants in the laundering or may have been unknowingly tricked into acting as a mule. A common technique to recruit unknowing money mules is through the advertising of fake employment positions on recruitment websites. These positions often define roles using terms such as “financial manager” or “work at home”.

Case Study: Digital Currency Laundering by Nominee

“Case 11: Use of digital currency account to facilitate Internet fraud and money laundering

A young person, acting as a nominee, opened a digital currency account to enable him to receive the proceeds of Internet banking thefts from an offshore associate. He then attempted to redeem the value of the digital currency account by requesting the digital currency exchanger to provide him with postal money orders. In an effort to conceal his identity he informed the cash dealer that he had lost his passport and requested that the exchanger call a money service business and inform them that a person matching his description would present himself to collect the money orders at a particular time. It is believed that he was not going to send money offshore but would keep the proceeds for himself. He has been arrested and prosecuted.

Source: Australia.”[31]

Case Study: Online Banking Fraud with Laundering Involving Mules and Virtual Currencies

“A bank offers online banking services to their customers, so that they can manage and make transfers from their homes via computers. Some customers had their account “hacked” and money was transferred from their account to accounts in other countries. The computers of the victims had been infected with malware which allowed the theft of account credential and other personal information (probably as part of a botnet). The international investigation conducted in the involved countries revealed a large and complex

[31] FATF-NPM, Page 39.

system of money mules spanning at least ten countries and large amounts of stolen money.

Mules were recruited via spam in different languages offering easy gain of money. Those who responded were contacted by telephone via Voice-over-Internet-Protocol (VOIP) which is difficult to intercept and for which bills had been paid with skimmed credit or stolen debit cards. The "first level" mules were asked to open a bank account. Within a few days they received money on this account. They were contacted again and instructed to withdraw the money and transfer it via money remittance providers to a given address in Eastern Europe jurisdictions. In Belgium, this breaking of the paper trail is considered money laundering.

The "second level" mules, in this case most of them located in Eastern European jurisdictions, withdraw the money and give it in cash to a third person, the "money collector". Neither the first nor the second level mules know any details about the origin of the money. The money collector is electronically informed about the amount to be received, the transaction code of the money remittance provider, and of the name and address of the first and second level mules. The money collector transfers the money to a fourth person, the e-banker, who converts it to WebMoney.

In the case investigated, the money collector received US$ 150,000 within two months.

All these processes appear to be very well organised and automatically followed up, so it can be assumed that the organisation involves a central data manager or similar.

Source: Belgium"[32]

4.4 Exploitation of the Non-face-to-face Nature of Virtual Currencies

Most involvement with virtual currencies involves minimal, or zero, face-to-face contact. This can give rise to situations where the virtual currencies can be abused by criminals for money-laundering purposes.

One category of exploitation that can take place involves the scenario where criminals gain control of the accounts of legitimate users and perform transactions. FATF-NPM contains two distinct cases where this is reported to take place:

[32] COE-CMF, Page 49.

- The first case is where non-virtual currency accounts of legitimate customers are compromised, money is stolen and used to fund virtual currency accounts, reported as follows:

  "In a number of cases NPM products were used to launder illicit proceeds gained from fraud following identity theft or from stealing money from bank accounts or credit/debit cards using computer hacking or phishing methods. Since the bank accounts or credit and debit cards were held in the names of legitimate customers, the criminals were able to use them as reference accounts for the funding of prepaid cards or IPS accounts. In such instances, the NPM providers could not detect that the transactions were actually not initiated by their legitimate customer, or detect any other suspicious activity."[33]

- The second case is where the identities of legitimate customers are compromised and used to create virtual currency accounts, which are then used as transit accounts to launder illegal proceeds. This is reported as follows:

  "In other cases, stolen or fake identities were used to create NPM accounts which were also used as transit accounts in the laundering of illegal proceeds, or to commit both criminal activities (e.g. fraud) and money laundering at the same time."[34]

The second category of exploitation of the non-face-to-face nature of NPM accounts revolves around the exploitation of the anonymous nature of some of these services. This is highlighted as an issue in COE-CMF as follows:

"In some jurisdictions e-money payment services can be used anonymously. It should also be noted that e-money circulates outside banks and, as such, outside the bank supervision system. Banks serve as agents, letting the money in or out of the e-payment systems, and in certain cases – as "issuers"/emitters of e-money."[35]

Contrary to the specific point made in COE-CMF, there appears to be very limited evidence of engagement between financial institutions and virtual currencies[36]. In fact, an increasing number of central banks are warning against their use[37]. The use of e-money (digital representations of fiat currency), as

[33] FATF-NPM, Section 4.2, Paragraph 126
[34] FATF-NPM, Section 4.2, Paragraph 127
[35] Reported by Russian Federation in COE-CMF, Paragraph 189
[36] "Bitcoin exchange gains clearance to operate as a real bank in France", The Verge, December 2012. (Source: http://www.theverge.com/2012/12/7/3740136/bitcoin-exchange-bank-france-bitcoin-central).
[37] http://www.virtualcurrencyreport.com/files/2014/03/Virtual-Currencies_International-

opposed to virtual currencies, is of course increasingly common but this form of digital currency would fall within the formal financial supervision system.

To summarise, the typologies associated with the non-face-to-face nature of virtual currencies can be categorised as follows:

1. Exploitation of the inherently anonymous nature of some virtual currencies. Decentralised virtual currencies such as Bitcoin have a high degree of inherent anonymity. This is based primarily on the fact that there is no association between a Bitcoin address and a real-world identity.

2. Exploitation of the ability to anonymously fund virtual currency accounts. Both centralised and decentralised virtual currencies may be anonymously funded, due to both the non-face-to-face nature of the relationship (discussed in this section) as well as the risk of funding by third party sources (discussed in Section 4.3).

Case Study 1

"The Ministry of the Interior received information from WM Transfer company that an unidentified user of their system violated the contract with the administrators of system and committed stealing of funds to the amount of $60 000 from the company's account, and opened in US payment system E-GOLD. The offender replenished the account of a credit card using the WM Transfer payment system service, and then cashed in the money.

Law enforcement agencies detained an individual who attempted to receive money of the amount of $14 000 in a bank, illegally using the passport and payment card of another person. The passport, sim-cards for mobile phone and bank payment card were confiscated. An IP address was identified, through which an illegal access to Internet and use of computer equipment were conducted. The equipment was used with a purpose to appropriate one's property (title marks of "exchange office" purse) involving fraud.

As a result of the investigation, the Ministry of Interior initiated a criminal case under Article 361, Chapter 2 of the Criminal Code. Two individuals were apprehended: a person of Caucasian region, who organized the withdrawal of money through the ATM network using counterfeit and lost passports of citizens of Ukraine; and another person, who was convicted for a term of 3,5 years for committing an analogical offense and was released due to the

probation period. The criminal case with indictment was forwarded to court.

Source: Ukraine"[38]

Case Study 2

"Case 25: Laundering of illicit proceeds through a digital currency provider.

In 2009, the suspect illegally accessed individual's Internet banking accounts and instructed the computer system to remit about JPY 740 000 (USD 8 300) to a digital currency exchanger to get e-currency units. Then, the suspect sold off a portion of the e-currency units to another digital currency exchanger to get real money. Finally the suspect made the digital currency exchanger deposit the money into some bank accounts that were acquired illegally and controlled by him.

Source: Japan."[39]

4.5 Relationship to Other Laundering Methods

Following on from the previous point, virtual currencies can be used in combination with other payment technologies, particularly the use of prepaid cards as a funding source, to incorporate multiple laundering methodologies into the process of laundering crime proceeds. This is particularly highlighted in FATF-NPM as follows:

*"**Internet payment services are increasingly interconnected with different new and traditional payment services.** Funds can now be moved to or from a variety of payment methods, ranging from cash, money remittance businesses (e.g. Western Union), NPMs, bank wire transfers, and credit cards. Furthermore, some IPS providers have started to issue prepaid cards to the customers, this granting them access to **cash withdrawal through the worldwide ATM networks**."*[40] [emphasis shown is present in the source document].

The same issue is addressed in COE-CMF:

[38] COE-CMF, Page 52
[39] FATF-NPM, Page 43.
[40] FATF-NPM, Section 2.2, Paragraph 47

"Unlike traditional money laundering schemes involving the use of the banking system, cyber laundering relies on various types of operations and financial services providers, ranging from bank transfers, cash withdrawals/deposits, the using e-currencies to money mules and money remitting services. Therefore, the detection and pursuit of the criminal money flows is much more difficult for law enforcement agencies.

Often the chain is "broken" by cash operations performed traditionally by money mules followed sometimes by the use of a traditional payment service. If the respective payment service is integrated with the Internet payment service provider, then the money could immediately be exchanged into e-currency ant [sic] transferred almost anonymously to other country."[41]

To highlight this point, several additional case studies are reproduced in the following sections where multiple laundering techniques, including virtual currencies, are used to create complex laundering schemes.

Case Study 1

"Case 30: Suspected use of IPS (including digital precious metals) and open-loop prepaid cards to launder proceeds of fraud schemes.

This case was initiated following the receipt of information from law enforcement and a foreign financial intelligence unit (FIU) which indicated that a Canadian IPS provider, its subsidiary in the United States and other associated entities were suspected of laundering illicit proceeds derived from pyramid schemes (Ponzi schemes) and telemarketing fraud schemes.

It was revealed that the Canadian IPS also had subsidiaries in a European and an Asian country. In addition it was found that at least five digital currency exchanges (located in Canada, the United States and a Northern European country), two digital precious metal providers (United States), three open-loop prepaid cards providers (in Canada and the United States) were knowingly or unknowingly used in this complex money laundering scheme. One of the prepaid card providers was found to have offered its product for the use of a virtual world's gamers who could fund their virtual world accounts and withdraw their virtual currencies into real currencies directly at ATMs.

Generally, funds sent from foreign countries to Canadian bank accounts held by the Canadian IPS and prepaid card providers were either used to load prepaid cards or to settle accounts with other IPS or prepaid card providers located in other countries. In some instances, suspicious funds entered the financial

[41] COE-CMF, Section 2.4.5, Paragraphs 130-131

system in Canada and appeared to be then layered through other countries, sometimes coming back to Canada.

Suspicious transactions included large deposits of cash and bank drafts often followed by international electronic funds transfers (EFTs) and the layering of illicit funds through EFTs sent between various bank accounts.

Source: Canada."[42]

Case Study 2

"Case 31: Laundering of illicit funds through digital currency and prepaid cards

Within the scope of an investigation, an international group of offenders transferred illegally-obtained money through a financial service provider to Eastern European countries, where it was withdrawn by members of the group and converted into electronic currency through digital currency exchangers.

The digital currency was then transferred to accounts held by offenders with a financial service provider handling electronic currency in the countries involved. In co-operation with a bank located in an offshore region this financial service provider issued MasterCard "Cirrus-cards" (prepaid cards), which were acquired anonymously and loaded with electronic currency. The cards could be used worldwide in payment transactions at points-of-sale (POS) and cash dispensers which accept "Cirrus".

In this way, the flow of illegally obtained money was effectively concealed, and the offenders were able to access the secure illicit money promptly and anonymously.

Source: Germany."[43]

[42] FATF-NPM, Pages 44-45.
[43] FATF-NPM, Page 45.

5 Investigative Challenges

The previous sections discussed the threats presented by virtual currencies and examined some techniques used by criminals to exploit these threats to launder crime proceeds. The detection and investigation of laundering of crime proceeds using virtual currencies presents some unique challenges, and in this section, these challenges will be highlighted.

5.1 Lack of Knowledge

There is limited awareness among investigators and prosecutors of the existence and capabilities of virtual currencies, as well as the tools and techniques to effectively perform investigations involving virtual currencies.

Further, considering the relatively novel nature of these currencies, there are very few individuals with experience dealing with virtual currency investigations.

Challenges related to the availability of training in the appropriate topics, as well as how to integrate such training into the careers of the relevant professions, have also been highlighted previously[44].

This manual is intended, in part, to address this lack of training material.

5.2 Reliance on Electronic Evidence

The core enabler for the use of virtual currencies is information and communications technology. Virtual currencies operate primarily in the online environment; all such transactions, at some point, involve computer systems and data. There is virtually no paper trail available, except for a limited set of operations that involve exchange of virtual currency into fiat money, or vice versa, and relevance of such paper trail in terms of virtual currency-related investigations is similarly limited. Therefore, in terms of illegal use of virtual currencies, evidence of crime will be almost exclusively in the form of electronic evidence, which is an important concept for law enforcement and financial intelligence units alike.

Electronic evidence is information generated, stored or transmitted using electronic devices that may be relied upon in court.[45] In contrast to traditional

[44] See, for instance, "Cybercrime training for judges and prosecutors: a concept", Council of Europe, October 2009. (Source: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Training/2079_train_concept_4_provisional_8oct09.pdf)

[45] UNODC Comprehensive Study on Cybercrime, pp. 157 et seqq. See also, "Electronic Evidence Guide: A basic guide for police officers, prosecutors and judges," produced

forms of evidence that are routinely introduced in criminal proceedings, such as documents, photographs, witness statements and so on, electronic evidence is sourced from computer systems and their peripheral devices. Such systems and devices may be vastly different in terms of technology and operation, including computer networks, mobile phones, digital cameras, data storage devices, cloud storage, and Internet as such – these all create, process and store information that can be used as electronic evidence.

In terms of evidentiary challenges, electronic evidence in general is not different from other, traditional forms of evidence, that is has to be authentic, admissible and relevant to the case. However, electronic evidence possesses some unique characteristics that distinguish it from other forms of evidence, and those are extremely relevant in the context of investigation of virtual currency-related offences:

Difficult traceability: Electronic evidence is often found in places where only specialists would search or locations reachable only by means of very specific tools. Digital forensics of electronic evidence requires specific tools that are tailored not only as to production of expert reports of already secured evidence, but also those that are geared toward examination and analysis of raw, unsorted and seemingly unconnected data found in computer systems;

Necessity for specialist insight: Without necessary expert knowledge and experience, information found in computer systems may be impossible to extract in a manner that ensures that the relevant information is truthful and has not been manipulated or tampered with. Specialist insight is also necessary to identify and properly process related evidence that may be relevant to investigation. In virtual currency investigations environment, this also has additional implication that knowledge of finance, taxation and/or money-laundering techniques and practices is highly important;

High volatility: Computer systems that create, process and store electronic evidence routinely destroy existing data every time a specific event happens, for example, an automated update system overwrites old information in order to leave spaces to store new information. Therefore, the challenge is to properly secure the devices on which electronic evidence might be stored in a timely manner before crucial data is lost;

Susceptibility to alteration: Computer systems and devices constantly change the state of their memories, be it on user request (e.g. saving, copying, updating operations) or automatically by the computer operating system (allocation of space, temporary storage of information for swapping, planned update process,

by EU/COE Joint Project on Regional Cooperation against Cybercrime, p. 11 (Source: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Electronic%20Evidence%20Guide/default_en.asp)

etc). This characteristic is important for understating of the temporal limitations and states of electronic evidence, and for ability to handle such evidence in an appropriate way from the moment it is identified, as relevant for an investigation;

Unlimited copying: digital information can be copied indefinitely and each copy will be a precise, flawless copy of the original. This unique attribute is a challenge in terms of initial positioning, where court or other party may request the original evidence as authentic. However, once the concept of equality of the original and cope of the computer date – and resulting evidence – is properly established, this challenge can turn into an advantage, which allows multiple, exact copies of the original to be distributed and analysed by different specialists at the same time, and to be presented as-is in a court along with the specialist witness report.[46]

The capacity to investigate cases involving virtual currencies will therefore depend on the availability of specialised units to gather and analyse the electronic evidence. Selection of appropriate staff, maintaining an appropriate level of expertise through training of staff and investment in equipment and other resources are highlighted as three key issues in enhancing the capability of such a specialised unit[47].

5.3 Legislative Loopholes

One has to argue that the biggest legislative loophole in terms of virtual currency-related offences is the lack of regulation and directly applicable laws. This section of the manual, however, is not intended to address issues of regulation, as already discussed in Module 1 of this manual; nor does it address the available substantive and procedural tools and regulations for investigating virtual currency-related offences, which is a subject of Module 3 of this manual. Rather, it is important to focus on the matters that relate to the rules of evidence in the context of securing and processing electronic evidence.

First of all, the challenge is the general availability and practical application of the concept of electronic evidence in national criminal justice systems. A preferred approach, of course, is to guarantee the recognition and applicability of electronic evidence in criminal proceedings by specialized definitions in criminal procedure legislation. For the most of the cases, however, the legal practitioners have to ensure that electronic evidence is properly recognized in

[46] Electronic Evidence Guide, pp. 11-12.
[47] Sections 6.4, 6.5 and 6.6 of "Specialised cybercrime units – good practice study". Council of Europe, CyberCrime@IPA project report. (Source: http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/Octopus2011/2467_HTCU_study_V30_9Nov11.pdf)

the national criminal justice system by an analogy, i.e. within the overarching concept of "documents" or "information", and is admissible in criminal proceedings based on the same standards and procedures (rules of evidence) as are applicable to other, established an recognised forms of evidence.

Furthermore, one of the important and often neglected aspects of admissibility of electronic evidence lies beyond criminal law and procedure framework and is generally related to recognition of electronic documents as legitimate sources of data and evidence. However, internationally accepted standards relating to electronic documents often require qualified electronic signatures so that signed documents can have equal legal standing to physical, paper-based documents in official proceedings,[48] which may lead to additional admissibility requirements that may prove difficult to prove in courts of law. In essence, there should be consideration by the investigators and prosecutors involved in investigation of criminal use of virtual currencies as to admissibility of electronic documents in criminal proceedings, from the perspectives of format, content or level of national regulation, as valid electronic evidence.

The concept of electronic documents is particularly important in financial investigations involving virtual currencies, since many of the leads and materials that may not be introduced into evidence later (for strategic or procedural purposes), but could have been or will be used for financial or criminal intelligence, may be in the format that is different from accepted format of officially recognised documents. Such concerns can potentially be used by the defence in criminal cases to undermine the evidentiary weight of introduced evidence.

Last but not least, electronic evidence, similar to traditional categories of evidence, shall not be subject to changes, deletions, additions or other alterations that have a significant impact on the form and content of such evidence. However, the very nature of data and information held in electronic form makes it easier to manipulate than traditional forms of data. This creates specific issues for the justice system and requires that the handling of such data is carried out in a manner that ensures the continued integrity of the information may be maintained and proved.[49] In this respect, the challenge of electronic evidence in virtual currency-related investigations is the compliance with the official standards of proof. In particular, standards of proof in criminal cases are often constructed in a manner that relies heavily on traditional evidence, while high volatility and possibilities of alteration of electronic evidence have impact on the compliance of such evidence even for the lowest standards of proof ("reasonable doubt", "reasonable suspicion" or "probable

[48] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures (Source: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:31999L0093)

[49] Electronic Evidence Guide, pp. 10.11.

cause"). Law enforcement has to assume by default that the defence will be prepared to attack the admissibility of electronic evidence based on the standard of proof, and more so in case of decentralized virtual currencies that base their transactions on the anonymity of users. It has to be always kept in mind that any evidence, which can be potentially struck out of the case due to the lack of compliance with the standards of proof, may have detrimental effects for the entire case.

5.4 Regulatory/Supervisory Challenges

The requirement for financial institutions to be regulated for compliance to anti-money-laundering best practice is well understood and published. In particular:

"Other financial institutions should be licensed or registered and adequately regulated, and subject to supervision or monitoring for AML/CFT purposes, having regard to the risk of money laundering or terrorist financing in that sector. At a minimum, where financial institutions provide a service of money or value transfer, or of money or currency changing, they should be licensed or registered, and subject to effective systems of monitoring and ensuring compliance with national AMF/CFT requirements."[50]

By the definition used by the FATF, there is no doubt that centralised virtual currency providers fall within the definition of financial institutions[51]. On the other hand, the situation is much less clear in the case of decentralised virtual currencies. To use the terminology of the FATF definition above, there is no financial institution providing a service of money or value transfer, or of money or currency changing. Nevertheless, a service of value transfer exists (the Bitcoin network itself), supported by services of currency changing (provided by virtual currency exchanges that buy/sell bitcoins).

To further compound the problem, even if an appropriate legislative basis for regulation of decentralised virtual currencies exists, implementing supervisory or regulatory oversight of such currencies presents significant practical challenges due to the absence of any form of centralised administrating authority.

5.5 Prosecution and Adjudication of Offences

Challenges related to prosecution of virtual currency offences are not radically different from applicable investigative challenges, since all GUAM member

[50] Recommendation 26, "International standards on combating money laundering and the financing of terrorism & proliferation – The FATF Recommendations", FATF-GAFI.

[51] "Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services.", FATF-GAFI, June 2013. (Source: http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf)

states have criminal procedure systems in which prosecutors exercise guidance and supervision in all criminal investigations.[52] Therefore, all of the above challenges noted with relation to electronic evidence would be dealt with, depending on stage on the proceedings or the role specifically assigned by law, either by investigators or prosecutors. At the same time, some of the specific powers of prosecutors in national criminal justice systems warrant a closer look in terms of virtual currency-related offences.

The prosecutors are empowered by law and routinely use discretion in dealing with criminal cases.[53] Discretionary prosecution means application of public interest standards to specific criminal cases in order to decide on initiating or continuing prosecution or to divert the perpetrator into alternative solutions. This would be particularly relevant in cases that potentially involve money-laundering through the use of virtual currencies. Since most of the predicate or auxiliary offences in this regard could be cybercrime offences that are usually addressed by significantly lesser sentences than money-laundering offences, there is a bigger chance of termination of proceedings in exchange for alternative proceedings. In these situations, legal practitioners should have a view on the potential or existing evidence of money-laundering in order not to undermine prospective prosecutions in favour of alternative adjudications.

Prosecutors in increasing number of jurisdictions are empowered to enter into a plea agreement with the defendant.[54] Plea agreements are increasingly popular investigation and adjudication tools that allow defendant to receive expedited administration of justice with significantly reduced sentences or absolution of criminal responsibility through cooperation with investigation. There are similar concerns with plea agreements in the context of virtual currency-related investigations as there are for discretionary powers, that is, there can be instances where defendants plead guilty to lesser charges of cybercrime offences to avoid heavier money-laundering charges – and avoid seizure of crime proceeds, too. However, plea agreements can be very effective investigation tools, getting investigators access to information that would otherwise require time-consuming and expensive efforts to uncover relevant evidence.

Finally, the prosecutors have unique perspective on criminal proceedings in terms of ensuring efficiency though, if necessary, establishment of joint investigative teams comprising investigators and experts from various agencies and backgrounds. Although there are undeniable benefits from bringing

[52] Article 84 of the Criminal Procedure Code of Azerbaijan; Article 33 of the Criminal Procedure Code of Georgia; Article 52 of the Criminal Procedure Code of Moldova; Article 36 of the Criminal Procedure Code of Ukraine.
[53] E.g., Articles 16 and 166-168[2] of the Criminal Procedure Code of Georgia;
[54] E.g. Chapter XXI of the Criminal Procedure Code of Georgia; Chapter III of the Criminal Procedure Code of Moldova.

together financial and cybercrime experts and investigators for cases of money-laundering through the use of virtual currencies, a proper guidance may be necessary to ensure efficient investigation due to radically different techniques and methods used by relative professionals in securing and analyzing evidence.

In terms of judiciary challenges in criminal cases involving the use of virtual currencies, these are not entirely relevant from the perspective of the legal challenges as such. Mostly, these are more general concerns that relate to the proper understanding by the judges of cybercrime and electronic evidence, and the proper level of training and knowledge to deal with such cases.[55]

5.6 National Cooperation Issues

Throughout this manual, the express links between cybercrime and virtual currency related crimes are explored. In fact, given the unregulated status of virtual currencies in many jurisdictions, offences that involve or are predicate to their illegal use can often lead to undefined or competing investigative jurisdictions of several agencies, such as financial investigation, financial intelligence, and high technology/cybercrime units. For this reason, primary concerns that are relevant for combating cybercrime are similarly relevant for virtual currencies, one of such prime examples being cooperation on national and international levels.

National cooperation modalities are primary solutions for both crime intelligence as well as prosecution of offences involving information technology. Without proper cooperation, crime reporting, investigative actions, expertise, recovery of proceeds as well as harm mitigation and future prevention would have limited chances of success. At the same time, there are numerous potential partners in national criminal justice systems and beyond, whose functions and expertise are relevant in investigation of virtual currency-related offences.

The primary partners for law enforcement in detection and investigation of virtual currency-related crimes are financial intelligence units (FIUs). FIUs are specialized supervision agencies that receive reports of suspicious transactions from financial institutions and other persons and entities, analyze them, and disseminate the resulting intelligence to local law-enforcement agencies and foreign FIUs to combat money-laundering.[56], [57] The continuous focus of these

[55] Council of Europe, "Judicial training: Introductory course on cybercrime and electronic evidence for judges and prosecutors", pp. 5-6 (Source: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/basic%20training%20for%20judges/Cyber_JudTrain_Basic_course_Manual_V_1_0.pdf.)

[56] International Monetary Fund/World Bank, "Financial Intelligence Units: An Overview" (Source: http://www.imf.org/external/pubs/ft/FIU/fiu.pdf).

[57] Recommendation 29 of "International standards on combating money laundering and the financing of terrorism & proliferation – The FATF Recommendations", FATF-GAFI, February 2012. (Source: http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf)

agencies on money-laundering and their specialized and up-to-date knowledge of typologies and practices of money-laundering offences make them particularly valuable sources of information and expert partners in investigation of virtual currency-related offences. The other way around, in the face of constantly evolving methods and practices of money launderers, as well as emergence of new information technology solutions that facilitate commission of money-laundering through cybercrime, financial intelligence units, on their part, are in need of up-to-date knowledge and expertise of high-tech crime units or other investigative agencies that deal with cybercrime offences on a daily basis. However, the level of cooperation is far from desirable at the moment.[58]

The need for similar partnerships is also highly relevant within the law enforcement system, namely, cooperation between cybercrime units and financial crime investigators.[59] The primary challenge for such cooperation is that often criminal and financial investigators belong to different institutions in countries and utilize different methods for detection and investigation of offences involving use of information technology. This is highly relevant in terms of virtual currency-related investigations, since financial investigators often rely upon methods of criminal intelligence and investigation that are applicable to traditional, tangible forms of evidence, while cybercrime units are very well versed in dealing with electronic evidence. The cooperation can be also potentially beneficial due to unique expertise of financial investigators with relation to financial fraud, taxation and accounting offences, and knowledge of organized crime groups can be highly relevant criminal intelligence sources in investigations focusing on illegal use of virtual currencies.

In terms of criminal intelligence, there are increasing instances of cooperation between high tech/cybercrime units and national Computer Security Incident Response Teams (CSIRTs). CSIRTs are key specialist groups that are instrumental in protection of national critical information infrastructures through a variety of methods, mostly focusing on prevention, handling and mitigation of consequence of cyber-security incidents.[60] CSIRTs process enormous amount of data, received from national monitoring mechanisms as well as international databases (such as Shadowserver or Arbor Networks), about computer security incidents and vulnerabilities of computer systems. In the context of virtual currencies, CSIRTs can be engaged as expert knowledge partners in terms of analysis of malware, hacking tools and known vulnerabilities of computer systems, as well as sources of information about the

[58] Council of Europe/MONEYVAL, "Criminal money flows on the Internet: methods, trends and multi-stakeholder counteraction", p. 6.
[59] Council of Europe, "Strategic Priorities for the Cooperation against Cybercrime in the Eastern Partnership Region, Cybercrime@EaP Porject" (Source: http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/CyberCrime@EAP/2523_EAP_Strat_Priorities_V7%20ENG.pdf).
[60] http://www.enisa.europa.eu/activities/cert.

hacker community that can be active in cybercrime for economic benefit. However, many of law enforcement agencies are not aware of the existence of CSIRTs and their operations in their own countries.

There are some other challenges that relate public-private cooperation in the context of virtual currency-related investigations. The cooperation with Internet Service Providers, being a primary source of subscriber information, traffic data and other important electronic evidence, is often hampered by either legal (confidentiality of user data, lack of legal mechanisms for preservation of retention of data) or practical (unwillingness to cooperate with state authorities due to lack agreements/memoranda, costs of specialized equipment for preservation and/or retention, etc.) considerations. [61] Financial sector institutions, which may be primary source of information and evidence about financial transactions and money-laundering schemes, may be similarly unwilling to cooperate for privacy reasons or may not have full understanding of issues that involve information technology for the commission of virtual currency-related offences.[62] Consumer protection organizations that may be a source for crime reporting in terms of e-commerce related offences (financial fraud, including use of virtual currencies) may lack understanding of the potential of formal cooperation arrangements with law enforcement.[63] These and other instances of potential cooperation are discussed in more detail in Module 3 of this manual.

5.7 International Cooperation Issues

Continuing with the theme of close links between virtual currency–related offences and cybercrime, one of the most distinguishable features of these types of offences is their transnational nature, where the elements of crime, offenders, victims or evidence can be often scattered across various jurisdictions. Therefore, international cooperation in the investigation of money-laundering offences involving use of virtual currencies is often dependent on the availability and expediency of international cooperation mechanisms between investigative agencies and criminal justice institutions of respective jurisdictions.

However, such cooperation is challenging for a number of reasons, not the least of these being the general lack of regulation of virtual currencies. Where at the national level, analogies can be used to address money-laundering, fraud and cybercrime aspects of virtual currency-related offences, international cooperation is based on the framework of international agreements that put

[61] http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/lea_isp/default_EN.asp.
[62] Council of Europe/MONEYVAL, "Criminal money flows on the Internet: methods, trends and multi-stakeholder counteraction", p. 4.
[63] http://www.ftc.gov/enforcement/consumer-sentinel-network.

time and effort into developing stringent definitions to which international cooperation mechanisms must adhere. To put it differently, international cooperation is far more formalized than national cooperation modalities. Therefore, legal practitioners should take utmost consideration of these circumstances so that the lack of understanding or recognition is not detrimental to the expediency of such cooperation.

Another challenge is inherent in the nature of international cooperation, especially in its formal sense that involves Mutual Legal Assistance (MLA) or similar judicial proceedings in criminal cases.[64] MLAs, whether based on bi-lateral or multi-lateral treaties, usually require lengthy and complex procedures and formalities, and can be, for this very reason, frustratingly time-consuming in the context of virtual currency-related investigations, with their focus on electronic evidence which is highly volatile and susceptible to alteration in very short periods of time. These issues and other international cooperation modalities are discussed in more detail in Module 3 of this manual.

Similar challenges, although to a lesser extent, are relevant in the context of police-to-police cooperation modalities and investigative cooperation in advance of or beyond formal MLA procedures. While there are several cooperation mechanisms available under different treaties for cybercrime (24/7 points of contact under the Council of Europe Convention on Cybercrime,[65] Interpol contact points,[66] G8 Network of high-tech crime units[67]) and money-laundering (FIU-to-FIU cooperation), such cooperation modalities are often under-utilized due to lack of knowledge on the part of law enforcement or supervisory/regulatory authorities, or are, in many cases, inefficient in providing timely responses to law enforcement requests due to discretionary approaches in such cooperation.

In terms of public-private cooperation, there is also another, often neglected, form of international cooperation that is directed toward foreign companies (i.e. persons of private law), which may hold data that is relevant to the investigation of virtual currency related offences, such as social networks, communications companies that operate subsidiaries in the local market, e-mail providers and similar, often global players. Particular challenge in this regard is legally binding cooperation with parent companies of foreign origin: even if legal acts and regulations are perfectly applicable to locally-based companies, some of the important data may be directly processed and/or held by a parent company, or another entity operating in a different jurisdiction. Unsurprisingly, practice shows that foreign corporations are, unless bound by a formal

[64] UNODC Comprehensive Study on Cybercrime, pp. 185 et seqq.
[65] http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/points%20of%20contact/aboutpoc_EN.asp.
[66] http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime.
[67] http://www.oas.org/juridico/english/cyb_pry_G8_network.pdf.

agreement of cooperation, less willing to cooperate with foreign law enforcement than nationally incorporated companies.[68] Therefore, securing contacts and keeping in constant touch with any available local representations are going to be important factors when access to information and evidence is needed.

[68] "Law Enforcement Challenges in Transborder Acquisition of Electronic Evidence from "Cloud Computing Providers", discussion paper prepared for the Council of Europe (Source: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/reports-presentations/2079_reps_IF10_reps_joeschwerha1a.pdf).

6 Trends

The phenomenon of virtual currencies changes rapidly with some virtual currencies and virtual currency exchanges closing down, while new ones are starting up all of the time.

Virtual currencies have entered the awareness of the general public in a much bigger way since the emergence of Bitcoin in 2009. Bitcoin was not the first virtual currency, nor will it be the last.

The purpose of this section is to highlight some trends relating to the evolution of virtual currencies over the past years.

6.1 Increasing Number of Virtual Currencies

As mentioned in Module 1, one of the first popular virtual currencies, E-Gold, was established in 1996. E-Gold was a centralised virtual currency, along with practically all other virtual currencies for the next thirteen years. The business models of the various centralised virtual currencies differed but in all cases there was either a central administrating authority or a centralised virtual currency exchange.

The first cryptocurrency (Bitcoin) was established in 2009. The source code of Bitcoin was made freely available and therefore anyone can create a decentralised virtual currency either identical to, or based on, the Bitcoin model. In the period between 2009 and 2014, many other cryptocurrencies have been established. The following table shows, for example, the increasing number of notable cryptocurrencies over time[69]:

Year	Total Num. Cryptocurrencies	Names of Cryptocurrencies
2009	1	Bitcoin
2010	1	Bitcoin
2011	3	Bitcoin, Litecoin, Namecoin
2012	4	Bitcoin, Litecoin, Namecoin, Peercoin
2013	8	Bitcoin, Litecoin, Namecoin, Peercoin, Ripple, Dogecoin, Mastercoin, Primecoin
2014	12	Bitcoin, Litecoin, Namecoin, Peercoin, Ripple, Dogecoin, Mastercoin, Primecoin, Auroracoin, Vertcoin, MazaCoin, Coinye

There is limited information available about the number of virtual currencies of all types that exist. However, the following observations can be made:

[69] http://en.wikipedia.org/wiki/Cryptocurrency#Notable_cryptocurrencies

- Noting the trend highlighted in the table above, it is possible that over the coming years there will be an increasing number of decentralised virtual currencies created.
- The business model of non-convertible, centralised virtual currencies now has a number of well-established precedents (Second Life Linden Dollars, World of Warcraft Gold, Project Entropia Dollars). There is no reason to believe that other role-playing game owners or virtual world administrators will not establish virtual currencies in future.
- Amazon.com recently introduced a virtual currency known as Amazon Coins. These can be used to purchase in-app items, e-books and other items on the amazon.com website. Amazon Coins can also be transferred to other users of amazon.com[70]. It is not clear how this business model will evolve, but if it is successful for amazon, there is no reason to expect that other large marketplace websites will not adopt a similar approach.

6.2 Increasing Availability of Virtual Currencies

In order to purchase a virtual currency, all that is required is a funding source that is acceptable to a virtual currency exchange selling the virtual currency of interest. As mentioned in Module 1, virtual currency exchanges are available that accept a wide range of possible funding sources including other virtual currencies, bank transfers, money remittance providers, payment cards, cash and other Internet payment services such as PayPal. The increasing number of available funding sources means that an increasing number of people will have the option to acquire virtual currencies should they wish to.

Bitcoins, for example, are available for purchase in a wide array of countries. At the time of writing, list of virtual currency exchanges are available online to facilitate the purchase of bitcoins in 246 countries around the world[71], [72].

In fact, there are no inherent geographical limitations on the acquisition of any convertible virtual currency, once the anti-fraud requirements of the administrating authority or virtual currency exchange are satisfied.

6.3 Growing Complexity of Laundering Schemes

As mentioned in Section 3.5, the dissociation of virtual currency accounts from real-world identities, combined with the ability for an individual to create an arbitrary number of accounts enables the development of novel, complex layering transaction patterns.

[70] http://www.amazon.com/gp/feature.html?docId=1001166401
[71] http://howtobuybitcoins.info/
[72] http://planetbtc.com/complete-list-of-bitcoin-exchanges/

Virtual currencies therefore can act as an enabler for the creation of new laundering methodologies. It is reasonable to expect that criminals will continue to evolve their techniques for laundering crime proceeds using virtual currencies and other techniques. This is sure to involve the development of increasingly sophisticated transaction patterns, exploiting the threats and challenges highlighted in this module to conceal the source of funds.

6.4 Increasing Regulation of Virtual Currencies

As mentioned in Section 5.4, centralised administrators of virtual currencies and virtual currency exchanges may be regulated as financial institutions offering value transfer services. It is expected that the trend towards increasing regulation of these types of virtual currency providers will continue.

Several recent initiatives to increase the regulation of decentralised virtual currencies have recently been announced. To date, two approaches have emerged:

- Prohibit or restrict the use of decentralised virtual currencies[73]
- Regulate the virtual currency as a commodity[74], [75]
- Regulation of certain activities occurring within the virtual currency ecosystem, as noted above.

Once again, it is expected that the trend towards increasing regulation of decentralised virtual currencies will continue, particularly considering the risk of virtual currencies being used to launder crime proceeds[76].

[73] "China Banks Financial Companies From Bitcoin Transactions", Bloomberg, December 2013. (Source: http://www.bloomberg.com/news/2013-12-05/china-s-pboc-bans-financial-companies-from-bitcoin-transactions.html)
[74] "US tax man says bitcoin is property, not currency", FinExtra, March 2014. (Source: http://www.finextra.com/News/FullStory.aspx?newsitemid=25895)
[75] "Texas will not regulate virtual currencies like bitcoin as money", RT.com, April 2014. (Source: http://rt.com/business/texas-bitcoin-regulation-currency-257/)
[76] http://en.wikipedia.org/wiki/Legality_of_Bitcoins_by_country

Self Assessment

Question 1: Describe threats presented by virtual currencies that make them an attractive technique for laundering crime proceeds.

Question 2: In the context of virtual currencies, discuss how criminals exploit the non-face-to-face nature of virtual currencies to launder crime proceeds.

Question 3: Describe how the regulatory and supervisory challenges relating to the administrating authorities of centralised virtual currencies present risks of laundering.

Question 4: List investigative challenges presented by virtual currencies and discuss possible ways in which those investigative challenges can be addressed.

Question 5: List some specific features of electronic evidence that distinguish it from physical (traditional) evidence.

Question 6: What are the legal grounds for admissibility of electronic evidence in criminal cases in your country?

Question 7: Describe the concept of discretionary prosecution and its applicability for investigations involving virtual currency.

Question 8: Explain the benefits that law enforcement can potentially reap from cooperation with financial intelligence units.

Question 9: Provide a list of international police-to-police cooperation mechanisms that can be used in investigations involving virtual currencies.

Question 10: What trends are likely to influence the use of virtual currencies as a technique for laundering crime proceeds?

Basic Manual on the Detection And Investigation of the Laundering of Crime Proceeds Using Virtual Currencies

Module 3
Detection and Investigation of Laundering Crime Proceeds Using Virtual Currencies

1 Summary

The purpose of this module is to focus on the tools and techniques available to detect and investigate the laundering of crime proceeds through the use of virtual currencies. The module categorises the available tools and techniques into two broad groups: legislative tools and investigative tools. Both of these groups will be examined in detail in this module.

Towards the end of the module there is also a discussion on the possible countermeasures that can be put in place to help to enhance the ability of investigators to detect and respond to such laundering.

2 Learning Objectives

By reading this module you will:

- Know the relevant legislative tools available for investigation of laundering crime proceeds through virtual currencies.
- Be aware of investigative tools that can be used to assist with investigations of laundering crime proceeds through virtual currencies.
- Understand the possible investigative methodologies that may assist with investigations of laundering crime proceeds through virtual currencies.
- Know the countermeasures that are available to help prevent the laundering of crime proceeds through virtual currencies.

3 Legislative Tools

3.1 Substantive Law

One of the major goals of every criminal investigation is to provide a proper qualification of alleged criminal activities to corresponding provisions of substantive criminal law, i.e. to define the elements of crime. Although much of the current practice in this respect is shaped by many years of case law, some new forms of criminal activity – criminal use of virtual currencies being one such example – may call for the need to re-think and re-adjust currently available substantive criminal law options to real-life cases that are yet to be addressed comprehensively either by law or practice. Therefore, the purpose of this section is to provide various options that are available in substantive criminal law to address the elements of crime of money-laundering in the context of virtual currencies.

Before addressing the issues at hand, one has to bear in mind the current ambiguity of the status of virtual currencies, and, since the use of those is not expressly criminalized in any of the GUAM states (or any other state, for that matter), the use of virtual currency *per se* cannot be considered an offence in itself due to the principle of technological neutrality.

3.1.1 Money-laundering offences: relevant elements

Money-laundering refers to a financial transaction scheme that aims to conceal the identity, source, and destination of illicitly-obtained money. The reasons for offenders – whether they are drug traffickers, corporate embezzlers or corrupt public officials – to make use of these mechanisms is to conceal or disguise the illicit origin of the concerned property, or to help any person who is involved in the commission of the predicate offence to evade the legal consequences of his or her action, such concealment or disguise applied to the true nature, source, location, disposition, movement or ownership of or rights with respect to criminally obtained property.[1] In other words, criminals try to launder criminally derived funds in order to disguise evidence of their crimes and, secondly, to protect illegally obtained money from seizure. Criminals are increasingly taking advantage of the globalization of the world economy by transferring funds quickly across international borders with the use, among other options, of information and communications technology that allows money to move anywhere in the world with speed and ease. Regardless of who uses the apparatus of money-laundering, the operational principles are based on the same three-stage process:

[1] Article 6 of the United Nations Convention against Transnational Organized Crime.

The **placement** stage represents the initial entry of the funds into the financial system. Where large sums of money are involved, this could very well be an arduous task, especially if cash is being used.

After placement comes **layering**, which usually consists of a series of transactions designed to conceal the origin of the funds. This is the most complex stage of the process, and the most international in nature. The money launderer might begin by sending funds electronically from one country to another, then break them up into investments in advanced financial options or in overseas markets, moving them constantly to evade detection, each time hoping to exploit loopholes or discrepancies in legislation and delays in judicial or police cooperation.

The final stage of money-laundering is termed the **integration** stage because it is at this point that the funds return fully assimilated into the legal economy. Having been placed initially as cash and layered through a number of financial operations, the criminal proceeds are fully integrated into the financial system and can be used for any purpose.[2]

At the current state of affairs, the money-laundering agenda for illicit use of virtual currencies is becoming increasingly relevant in the light of real-life cases. While there are significant differences in terms of operation of centralized or decentralized virtual currencies, as illustrated perhaps most clearly by the cases of Silk Road and Liberty Reserve, the anonymity, traceability or reliance on cryptography of decentralized currencies can be attractive options for concealment of proceeds of crime.

Case Study: Liberty Reserve

In what is to date the largest online money-laundering case in history, in May 2013, the U.S. Department of Justice charged Liberty Reserve, a Costa Rica-based money transmitter, and seven of its principals and employees with operating an unregistered money transmitter business and money-laundering for facilitating the movement of more than $6 billion in illicit proceeds. In a coordinated action, the Department of the Treasury identified Liberty Reserve as a financial institution of primary money-laundering concern under Section 311 of the USA PATRIOT Act, effectively cutting it off from the U.S. financial system.

Established in 2006, Liberty Reserve was designed to avoid regulatory and law enforcement scrutiny and help criminals distribute, store, and launder

[2] Asian Development Bank, 'Manual on Countering Money-laundering and the Financing of Terrorism', p. 10-11 (Source: https://www.unodc.org/tldb/pdf/Asian-bank-guide.pdf).

the proceeds of credit card fraud, identity theft, investment fraud, computer hacking, narcotics trafficking, and child pornography by enabling them to conduct anonymous and untraceable financial transactions. Operating on an enormous scale, it had more than a million users worldwide, including more than 200,000 in the United States, and handled approximately 55 million transactions, almost all of which were illegal. It had its own virtual currency, Liberty Dollars (LR), but at each end, transfers were denominated and stored in fiat currency or gold.

To use LR currency, a user opened an account through the Liberty Reserve website. While Liberty Reserve ostensibly required basic identifying information, it did not validate identities. Users routinely established accounts under false names, including blatantly criminal names ("Hacker Account," "Joe Bogus") and blatantly false addresses ("123 Fake Main Street, Completely Made Up City, New York"). To add a further layer of anonymity, Liberty Reserve required users to make deposits and withdrawals through recommended third-party exchangers—generally, unlicensed money transmitting businesses operating in Russia, and other countries with weak governmental money-laundering oversight or regulation, such as Malaysia, Nigeria, and Vietnam. By avoiding direct deposits and withdrawals from users, Liberty Reserve evaded collecting information about them through banking transactions or other activity that would create a central paper trail. Once an account was established, a user could conduct transactions with other Liberty Reserve users by transferring LR from his or her account to other users, including front company "merchants" that accepted LR as payment. For an extra "privacy fee" (75 U.S. cents per transaction), users could hide their Liberty Reserve account numbers when transferring funds, making the transfers completely untraceable. After learning it was being investigated by U.S. law enforcement, Liberty Reserve pretended to shut down in Costa Rica but continued to operate through a set of shell companies, moving millions through their accounts in Australia, Cyprus, China, Hong Kong, Morocco, Russia, Spain, and elsewhere.[3]

3.1.2 Auxiliary or predicate offences of cybercrime

As noted in Section 7.2 of Module 1 of this Manual, cybercrime aspects of the misuse of virtual currencies can manifest themselves in a multitude of ways. Standalone offences of cybercrime that are connected, in one way or another, with virtual currencies, may not be, at a first glance, particularly relevant for the investigations focusing on laundering of crime proceeds. At the same time, even

[3] "Manhattan U.S. Attorney Announces Charges Against Liberty Reserve, One of World's Largest Digital Currency Companies, And Seven Of Its Principals And Employees For Allegedly Running A $6 Billion Money Laundering Scheme", US Department of Justice, May 2013. (Source: http://www.justice.gov/usao/nys/pressreleases/May13/LibertyReservePR.php?print=1)

standalone cybercrime offences against virtual currency systems can be often important sources of criminal intelligence that may lead to identification of money-laundering schemes.

A "predicate offence" is an offence whose proceeds may become the subject of any of the money-laundering offences.[4] Offences that involve money-laundering by use of virtual currencies may be connected to criminal proceeds derived from forms of cybercrime such as computer-related identity offences, or computer-related fraud or forgery. The status of an offence being predicate to a money-laundering offence varies by jurisdictions. Therefore, if allowed by legal regulations, cybercrime offences may be deemed as predicate offences to money-laundering; in this case, investigations will be relying on cybercrime elements of crime to construct the offence of money-laundering. In other perspective, in the context of virtual currencies, cybercrime offences, more often than not, will be auxiliary offences to money-laundering committed through the use of virtual currencies; therefore, investigation of such offences can have a direct relationship with the core charges of money-laundering, and provide important evidence for law enforcement in the prosecution of money-laundering offences involving the use of virtual currencies.

As described in Section 7.2 of Module 1, 'core' cybercrime offences against computer systems or data may also be auxiliary to a range of offences involving virtual currencies, such as when personal wallet is 'hacked', with a view to stealing bitcoins or when accounts of third parties are used without the consent of that person for transactions. As such, it is important to understand the nature of specific cybercrime offences, including illegal access; system interference; data interference; and misuse of devices. Practice shows that many of the potential cybercrime cases are not investigated properly due to the lack of understanding of what constitutes a cybercrime. Therefore, some important definitions are necessary in terms of their applicability and use for investigation of virtual currency-related offences: [5]

The offence of **illegal access** is the basic offence of threats to and attacks against the security (i.e. the confidentiality, integrity and availability) of computer systems and data; in other words, this denotes basic "hacking" conduct that does not necessarily involve immediate adverse effects on systems or data (interference, loss, etc.), but is in itself a dangerous conduct that compromises safety and confidentiality of systems/data (e.g. opening access to

[4] UNODC Toolkit to Combat Trafficking in Persons, p. 119 (Source: http://www.unodc.org/documents/human-trafficking/Toolkit-files/08-58296_tool_3-5.pdf)

[5] Please note that the descriptions of cybercrime offences, especially in the part of required elements, are, for the most part, based on the texts of national legal provisions as identified in corresponding footnotes. Accompanying descriptive elements and explanations are included for the purpose of this manual only, and do not constitute official, binding definitions.

confidential data, including passwords, information about the targeted system) and can be used as a basis for more advanced attacks/offences.[6] The elements of offence of illegal access[7] that are relevant to both centralized and decentralized virtual currencies include: a) an act of "access" comprises the entering of the whole or any part of a computer system (hardware, components, stored data of the system installed, directories, traffic and content-related data), irrespective of the type of connection and method of communication; targets may include computer game accounts database, wallets/lockers for bitcoins, currency exchange sever infrastructure and the like; b) access to computer system should be committed "without right", i.e. without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law; c) intent to access computer system without right must be always present and proven; d) no specific damages, impact or adverse effect whatsoever is necessary – the mere act in itself, without triggering any specific effects, is a criminal offence (this distinction may be important in qualifying offences of attempted money-laundering);

Criminalization of **data interference** as a cybercrime offence aims to protect integrity and confidentiality of computer data from the conduct that endangers its integrity and/or availability.[8] This office can be interpreted as being directed against the proper functioning or use of stored computer data or computer programs, through the acts of damaging, deletion, deterioration, alteration or suppression of computer data without right.[9] It consists of the following elements:[10] a) Acts of manipulation with data (damaging, deletion, deterioration, alteration or suppression of computer data), such as use of virus or Trojan programs or any other malware that may compromise both the currency or personal data of system users, including identity theft; b) Data interference should be committed "without right", which, similar to offence of illegal access, stands for any unauthorised action – either by agreement or by law, and, in terms of virtual currencies, prohibiting "certain abuses related to anonymous communications, such as where the packet header information is altered in order to conceal the identity of the perpetrator in committing a crime"[11] – this may mean that use of additional online anonymity tools to

[6] UNODC Comprehensive Study on Cybercrime, p. 82.
[7] Article 271 of the Criminal Code of Azerbaijan; Article 284 of the Criminal Code of Georgia; Article 259 of the Criminal Code of Moldova.
[8] UNODC Comprehensive Study on Cybercrime, p. 88.
[9] See, for example, the Explanatory Memorandum to the Council of Europe Convention on Cybercrime, par. 61.
[10] Article 286 of the Criminal Code of Georgia; Article 260^2 of the Criminal Code of Moldova; Articles 361 and 362 of the Criminal Code of Ukraine.
[11] See, for example, Explanatory Memorandum to the Council of Europe Convention on Cybercrime, par. 64 (Source: http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm).

further enhance anonymity of decentralized virtual currency users may be brought forward as an element of offence; c) intent to interfere with computer data should be proven;

The offence of **system interference** is similar to the offence of data interference for most of its objectives and applicable elements, save for the difference in object and/or effect of the offence, that is, hindering of the functioning of the computer system.[12] The following elements[13] are required to be present to constitute an offence of system interference: a) the act of hindering by inputting, transmitting, damaging, deleting, altering or suppressing computer data, such as acts that cause short or long-term breakdown of virtual currency processing systems, or take down server infrastructure of computer games that use centralized virtual currency; b) such hindering must be "serious" i.e. it has a significant detrimental effect on the ability of the owner or operator to use the system, or to communicate with other systems (e.g., by means of programs that generate "denial of service" attacks, malicious codes such as viruses that prevent or substantially slow the operation of the system); c) the hindering must be "without right"; d) intent to seriously hinder functioning of a computer system must be proven.

The offence of **misuse of devices** recognizes the potential of the software and hardware that can be used for the commission of crimes against confidentiality, integrity and availability of computer systems or data. It is also understood that many such tools can be dual-purpose devices or technologies (i.e. can be used for both legitimate and illegitimate means); thus the focus is, in order to avoid over-criminalization, on devices that can be primarily used or adapted for such purposes.[14] There are specific elements of the offence of misuse of devices, [15] such as: a) the acts of possession, production, sale, procurement for use, import, distribution or otherwise making available of a device, including a computer programme, designed or adapted primarily for the purpose of committing offences against computer system and data, such as hacking tools, targeted viruses or malware programs, which can be used for targeted attacks against computer systems and data of virtual currency systems and their users, and hacked systems and user accounts used for laundering of criminal proceeds; b) the acts of production, sale, procurement for use, import, distribution or otherwise making available of a computer password, access code or similar data by which the whole or any part of a computer system is capable of being accessed, such as protected information about virtual currencies users login and

[12] UNODC Comprehensive Study on Cybercrime, pp. 88-89.
[13] Article 286, p. 2 of the Criminal Code of Georgia; Article 260^3 of the Criminal Code of Moldova; Articles 361 and 363^1 of the Criminal Code of Ukraine.
[14] UNODC Comprehensive Study on Cybercrime, pp. 92-93 (reference to "computer misuse tools").
[15] Article 271^6 of the Criminal Code of Azerbaijan; Article 285 of the Criminal Code of Georgia; Article 260^4 of the Criminal Code of Moldova; Article 361^1 of the Criminal Code of Ukraine.

password data; c) such acts must be committed "without right"; d) the element of intent in relation to any of the acts listed above must be proven.

The offence of **computer-related fraud** is an assimilative offence that tailors traditional fraud offences to the environment of information and communications technology. The offence of computer-related fraud, therefore, is often not criminalized separately but is rather a legal construct, with the elements of information and communication technology being integrated into the core charges of fraud. Such elements, accordingly, can be narrowed down, in the context of virtual currencies, to manipulations with computer data, such as input, alteration, deletion, suppression or more general interference with the functioning of a computer programme or system. There are, however, differences to other cybercrime offences in requiring two combined elements in the element of intent: first, the general intent to input, alter, delete, suppress or interfere with the functioning of a computer programme or system and, second, proof of a specific fraudulent or other dishonest intent to gain an economic or other benefit for oneself or another.

Case Study: Mt. Gox

Mt. Gox was the most popular Bitcoin exchange based in Tokyo, Japan, which was launched in July 2010, and already by 2013 was handling 70% of all Bitcoin transactions. It filed for bankruptcy in February 2014, citing the loss of almost 850,000 bitcoins belonging to customers.

Mt. Gox alleges its troubles resulted from an issue with Bitcoin known as "transaction malleability". When a bitcoin transaction is made, the account sending the money digitally signs the important information, including the amount of bitcoin being sent, who it's coming from, and where it's going to. A transaction ID, a unique "name" for that transaction, is then generated from all of the information in the transaction. But some of the data used to generate the transaction ID comes from the unsigned, insecure part of the transaction. As a result, it's possible to alter the transaction ID without needing the sender's permission.

Nothing important is lost in that scenario, because the crucial payment information is still securely signed. But it can cause problems down the line if the sender is expecting the transaction to show up under a particular ID. In MtGox claims that the site was expecting transactions to show up in the public ledger under the specific transaction ID it had recorded. When those transactions didn't show up – because the thief had edited the ID – the thief could then complain that the transaction had failed, and the system would automatically retry, initiating a second transaction and sending out more

bitcoins.

Transaction malleability is a flaw in Bitcoin itself, and it's not MtGox's fault that transactions can be renamed in this way. But it's also a flaw which has been known about since 2011, and one which can be rendered harmless with software which accurately reports balances and transactions.[16]

Data and system interference, in current practice, seem so far to be the least relevant offences in terms of virtual currencies; nevertheless, the case of Mt. Gox has proven that the effects of such offences can have an immediate effect on virtual currencies market.

3.1.3 Use of virtual currencies: objective and subjective elements

In more traditional theory of criminal law accepted in the GUAM states, elements of crime can be categorized into objective (an act in itself, as well as objects and tools of crime) and subjective (intent, purpose, complicity, etc.) categories. The use of virtual currencies for money-laundering purposes is going to highlight this distinction. The objective elements of the crime that involve the acts of use of virtual currency are not going to be different, technically speaking, from objective elements of any other crime, including "traditional" money-laundering offences; the use of experts and their expert opinions may be necessary to describe the technical matters relevant to centralized and decentralized virtual currencies, and to draw analogies to traditional financial transactions.

Generally speaking, the use of virtual currency as objective elements of criminal offence of money-laundering can be brought down to the following aspects:

- In terms of **placement** (when criminally derived funds are introduced in the financial circulation), the procurement of the virtual currency through an exchanger (in case of decentralized currencies) or administrator (in case of centralized currencies) may be used as a relevant element of crime;

- In terms of **layering** (the process in which criminally derived funds are legalized and their ownership and source is disguised), the essential features of virtual currency (most relevantly, anonymity and difficult traceability of transactions) can be brought forward as an element of money-laundering offence where the prosecution will be willing to prove the case that the virtual currency was selected precisely for these features, in order to conceal the criminal origin of funds. In fact, focus on

[16] The Guardian, "How a bug in Bitcoin led to MtGox's collapse" (Source: http://www.theguardian.com/technology/2014/feb/27/how-does-a-bug-in-bitcoin-lead-to-mtgoxs-collapse)

layering in terms of virtual currency use is perhaps a central argument for the proof of intent (see below);

- In terms of **integration** (the process by which the property legalized through layering is re-introduced into the economy), the use of virtual currency may be one of the elements, depending on the case: basically, if the laundered proceeds are re-invested into the virtual currency market, this may be an additional element of offence that can be used.

In terms of proof of **intent**, which is an essential feature of money-laundering offences, the situation will be different. The arguments of the state may be reinforced by focusing, again, on the most relevant features of the virtual currencies:

- **anonymity** and general lack of face-to-face interaction may be a valid proof of intent to commit offence related to illegal use of virtual currencies, in contrast to the availability of traditional, more transparent and established financial mechanisms;
- **difficult traceability**, including lack of paper/document trail can be specifically noted as element of intent, with similar logic of avoiding traditional financial mechanisms can be proven;
- in case of decentralized virtual currencies, reliance on **cryptography** that would make any forensic analysis extremely difficult;
- an overarching issue with virtual currencies in terms of proof of intent is the nature of virtual currencies themselves, that is, their operation beyond established financial institutions and overall **lack of regulation** that can be proven as a deliberate choice.

3.2 Procedural Law

The procedural aspects of money-laundering investigations involving the use of virtual currencies are aimed to provide a legal framework for specific actions that supervisory authorities or law enforcement may undertake in order to detect, investigate and prosecute such offences. Continuing with the logic of cybercrime offences being predicate or auxiliary to money-laundering offences in cases involving virtual currencies, the focus of this section is on the procedural tools and regulations of cross-cutting nature between money-laundering and cybercrime that allow for obtaining and securing electronic evidence. At the same time, even where cybercrime is not a predicate or auxiliary offence to money-laundering, the following procedures are important to understand in the sense that they are, by design, specifically tailored to securing and processing electronic evidence.

In addressing the legal framework for such procedural powers, the following distinctions as to the purpose of procedural actions must be made:

- Procedures that aim at the collection of criminal intelligence, i.e. uncovering criminal acts and/or proceeds from crime; and
- Procedures that aim at securing and introducing evidence into criminal proceedings.

3.2.1 Criminal intelligence

Criminal intelligence in the context of the use of virtual currencies for laundering illegal proceeds of crime is focusing on cyber-security operations and cybercrime investigations. Each of these is addressed below.

3.2.1.1 Computer incident reporting by CSIRTs

CSIRTs (Computer Security Incident Response Teams) are long-standing partners of law enforcement in cybercrime investigations, providing data and information on various incidents against computer systems and data. Some of these would potentially be investigated by cybercrime/high-tech crime units, but in reality, the majority of such incidents (that may be reported in hundreds on a single day) will be handled by CSIRTs according to CSIRT-specific procedures that do not necessarily produce evidence that is admissible in criminal cases.

Therefore, taking into account the strong connections between cybercrime, virtual currencies and money-laundering on the Internet, the following reporting sources managed by national CSIRTs can be used:

- Computer incident reporting in cases specifically involving the financial sector. Incident reports can be received from both local, sector-specific or national sensor networks (hardware or software specifically designed to monitor the national segment of the Internet for suspicions deviations in traffic), and international CSIRT databases such as ShadowServer[17] or Arbor Networks.[18] Incident reporting may require specific, often written, agreement with CSIRTs as to the use of incident reporting information (which may contain sensitive or confidential information), and specific uses for such information need to be identified in the request;
- Use of malware that is specifically targeted toward identity theft or breaches of privacy of financial information, including instances where traces of traffic generated by such malware include data or software used for management of centralized or decentralized virtual currencies;
- General intelligence information about the hacker community and threats in national cyberspace that may be often the most valuable source of criminal intelligence in cases of virtual currencies. CSIRTs are,

[17] http://www.shadowserver.org/wiki/
[18] http://www.arbornetworks.com/

by nature of their operations, closely involved with hacker communities and often provide advanced intelligence about cybercrime rings, forums and other information exchange platforms.

Computer incident reporting, due to the concerns related to private and/or confidential nature of data processed by CSIRTs, shall be requested on a case-by-case basis and in the framework of an on-going investigation of money-laundering offence. Although regular reporting modalities may be established as a part of inter-agency cooperation, due to the large amount and extremely technical nature of information processed, regular reporting would not have much relevance or value for the investigation of money-laundering offences.

3.2.1.2 Real-time collection of traffic data

Real-time collection of traffic data[19] is a procedure that is geared toward collection of data generated by computers in the chain of communication in order to route a communication from its origin to its destination, auxiliary to the communication itself ("traffic data"). The categories of traffic data that that can be collected by real-time procedures include: the origin of a communication, its destination, route, time (GMT), date, size, duration and type of underlying service..[20]

Technically speaking, collection of traffic data is possible through specialized equipment owned and managed by law enforcement (cybercrime/high tech crime units) and/or Internet Service Providers.[21] Real-time collection of traffic data requires, as a matter of rule, a judicial order; therefore, proper procedures must be followed: depending on the jurisdiction, investigator's or prosecutor's motion to the judge competent to grant orders on investigative measures. Means for, and units tasked with, collection of such data must be specifically noted in the motion.

Cybercrime or high-tech crime units in the country are usually the ones involved and experienced with real-time collection of traffic data, although in practice these procedures may be used only in most serious cases due to the need to balance the public interests of investigation versus intrusion into the privacy of Internet users. Even if there are state-owned (e.g. digital forensics expert centre) or private (Internet Service Providers themselves) partners who may be able to and willing to undertake real-time collection of traffic data, requests from financial investigators or FIUs dealing with relevant cases, as a matter of good practice, should still be referred to cybercrime/high-tech crime

[19] Article 137 of the Georgian Criminal Procedure Code; Article 263 of the Criminal Procedure Code of Ukraine.
[20] See, for instance, Explanatory Memorandum to the Convention on Cybercrime, par. 30 (Source: http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm)
[21] UNODC Comprehensive Study on Cybercrime, p. 131.

units for performance of real-time collection of data, and seek guidance on further procedures/motions where such are deemed necessary by such units.

3.2.1.3 Interception of content data

In contrast to real-time collection of traffic data, interception of content data (that is, any other data in communication that is different from traffic data) aims to assimilate traditional options for the collection of content data in respect of telecommunications (e.g., telephone conversations) into the environment of information technology. In terms of criminal intelligence, it is a useful investigative tool to determine that the communication is of an illegal nature (e.g., the communication constitutes a criminal threat or harassment, a criminal conspiracy or fraudulent misrepresentations). In terms of cybercrime investigations, interception means the acquisition, viewing, capture, or copying of the contents or a portion thereof, of any communication, including content data, computer data, traffic data, and/or electronic emissions thereof, whether by wire, wireless, electronic, optical, magnetic, oral, or other means, during transmission through the use of any electronic, mechanical, optical, wave, electromechanical, or other device.[22]

In the context of the GUAM states, interception procedures are provided by either by laws on Operative-Detective Activity (possibilities to intercept data from any information and communications networks as an extension of traditional interception/wiretapping procedures)[23] or incorporated in the mainstream criminal procedure legislation.[24] Irrespective of the source of law, interception of content data may be provided by a variety of players, most notably either cybercrime/high-tech crime units or operative departments of the national police. Interception of content, due to privacy concerns, is strictly a procedure based on a judicial order; therefore, all necessary motions shall be properly brought before the court, and means for, and units tasked with, interception of content data must be specifically noted in the motion.

3.2.2 Securing evidence of crime

The purpose of this section is to familiarize law enforcement with the special procedural powers that are used by the cybercrime/high tech crime units and are specifically tailored toward obtaining electronic evidence.

[22] International Telecommunication Union, "The ITU Toolkit for Cybercrime Legislation", p. 12 (Source: http://www.cyberdialogue.ca/wp-content/uploads/2011/03/ITU-Toolkit-for-Cybercrime-Legislation.pdf)

[23] Section 10 of the Law of Azerbaijan on Operative-Detective Activity; Article 18 of the Moldovan Law on Special Detective Activities.

[24] Article 138 of the Criminal Procedure Code of Georgia; Articles 258 and 264 of the Criminal Procedure Code of Ukraine.

3.2.2.1 Expedited preservation of stored computer data

Law enforcement may order or similarly obtain the expedited preservation of specified stored computer-data in connection with a specific criminal investigation or proceeding; basically this is done for the purpose of preventing the deletion of computer data important to cybercrime investigations[25] Data preservation keeps the stored data's integrity intact and the data secure in stored form and protected from anything that would cause its current quality and availability to change or deteriorate.[26]

Preservation of stored computer data[27] allows for expeditious preservation of specified computer data, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification (e.g. there is a business policy to delete the data after a certain period of time or the data is ordinarily deleted when the storage medium is used to record other data, or simply traffic data that is retained for limited time).

The use of an order for preservation of stored computer data is particularly effective since it allows preservation of integrity of that computer data for a period of time as long as necessary, up to a maximum of 90 days, so that competent authorities may later seek its disclosure; to this effect, it can be used as one of the guarantees as to authenticity of data when it is introduced as evidence in criminal proceedings. Moreover, persons or entities in who are in possession or control such data are obliged to maintain confidentiality regarding the undertaking of preservation procedures.[28]

In terms of implementing authorities, in contrast to more specialized criminal intelligence actions, the order for preservation of stored computer data may be used by any investigative authorities since it does not require much of the specialist knowledge for handling of electronic evidence but rather knowledge of which data is to be preserved. Consultation with cybercrime/high-tech crime units as to the practicalities of such orders and their execution may be desirable, but is entirely optional.

3.2.2.2 Expedited preservation and partial disclosure of traffic data

Where data preserved in compliance with the order for preservation of stored computer data, as discussed in the previous section, also includes or is specifically directed at traffic data, such data can be preserved in an expedient manner on the request of law enforcement seeking disclosure of such

[25] UNODC Comprehensive Study on Cybercrime, p. 127.
[26] ITU Toolkit for Cybercrime Legislation, p. 35.
[27] Article 7 of the Moldovan Law on Combating Cybercrime.
[28] See, for instance, Explanatory Memorandum to the Convention on Cybercrime, par. 162 (Source: http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm)

information. Obtaining stored traffic data that is associated with past communications may be critical in determining the source or destination of a past communication, which is crucial to identifying the persons who committed offences against computer systems or data. However, this data is frequently stored for only short periods of time, data protection frameworks that specify that data must not be retained for periods longer than that required by the purposes for which the data are processed.[29]

On the other hand, traffic data that relates to commission of computer-related offences may not be constrained to a single communications provider but rather it may be communicated by several other providers. In this case, the service provider tasked with preservation of traffic data should also promptly disclose to the requesting law enforcement authority a sufficient amount of traffic data to enable the competent authorities to identify any other service providers and the path through which the communication was transmitted.[30]

Similar to expedited preservation of stored computer data, no particular expert or specialist knowledge or expertise is required to effect such order upon service providers. However, a solid understanding of what constitutes "traffic data" and its further use as evidence in criminal proceedings are necessary; therefore, at least some consultations may be sought from cybercrime/high-tech crime units as to the practicalities of such orders.

3.2.2.3 Production orders

Significant part of the infrastructure and computer systems used for internet communications are owned and operated by the private sector. Internet service providers, as well as electronic communication providers and web-service providers, therefore route, store, and control a significant amount of computer data related to internet connections, transactions, and content. The use of coercive measures, such as search and seizure, by law enforcement for obtaining these data are unfeasible in the majority of circumstances – due both to the volume of individual cases investigated, and disruption to legitimate business activity. Orders to such third parties to the investigation for computer data thus provide a due legal process route to obtaining electronic evidence[31]

A production order is aimed at computer data or subscriber information that is in the possession or control of a person or a service provider. The concepts of "possession" and "control" relate to data that is, legally and technically, subscriber information in the service provider's physical possession, or is available to the provider remotely (e.g. in managed cloud or remote data storage facility). As to "subscriber information", this term refers to any

[29] UNODC Comprehensive Study on Cybercrime, p. 127.
[30] Explanatory Memorandum to the Convention on Cybercrime, par. 169 (Source: http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm).
[31] UNODC Comprehensive Study on Cybercrime, p. 128.

information held by the administration of a service provider relating to a subscriber, to its services, and can be used to identify which services and related technical measures have been used or are being used by a subscriber or, when a technical address is known, subscriber information is needed in order to assist in establishing the identity of the person concerned. [32]

Production orders[33] can be effected by any law enforcement authorities that have staff with the sufficient understanding of subscriber information as well as privacy and confidentiality requirements in electronic communications.

3.2.2.4 Search and seizure of stored computer data

Search and seizure procedures for computer data (i.e., electronic evidence) are, in essence, assimilative provisions that aim to harmonize already existing criminal procedural law powers for search and seizure of tangible objects, in terms of their application to computer systems and data. The search and seizure of stored data, therefore, is mostly different from search and seizure of a tangible object, which involves inspection of a physical area and removal of the tangible object from the searched premises. In the digital environment, the gathering of data occurs during the period of the search and with respect to data existing at that time. There are two main ways of conducting an investigation: accessing and searching data which is contained within a computer system or part of it (such as a connected storage device) or on an independent storage medium (removable storage, etc.).[34]

At the same time, the nature of electronic evidence (i.e. data stored in a computer system in intangible, digital form) may also require different approach compared to traditional search and seizure procedures. Most importantly, readability of data must be ensured: where the data can be read only by a computer system on which they're stored, the entire system must be seized; in other cases, a copy of the data may be made and taken away on a physical storage device. Similarly, data may be extracted from connected devices (storage, network, etc,). In this respect, seizure procedures of searched computer data are, in essence, no different from traditional seizure procedures.[35]

One of the most distinctive powers that is provided by the Council of Europe Convention on Cybercrime in terms of search and seizure of stored computer data is rendering relevant data inaccessible, which is relevant to the GUAM

[32] Explanatory Memorandum to the Convention on Cybercrime, par. 177 (Source: http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm)
[33] Article 136 of the Criminal Procedure Code of Georgia; Chapter 15 of the Criminal Procedure Code of Ukraine.
[34] ITU Toolkit for Cybercrime Legislation, p. 36.
[35] Explanatory Memorandum to the Convention on Cybercrime, par. 187 (Source: http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm)

Member States, who are Parties to the Convention.[36] This is particularly relevant in terms of money-laundering offences involving the use of information technology, since the taking down of hardware, software and online platforms used for laundering proceeds of crime may be necessary to minimize harm to victims. However, not many jurisdictions implement similar powers in the context of criminal procedure, leaving this as a highly desirable procedural power that is often unavailable to law enforcement.

In terms of practical application, the situation with search and seizure can be less clear than with other, more specialized procedural powers. On one hand, search and seizure in a traditional sense may be undertaken by any law enforcement agency, and, where necessary, experts of specialists may be involved to facilitate search and seizure.[37] On the other, removal of evidence from computer systems or even removal of computer systems themselves from the searched premises may require advanced expertise in order to preserve readability and integrity of data. Therefore, guidance and, where necessary, direct involvement of the cybercrime/high-tech crime units is essential in such cases.

3.3 Electronic Evidence and Chain of Custody

Electronic evidence secured through proper legal procedures, as discussed in the previous sections, still needs to be processed properly in order to become legitimate, admissible evidence that can be presented in the courtroom to support the case. In most cases, compliance with legal requirements set for procedural actions that secure and extract evidence is going to be sufficient to guarantee admissibility of evidence in criminal proceedings; however, electronic evidence has some additional features that need to be taken into account in compliance with such requirements.

3.3.1 Expert handling and reports

Criminal justice systems of the GUAM states rely on expert analysis and testimony in many cases where evidence needs to be properly introduced and processed in criminal proceedings.[38] Reliance on expert support is particularly relevant in terms of handling electronic evidence, since modern computer systems and devices are built to customized or specific characteristics and configurations, requiring exact adherence to specific procedures to extract relevant data from such systems and devices. Handling of electronic evidence by non-specialists therefore significantly increases the risk of its unintentional modification and, as a result, inadmissibility in criminal proceedings.

[36] Article 19, p. 3 of the Council of Europe Convention on Cybercrime.
[37] Article 19, p. 4 of the Council of Europe Convention on Cybercrime.
[38] Article 97 of the Criminal Procedure Code of Azerbaijan; Article 52 of the Criminal Procedure Code of Georgia; Article 88 of the Criminal Procedure Code of Moldova; Article 69 of the Criminal Procedure Code of Ukraine.

There are numerous types of expertise that may be sought in the course of criminal proceedings involving money-laundering with the use of virtual currencies. Most obvious would be financial expertise seeking expert review of transactions or determination of the value of proceeds of crime. However, electronic evidence that is prevalent in such cases may often call in more specialized expertise of technical nature, that is, digital forensics.

Digital forensics can be provided by several institutions in a single jurisdiction. Primary expertise related to crime intelligence is usually provided by specialized cybercrime or high-tech crime units themselves, and it is therefore proper to seek such expert support from these units where real-time collection of traffic data or content interception is concerned. However, most of the digital forensics aimed at processing already secured evidence is performed either by specialized digital forensics centres (incorporated primarily in police forces) or by independent, state owned or private expertise centres that have a wider expertise on all kinds of traditional and electronic evidence. An important factor in the choice of such institutions is the level of expertise and experience, which can be often obtained only through specialized training and certification.

Besides level of individual expertise, use of proper procedures, tools and techniques is of utmost importance. Unless the general computer system diagnostics is enough for provision of reliable evidence, specialized hardware and software are important elements of evidence analysis that have direct impact on its admissibility. Such tools, techniques and procedures need to be traceable and repeatable by other specialists, so that the captured information is of evidentiary value and can be proven to be so in case such procedures are questioned in court.

Besides expert reviews and reports on secured evidence, there are additional avenues in which digital forensics experts or specialists of similar expertise may be called to assist in investigative actions, such as search and seizure, interception of content or preservation of data. Expert assistance in such procedures, who may be invited in the status of either experts or specialists, can be viewed as an additional guarantee of the proper handling of electronic evidence with a view to its admissibility in criminal proceedings.

Expertise required in handling and analyzing electronic evidence can be found across many institutions, whether public or private, and the choice for expert review and report must take into account not only the quality or expedience of expert review, but also the issues of objectivity. Since the experts will be, as matter of rule, called to court proceedings to be questioned as witnesses, their background and, more importantly, professional affiliation can be called into question. To put this into electronic evidence perspective, it may be tempting to secure expert analysis from cybercrime/high-tech crime unit; however, since

such units are part of the criminal police departments and are involved in investigation and prosecution of cybercrime cases, their bias toward prosecution and state interests may be called into question.

3.3.2 Chain of custody

The chain of custody of electronic evidence is, in essence, no different from that of traditional evidence. Criminal proceedings rely on highly formalized procedures and requirements; therefore, adherence to set procedures, ensuring handling by persons having sufficient qualifications to do so, and keeping a document trail to show when and how evidence was stored, accessed or used, represent the standard approach applicable to any criminal proceedings, and to any type of evidence that may be used in such proceedings. Electronic evidence, on the other hand, has some additional specific features that need to be taken into account in order to ensure proper chain of custody:

- **Data integrity**: Electronic evidence is highly volatile. Access to computer system, even for mere browsing purposes, will, in most cases, modify the data (such as "recently accessed" documents list) to an extent that this cannot be used as evidence criminal proceedings. Computer data should be, therefore, always kept from possible modifications, and a range of techniques and methods (such as access only in "read mode", examination of a digital copy and not "original" evidence, imaging or recording of handling, etc.) used to keep authenticity of data.

- **Audit trail**: Keeping a trail of formal documents supporting the investigation process is highly important. In criminal proceedings, investigators use standardised forms or checklists to document their analysis and also ensure that they do not forget to perform all stages of the examination to obtain an exhaustive scrutiny of the victim's and suspect's computer system. Similarly, notes should be taken describing all stages of handling the evidence, whether it is a crime scene or forensic laboratory. Screenshots, photographs and video records greatly enhance quality of audit trail of electronic evidence.

- **Specialist support**: In many cases, the highly technical nature of the computer environment and data contained therein requires the use of computer forensics specialists. The need for specialist support may be called for due to the highly specialized area of digital forensics (e.g. mobile malware analysis), as well as limited availability of equipment for such analysis. Therefore, although not necessarily mandatory in all cases, specialist analysis will be an important part of the case file that further enhances the arguments of the party willing to bring such evidence forward.

- **Legality**: Computer systems that are used as a source of electronic evidence usually contain at least some amount of private information which is not going to be of relevance or value to the investigation. Proper sorting of the data that is relevant to investigation and sensitive information that must not be looked into is therefore necessary. In some cases, these distinctions are not going to be clearly drawn; thus, court orders preserving such data may be necessary to further proceed with analysis of information.[39]

3.3.3 Admissibility of electronic evidence

Since the ultimate goal is the use of acquired and analysed evidence to support a case in court, electronic evidence must be obtained in compliance with existing legislation and best practice procedure to be admissible in a trial. Although the details differ depending on national legislation, the following basic criteria must generally be taken into account:

- **Authenticity**: It must be possible to positively tie evidentiary material to the investigated incident. Electronic evidence is no different to physical evidence, such as a document recorded on a piece of paper. It is necessary to ensure that the evidence is authentic. The difference between electronic evidence and physical evidence is usually the ease by which electronic evidence can be changed and altered, either deliberately or inadvertently.

- **Completeness**: It must tell the whole story and not just a particular perspective. The evidence should be weighted in terms of balance and objectivity, and, where supported by other evidence, whether physical or electronic, should provide a coherent picture of the events it is called to prove.

- **Reliability**: There must be nothing about how the evidence was collected and subsequently handled which causes doubt about its authenticity and veracity. In the event that there is a doubt about electronic data adduced in evidence, it is for the defence to raise a challenge to its admissibility. Once the issue is raised, the prosecution has to deal with it, usually by providing sufficient evidence that the 'integrity of the data is trustworthy, and is therefore considered to be reliable.'

[39] "Electronic Evidence Guide: A basic guide for police officers, prosecutors and judges," produced by EU/COE Joint Project on Regional Cooperation against Cybercrime, pp. 131-134 (Source: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Electronic%20Evidence%20Guide/default_en.asp)

- **Believability**: It must be readily believable and understandable to the participant of criminal proceedings, especially judicial authorities. Presentation is important to give expert evidence the weight it deserves. Presentation of electronic evidence to the judge and jury needs to be visual, using computer demonstrations, video demonstration, computer graphics, schedules and charts. Parties introducing evidence should be aware of the bias that using such technology can cause, and be prepared to discuss these issues with authority if the defence challenges the use of such technology.[40]

3.4 Safeguards and Guarantees

All procedures that involve processing of electronic evidence shall be based on the respect for fundamental rights and guarantees of parties to the criminal proceedings. Since procedural actions relevant for investigation of money-laundering with the use of virtual currencies are sourced from cybercrime laws and regulations, similar approaches required by applicable standards[41] will be applicable here as well. These safeguards and guarantees are of a practical nature and require to be viewed as an integral feature of procedural actions to which they apply.[42]

First of all, all of procedural actions that intrude into the private life of individuals shall be undertaken in the framework of on-going criminal case investigations. In terms of on-going investigations, it does not matter whether cybercrime, money-laundering or fraud offences are being investigated – a formal decision on commencement of an investigation is viewed as one of the guarantees against abuse of authority with the use of procedural powers that have impact on the privacy of individuals.

For some of the special investigative powers applicable to securing electronic evidence, such as interception of content data or preservation of stored traffic data, the prerequisite in some jurisdictions is serious the nature of the offence, meaning an offence punishable with a specific term of imprisonment. This needs to be taken into account for a simple reason: most of the cybercrime offences against computer systems and data are not qualified as serious offences in the national framework, thus negating the possibility of use of special procedural powers. In this context, a choice for legal practitioners would be to qualify cybercrime acts in the framework of charges of money-laundering, which is going to be a serious offence in all cases.

[40] Electronic Evidence Guide, pp. 146-147.
[41] Such as, for example, Article 15 of the Council of Europe Convention on Cybercrime, which applies to the GUAM Member States.
[42] For a more extended overview of applicable safeguards and guarantees, as well as national examples, please consult the UNODC Comprehensive Study on Cybercrime, pp. 136-141.

Judicial order for special procedural powers intruding into the privacy of individuals, in particular interception of content, is viewed as an essential guarantee for balancing of private and public interests at stake. In terms of virtual currency-related offences, this would often mean a deliberate choice by law enforcement against the use of such procedures, not least for reasons of expediency. At the same time, substituting less intrusive measures with other options (e.g. search and seizure in exigent circumstances without court warrant) can prove to be problematic if such choices are challenged in court based on the principle of proportionality.

Finally, particular attention must be paid to national regulations related to personal data protection and, in particular, sensitive data categories that may include data which is sought in the course of an investigation. Although there is a general, international standard of non-applicability of data protection guarantees (e.g. consent of the data subject to process data) in cases of criminal investigations, there is a trend to subject police operations aimed at criminal intelligence to data protection requirements. Law enforcement should be aware of such standards, if applicable, and consult specifically with local data protection authorities with a view to obtain guidance on such matters.

4 Investigative Tools And Methodologies

The purpose of this section is to list some of the available tools that can be used to detect and investigate laundering of crime proceeds through the use of virtual currencies.

4.1 Red Flags/Indicators

Red flags/indicators are an important investigative tool in financial investigations. A "financial investigation" in this context means an enquiry into the financial affairs related to a criminal activity, with a view to:

- Identifying the extent of criminal networks and/or the scale of criminality;
- Identifying and tracing the proceeds of crime, terrorist funds or any other assets that are, or may become, subject to confiscation; and
- Developing evidence which can be used in criminal proceedings[43].

Regardless of whether the competent authority for financial investigations is a Financial Intelligence Unit (FIU), law enforcement authority, supervisory authority, cybercrime unit or any other investigative agency, the investigative challenges presented by virtual currencies are still the same. Further discussion of specialised units for financial investigations can be found in Section 5.5.

There is no study that has been carried out specifically to investigate and identify red flags/indicators relating to the use of virtual currencies, but there are several studies that have identified red flags/indicators in the more general case of laundering crime proceeds on the Internet, or using new payment methods.[44], [45]

Many of the red flags/indicators identified in these studies are applicable in the case of laundering crime proceeds through the use of virtual currencies. Some examples of the red flags/indicators identified in the studies are:

---

[43] Interpretive note to Recommendation 30, "International standards on combating money laundering and the financing of terrorism & proliferation – The FATF Recommendations", FATF-GAFI, February 2012. (Source: http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf)

[44] "Money Laundering Using New Payment Methods", FAFT-GAFI, October 2010. (Source: http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20using%20New%20Payment%20Methods.pdf)

[45] "Criminal money flows on the Internet: methods, trends and multi-stakeholder counteraction.", Council of Europe Global Project on Cybercrime and MONEYVAL, March 2012. (Source: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/reports-presentations/MONEYVAL_2012_6_Reptyp_flows_en.pdf)

- Discrepancies between submitted customer identification and IP address. For example, if a user provides documentation on account creating indicating an address in the UK and then all IP addresses associated with the customer's activity are noted as being from Japan.
- Suspicious IP addresses and suspicious usernames (monikers, nicknames, ICQ numbers) would help in the detection of criminal money flows.
- Logins or attempted logins from non-trusted IP address or from user's IP previously identified as associated with suspicious activity.

However, the red flags/indicators provided in these studies, including the ones just mentioned above, are very general and applicable in many forms of investigation involving the Internet.

Perhaps somewhat more relevant are the red flags/indicators provided by the FATF that can suggest a complicit payment provider. In the FATF study, these red flags/indicators are provided in the context of a complicit prepaid card provider. However, as mentioned in Module 2, this is a typology that is applicable to virtual currencies. Therefore, the red flags/indicators of activity that may be suspicious in the case of prepaid card providers may be useful in the case of virtual currency providers. The provided red flags/indicators, interpreted for the case of virtual currency providers are:

- Large number of bank accounts held by the same virtual currency administrator or virtual currency exchange company (sometimes in different countries) apparently being used as flow-through accounts (may be indicative of layering activity), without a business rationale for such a structure.
- Virtual currency administrator or virtual currency exchange company located in one country but holding accounts in other countries where it does not have a significant customer base (unexplained business rationale which could be suspicious).
- Back and forth movement of funds between bank accounts held by different virtual currency administrator or virtual currency exchange companies located in different countries (may be indicative of layering activity as it does not fit the business model).
  The volume and frequency of cash transactions (sometimes structured below reporting threshold) conducted by the owner of a virtual currency administrator or virtual currency exchange company do not make economic sense.

4.2 Investigative Indicators

When examining a suspect PC, there can be various indicators of the use of virtual currencies. This section will provide a discussion of some of the

techniques that can be used to determine whether there is evidence of the presence of use of virtual currencies by the suspect.

4.2.1 Presence of Software Associated with the Use of Virtual Currencies

Some virtual currencies, particularly decentralised virtual currencies, involve the installation of software. The presence of this software on a suspect computer can be an indicator of the use of virtual currencies. The following sections contain some examples of the software installed to use virtual currencies.

4.2.1.1 Bitcoin

The software installed on a computer to use the Bitcoin network is called a Bitcoin wallet. There are a variety of different Bitcoin wallet software packages available. For example:

- Bitcoin Core[46]
- MultiBit[47]
- Hive[48]
- Bitcoin Armory[49]
- Electrum[50]

Some, but not all, of these software packages will, after installation, download a complete copy of the entire Bitcoin block chain. This is very large, almost 20Gb in size. The large size of the block chain can be helpful to identify the data directory in use by Bitcoin software. Additionally, the presence of a wallet file, often called wallet.dat, is a strong indicator of the use of the Bitcoin network.

4.2.1.2 Other Distributed Virtual Currencies

LiteCoin wallet software[51] and DogeCoin wallet software[52] are also available. The presence of this type of software package is an indicator of the use of these virtual currencies.

[46] https://bitcoin.org/en/download
[47] https://multibit.org/
[48] https://www.hivewallet.com/
[49] https://bitcoinarmory.com/
[50] https://electrum.org/
[51] https://litecoin.org/
[52] http://dogecoin.com/

Similarly to the Bitcoin software mentioned above, some of these software packages make large downloads when they are installed. In each case they are downloading that virtual currency's equivalent of the Bitcoin block chain.

WebMoney also provides a downloadable client for sending and receiving WebMoney transfers.[53]

4.2.1.3 "In-world" Virtual Currencies

Multiple "in-world" virtual currencies such as Second Life Linden Dollars[54], Project Entropia Dollars[55] or World-of-Warcraft Gold[56] can be acquired through the applications that are used to interact with the virtual world.

The presence of these software applications may, in the correct context, also indicate the use of their virtual currencies.

4.2.2 Browsing History Containing Virtual Currency Related Websites

Not all distributed virtual currencies involve the installation of software. For example, the Ripple client operates as a JavaScript application in the user's browser.[57] Other virtual currencies offer both downloadable software and interaction through a web browser as options to send and receive virtual currency.[58]

In addition, the trading of virtual currencies on virtual currency exchanges is typically carried out in a web browser.

Therefore, the bookmarks, browsing history and cache of a suspect computer may provide valuable indicators of use of virtual currencies.

4.2.3 Remote Storage Services

Recall that virtual currencies, particularly decentralised virtual currencies, are a digital representation of value and that it is the digital representation itself rather than how or where that representation is stored that is actually the important indicator of stored value.

With that in mind, there is no reason why the digital representation need necessarily be stored locally on the suspect PC. The amount of data in the digital representation is typically small (less than 100 bytes) so there are almost

[53] http://www.wmtransfer.com/eng/about/demo/classic/index.shtml
[54] https://secondlife.com/support/downloads/
[55] http://www.entropiauniverse.com/download/
[56] http://us.battle.net/wow/en/
[57] https://ripple.com/wiki/Client_Manual
[58] http://www.wmtransfer.com/eng/about/demo/light/index.shtml

innumerable ways in which a suspect could remotely store the digital representation.

One possible way in which the digital representation could be stored is in a remote storage service. There are many such services that offer virtual storage, with most offering some sort of limited free service.[59], [60], [61]

Additionally, other remote services that are not specifically storage services could also be used for the same purpose. One notable example of this would be use of a web-based email provider[62], [63] some of which specifically offer privacy as a feature.[64], [65] Another example would be note or task management services.[66]

Many of these services can also be accessed in a variety of ways including:

- Specific, downloadable desktop software
- Web-based interface
- Standard applications such as email applications
- Mobile applications

Identification of the use of these remote storage services may not, of itself, indicate the use of virtual currencies. However, if virtual currencies are suspected or known to be in use, identification and investigation of remote storage services could be a very important source of evidence.

4.2.4 Credential Storage Software

Software is available that can be used to manage the login and account details of a user.[67], [68], [69], [70] These typically operate by having a single password that the user needs to remember and storing all of the user's other credentials in an encrypted file. These software packages also often have the ability to store small text notes.

---

[59] https://www.dropbox.com/
[60] https://drive.google.com/
[61] https://www.amazon.com/gp/feature.html?ie=UTF8&docId=1000796931&ref_=cd_lm_rd_fp
[62] https://www.gmail.com/intl/en/mail/help/about.html
[63] https://mail.yahoo.com/
[64] https://www.hushmail.com/
[65] https://lavaboom.com/
[66] https://evernote.com/
[67] https://agilebits.com/onepassword
[68] https://lastpass.com/
[69] https://www.my1login.com/content/index.php
[70] http://www.f-secure.com/en/web/home_global/key

Many web browsers also have the ability to store passwords associated with logins to websites.[71], [72], [73], [74]

It may be possible if such software is identified, that credentials associated with the use of virtual currencies, or even digital representations of virtual currency are stored within such software.

Many of these software packages support remote storage of information (credentials, notes, etc.), browser plugins and synchronisation of information with a mobile application.

Once again, however, identification of the use of these software packages may not, of itself, indicate the use of virtual currencies but if they are identified in cases where virtual currencies are suspected or known to be in use, they can potentially provide valuable evidence.

4.2.5 Virtual Machines

Virtual machine software allows a user to execute an operating system essentially as an application on their computer.[75], [76], [77] This means, for example, that a user could have a second windows computer, referred to as the "guest", stored on their computer, referred to as the "host". Most virtual machine software allows the files that represent the hard drive of the virtual machine to be encrypted, meaning that the virtual machine cannot be booted up without knowing the corresponding password.

In such a case, it would be possible to use an encrypted virtual machine for all virtual currency activity and there would be no evidence of the use of virtual currencies in the "host" operating system.

There are many legitimate uses of virtual machines, and for encrypting the hard drives of virtual machines, but in cases where virtual currencies are suspected or known to be used, the presence of virtual machines would be worthy of investigation.

---

[71] https://support.mozilla.org/en-US/kb/password-manager-remember-delete-change-passwords
[72] http://www.cnet.com/uk/how-to/how-to-save-passwords-for-all-web-sites-in-safari/
[73] https://support.google.com/chrome/answer/95606?hl=en
[74] http://windows.microsoft.com/en-ie/internet-explorer/fill-in-forms-remember-passwords-autocomplete#ie=ie-11
[75] http://www.vmware.com/
[76] https://www.virtualbox.org/
[77] http://www.parallels.com/

4.2.6 Mobile Devices

The software for virtual currencies, as discussed in Section 4.2.1, and browsing related to the use of virtual currencies, as discussed in Section 4.2.2, can also be found on mobile devices. Examples of the software available for mobile devices include Bitcoin[78], [79], WebMoney[80] and Ripple[81] clients.

Evidence gathered through the investigation of mobile devices can therefore also be an important indicator of the use of virtual currencies to launder crime proceeds.

4.3 Forensic Analysis

Correctly gathering evidence is essential to building a case and evidence in cases involving virtual currencies may be available in many places. The following sections discuss some of the different sources of data and the nature of the forms of evidence that may be recovered there.

A full discussion of the technical processes for gathering and analysing this evidence is beyond the scope of this manual, but it should be performed by a specialised forensic investigation unit, following best practice for gathering and managing electronic evidence as discussed in Section 3.3.

4.3.1 Suspect Computer

A suspect's computer may, as in many cases, be a valuable source of evidence. Of course, such a discussion is not limited to the physical computer itself, but also any other storage media (CDs, DVDs, external hard drives, flash drives, etc.) that are found with, or known to have been used with, a suspect computer.

Some examples of the evidence that can be retrieved from a suspect computer would be as follows:

- There may be evidence in the form of credentials, visits to websites, emails, etc. that establish the suspect's relationship with a virtual currency administrator or virtual currency exchange.
- It may be possible to gather evidence to demonstrate a suspect's possession of particular virtual currency value.
- In the case of bitcoins, it may be possible to identify particular addresses that are in the control of the suspect. Bitcoin addresses can subsequently be investigated to determine from which other addresses value was

[78] https://play.google.com/store/apps/details?id=com.mycelium.wallet
[79] https://play.google.com/store/apps/details?id=de.schildbach.wallet
[80] https://wiki.wmtransfer.com/projects/webmoney/wiki/WM_Keeper_Mobile
[81] https://ripple.com/blog/introducing-ripple-client-the-ios-app/

transferred to the suspect address and to which other addresses value was transferred by the suspect address.[82]

- The IP address of the computer at a particular time may be associated with known suspect transactions or other financial activity.
- Evidence of the use of remote storage services, upon which virtual currency value may be stored (see the next section).
- Passwords or other credentials that may be used to unlock virtual currency accounts or value.

Case Study: Bitcoin Wallet

This case study focuses on the Bitcoin wallet software, MultiBit.[83] MultiBit is a lightweight Bitcoin wallet for Windows, MacOS and Linux.[84] This study will focus on the structure and operation of the software and will assume that the investigator has appropriate tools and expertise to gather evidence in a forensically sound way.

The application is installed, by default in C:\Program Files (x86)\Multibit-0.5.18. The first time MultiBit is started, a new, empty wallet is created called "multibit.wallet". By default this wallet is not password protected and it is stored in C:\Users\<user>\AppData\Roaming\MultiBit\multibit.wallet, where "<user>" is the user name of the currently logged in user. It is possible for a user to create as many wallets as they want, which will, by default, be stored in the same folder as multibit.wallet.

MultiBit will create various backups of the configured wallets in a folder called "<wallet name>-data" where <wallet name> is the name of a particular wallet. This backup folder is also stored, by default, in the default MultiBit data directory mentioned above.

An example of the main screen of MultiBit can be seen in Figure **2**. On the left hand side of the MultiBit main screen is a list of wallets that the user has configured along with the amounts of bitcoin value stored in each wallet. On the right hand side of the screen is a tab for sending bitcoins to another wallet, a tab for receiving bitcoins, including the selected Bitcoin receiving address and a tab where all transactions can be reviewed.

It is possible for the user to create any number of Bitcoin receiving addresses using the "New" button on the receiving tab.

[82] http://blockchain.info/
[83] https://www.multibit.org/
[84] This case study was developed on Windows 7 Professional, 64-bit, with MultiBit version 0.5.18.

A Bitcoin receiving address is an alphanumeric string such as:

1FjckeaGiEZWawYHmhKU79BxPHvNu4Egqu

The ".wallet" file contains the private keys associated with each of the Bitcoin wallet IDs, as well as transaction data associated with each address.[85] The file is stored in a binary format, which can be opened with MultiBit. The easiest way to examine the content of the wallet file from a suspect computer is to copy the MultiBit data directory to a forensic workstation and open the wallet with MultiBit.

Transactions associated with Bitcoin addresses are stored in the Bitcoin block chain, which can be queried online[86]. Therefore, information about Bitcoin addresses gathered from suspect computers can be further investigated to see which transactions preceded or followed on from transfers to/from Bitcoin addresses known to be associated with a suspect.

It is not possible, using information stored by MultiBit, to associate any Bitcoin addresses with IP addresses or other identifying information, except of course any Bitcoin addresses that are found in the configuration files of MultiBit that can be associated with other identifying information found on the suspect computer.

Alongside each ".wallet" file there can be found a corresponding ".info" file. The ".info" file will contain all of the configured sending and receiving addresses. An example ".info" file can be seen in Figure **3**. Each line beginning with "receive" is a configured receive address and send addresses will be in the same format but the line will begin with "send". The location of the wallet backup file can also be seen at the end of the ".info" file.

[85] https://multibit.org/en/help/v0.5/help_fileDescriptions.html
[86] http://blockchain.info/

Figure 2: MultiBit Main Screen

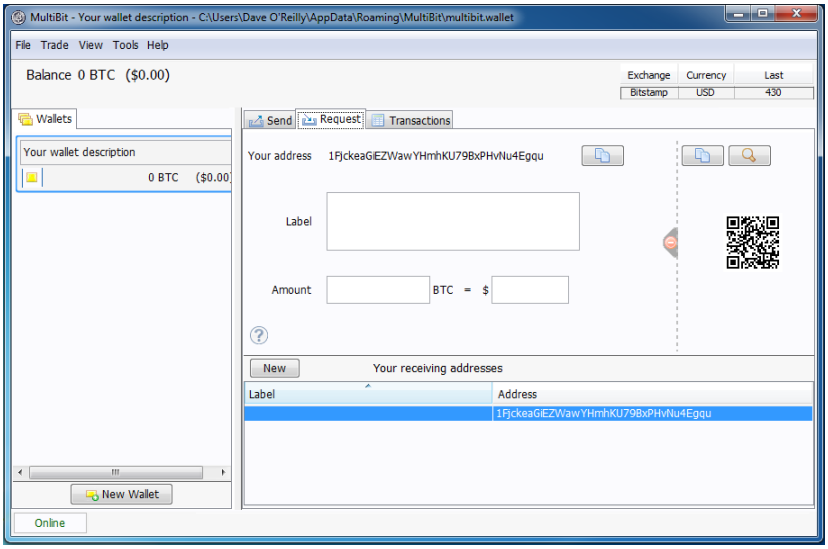


Figure 3: MultiBit wallet info file

```
multiBit.info,1
walletVersion,2
receive,16tX9dKcSLDuKDUhbB9Qy2KvdRKUKFgzNU,
receive,1CMVGKneZJD3S8vaARnHdnQLYmGrApVucE,
receive,16wGizcLnQo6xSs5iSigstN9Ah3KLK4yvK,
receive,1Bi8bwvaA8PWU1XoC8PD1UDHd16MfcT1x7,
receive,1LKTxZrLd2vbT3uRFKPSLn9pm8ZnHnjFiH,
receive,1GG6Sq5JxAm3aEWNc98m1NzQmFMwyggLVq,
receive,1PZtgVQHErx1aCtZfGxcx3zutbCaaCPEwu,
receive,1MCsQKTsqBfg2asQNy1x8dGDkxB6mkvpRy,
property,walletDescription,Your%20wallet%20description
property,receiveLabel,
property,walletCleanedOfSpam,true
property,receiveAddress,14nuoifKUmXDTnTbGDyXKFZr9rbDDteiao
property,walletBackupFile,C%3A%5CUsers%5CDave%20O%27Reilly%5CAppData%5CRoaming%5CMultiBit%5Cmultibit-data%5Crolling-backup%5Cmultibit-20140506170256.wallet
```

Case Study: Second Life Linden Dollars

Second Life Linden Dollars can either be purchased using the Linden Exchange, LindeX[87] or "in-world" using the Second Life Viewer.[88]

The process of purchasing Linden Dollars in the Second Life Viewer is simply to click the "Buy L$" button, as shown in Figure **4**. The amount of Linden Dollars required is entered here and the purchase is made. In order to purchase Linden Dollars in this way, a payment method must be set up via the Second Life website.

Purchases and sales of virtual currency can also be carried out through the Linden Exchange directly on the Second Life website, or through another third party exchange. Buying on the Linden Exchange is performed by specifying either the amount of Linden Dollars to be purchased or the amount of US Dollars to be spent, as shown in Figure **5**. Selling is performed in a similar fashion.

Passwords associated with Second Life accounts cannot be recovered directly from the Second Life viewer, but it is possible they can be recovered from password management software, as discussed in Section 4.2.4. Similarly, it is possible that passwords associated with Second Life account may be stored by a web browser.

Linden dollar balances, payment methods and transaction records are stored with the Second Life account. It is possible therefore for Linden Labs to disclose this information, subject to the appropriate legal process, which can be one or all of the following:

- Direct contact with Linden Labs with the request seeking account-related information which is not confidential under the Terms of Service.[89]
- Police-to-police cooperation procedure seeking production order through 24/7 point of contacts (for members to the Convention on Cybercrime) or through G8 Network of High-Tech Crime Units, or through Interpol contact points if none of the former can provide assistance. The ability or expedience of response is entirely dependent on the receiving authority but is going to be much faster than formal

[87] http://www.lindex.com/eu/
[88] https://secondlife.com/support/downloads/
[89] http://lindenlab.com/tos#tos7

mutual legal assistance requests.

- Mutual legal assistance procedure launched through central prosecution office or Ministry of Justice, which is then fully managed by the authority in question; expediency is a major concern for such procedures.

Figure 4: Buying Linden Dollars through the Second Life Viewer

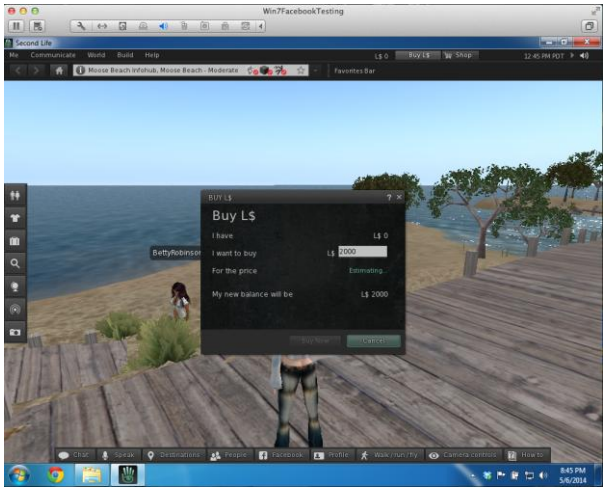
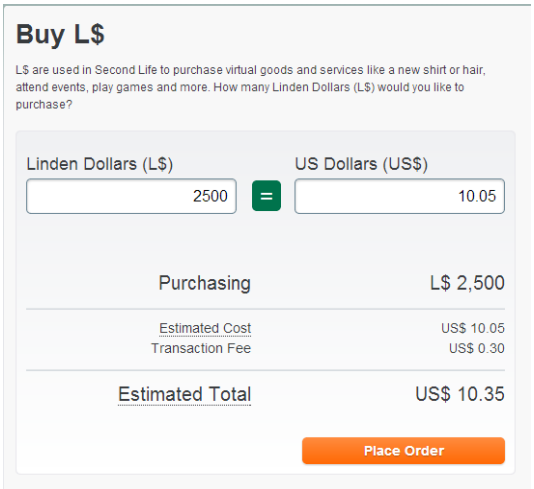


Figure 5: Buying Linden Dollars through the Second Life Website



4.3.2 Cloud Services

Since virtual currencies are a digital representation of value, as discussed in Module 1, there is no reason why the digital representation need necessarily be stored locally on the suspect's PC. The suspect might choose to store the digital representation on an Internet storage service. There are a multitude of possibilities for how this could be achieved in practice. Some examples include;

- The use of a cloud storage service such as DropBox or similar.[90], [91], [92]
- The use of an Internet-based email service provider.[93], [94]
- The use of any form of Internet service that facilitates the storage of notes or other forms of data.[95]

It may be possible to identify evidence of the suspect's use of such a service from their computer by identifying either software associated with the use of the cloud service or browsing activity indicative of the use of a web-based service. This can be followed up with a request for information from the service provider using the appropriate legal channels, such as:

- Direct contact with the service in question with the request seeking disclosure of requested information.
- Police-to-police cooperation procedure seeking production order through 24/7 point of contacts (for Parties to the Council of Europe Convention on Cybercrime) or through G8 Network of High-Tech Crime Units, or through Interpol contact points if none of the former can provide assistance. The ability or expedience of response is entirely dependent on the receiving authority but is going to be much faster than formal mutual legal assistance requests.
- Mutual legal assistance procedure launched through central prosecution office or Ministry of Justice, which is then fully managed by the authority in question; expediency is a major concern for such procedures.

Case Study: The Presence of a Cloud Service Application

DropBox is a file hosting service that offers cloud storage of files and synchronisation of shared files across multiple devices[96]. To use DropBox, a

[90] https://www.dropbox.com/
[91] https://cloud.google.com/products/cloud-storage/
[92] http://www.amazon.com/gp/feature.html/ref=cd_def?ie=UTF8&*Version*=1&*entries*=0&docId=1000796931
[93] https://www.gmail.com/intl/en/mail/help/about.html
[94] https://login.yahoo.com/config/login_verify2?&.src=ym&.intl=us
[95] http://evernote.com/

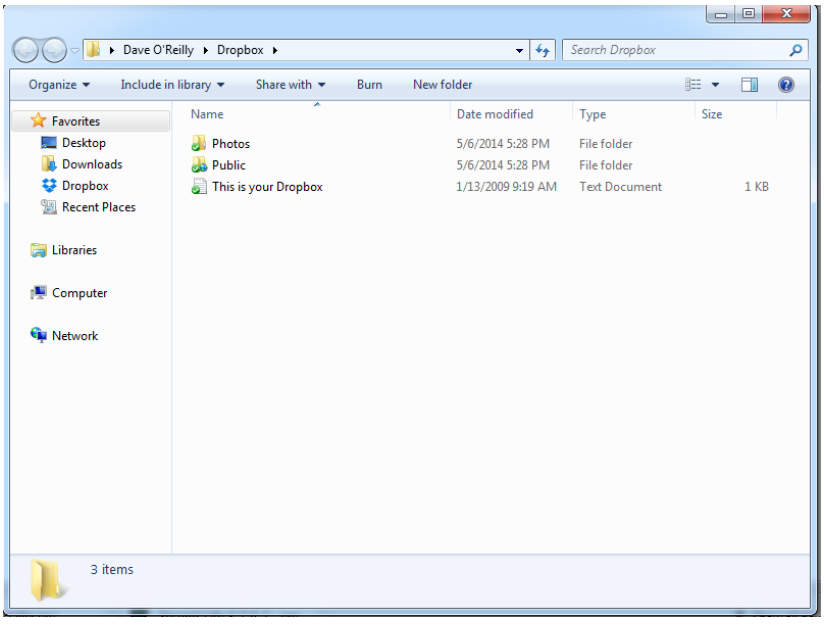
client application can be installed on the user's computer to access their shared files[97].

When DropBox is installed, an additional folder shortcut is added to the list of user's favourites, as shown in Figure **6**. A user can then simply drag files or folders from their computer into this shared folder to synchronise them with DropBox.

Having shared files from a computer using DropBox it is possible to access them through a variety of methods, including through a web browser, as shown in Figure **7**.

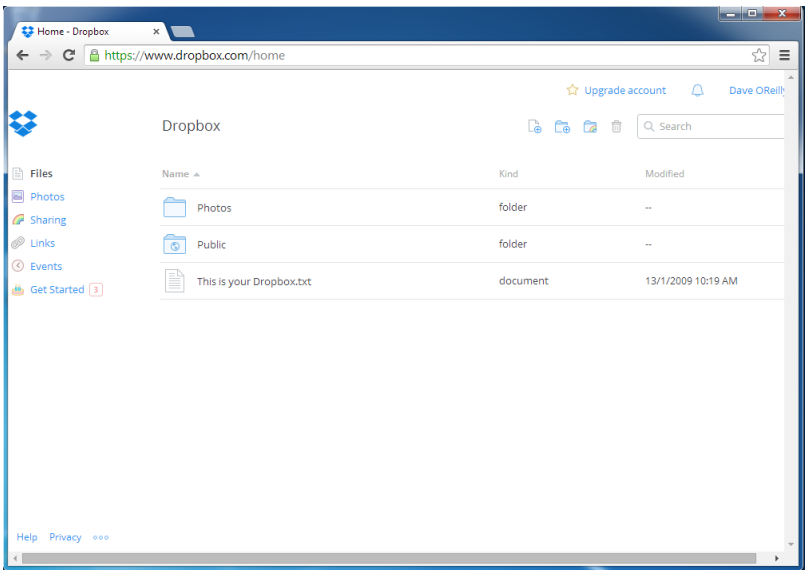
Regarding virtual currencies, credentials or digital representations of value could be stored in a text file, or any number of other file formats (Excel Spreadsheet, Word document, etc.) and stored in a DropBox folder. This information could then be accessed from the computer or from any remote location using a mobile device or web browser.

Figure 6: Dropbox added to favourites



[96] https://www.dropbox.com/
[97] For the purposes of this case study, DropBox version 2.6.31 is used on Windows 7 Professional 64-bit.

Figure 7: Dropbox web interface



4.3.3 Network Investigation

By capturing and analysing the network traffic to and from a suspect's computer it may be possible to identify communication that is indicative of the use of virtual currencies. In particular, the following categories of traffic may be identified:

- Involvement in a distributed currency peer-to-peer network.
- Engagement of the suspect computer with a virtual currency administrating authority or a virtual currency exchange.
- The use of cloud services, as discussed in Section 4.3.2.

Specialist network investigators will be required to perform this type of investigation and there are a number of issues that may complicate the collection of this type of evidence.

Firstly, the communication between the suspect computer and the computer with which they are communicating will, in all probability, be encrypted. This is virtually certain to be true in the situations under consideration in this manual, where financial transactions are being carried out. The implication of this fact is that it will not be possible through network traffic analysis to see the content of the communication that has taken place. However, even if the communication is

encrypted, it is still possible to establish that the communication between two particular IP addresses has taken place; between the IP address of the suspect's computer and an IP address associated with a virtual currency exchange, for example.

Secondly, there are options available online for individuals who are keen to shield the fact that they are the source of particular communication. These are known as anonymising proxies, and there are several types available. The first, and perhaps most famous, is Tor, previously known as "The Onion Router".[98] Tor operates by encrypting and forwarding traffic through a series of intermediary nodes. The traffic exits the tor network at some point, and will appear to other servers on the Internet as if it is originating from that point and not from the true source (i.e. the suspect's computer). Tracing the traffic back to the true source is extremely difficult, if not impossible.

Another alternative is the use of web-based anonymising proxies.[99] These operate by performing browsing requests on behalf of a user who simply enters the web site they want to browse into the website of the anonymising proxy, rather than directly into their own web browser. If such a service is used, it may be possible, through the appropriate legal channels, to uncover the identity of the true source of the traffic[100], in the following manner:

- Direct contact with the proxy service in question with the request seeking disclosure of requested information, based on Terms of Service or Privacy Policy that do not specifically prohibit this;[101]
- Police-to-police cooperation procedure seeking production order through 24/7 point of contacts (for Parties to the Council of Europe Convention on Cybercrime) or through G8 Network of High-Tech Crime Units, or through Interpol national contact points where none of the former can provide assistance. The ability or expedience of response is entirely dependent on the receiving authority; however, is going to be much faster than formal mutual legal assistance requests;
- Mutual legal assistance procedure launched through central prosecution office or Ministry of Justice, which is then fully managed by the authority in question; expediency is a major concern for such procedures.

[98] https://www.torproject.org/
[99] http://www.hidemyass.com/
[100] For example, http://www.theinquirer.net/inquirer/news/2112002/hidemyass-hide-ass
[101] http://hidemyass.com/legal/privacy/

4.4 Engagement with Administrating Authorities/Currency Exchanges

In line with the procedural powers and investigative tools discussed in previous sections of this Module, engagement of administrating authorities of centralized virtual currencies is going to be established and developed along the lines of public-private cooperation models tested in cybercrime investigations. See Section 5.7 for further discussion of public-private cooperation.

First of all, direct contact with the administrating authorities may be attempted based on the Terms of Service or Privacy Policies, many of which contain clauses on the cooperation with law enforcement, waiver of confidentiality guarantees and/or retention of certain data (accounts, transactions, etc.) for certain periods of time. Legal departments of administrating authorities may be willing to cooperate directly with foreign law enforcement unless there are specific regulations prohibiting such practice.

Being incorporated as legal entities in their respective jurisdictions, central administrating authorities will be, in any case, obliged to cooperate with local law enforcement in investigation of criminal offences. That is why police-to-police cooperation modalities are a preferred approach in many cases where direct, informal cooperation is unlikely or is taking too much time. Police cooperation modalities have been discussed numerous times throughout this manual, including 24/7 point of contacts under the Convention on Cybercrime, G8 Network of High-Tech Crime Units, or Interpol national contact points who will be eligible to undertake specific actions on behalf of foreign law enforcement, such as expedited preservation of stored computer data or other investigative actions allowed in the framework of bilateral agreements.

Mutual legal assistance procedures are most formal procedures that are based on traditional cooperation procedures in criminal cases in the framework of bilateral or multilateral treaties. Mutual legal assistance requests concerning central administrative authorities and investigative activities to be taken should be routed through central channels for MLA cooperation, which are primarily chief (General) prosecutor's offices or Ministries of Justice.

The approach to exchanges of decentralized or centralized virtual currencies would not be different from the one employed with regard to central administrative authorities. Even where such institutions are incorporated into the traditional financial systems of their respective states, exchange services related to virtual currencies may not be covered by applicable financial regulations; therefore, for public-private cooperation purposes, currency exchanges should be treated as regular legal entities incorporated in respective jurisdictions. Therefore, production orders can be served on such entities either

through police cooperation modalities (where such procedures are allowed) or, more realistically, through formal MLA procedures.

5 Countermeasures

Several countermeasures and good practices have been identified in previous studies that are applicable to the case of virtual currencies. Many of the countermeasures cited below arise from studies into broader issues of cybercrime, money-laundering, financing of terrorism as well as search, seizure and confiscation of proceeds of crime on the Internet. Nevertheless they are applicable in the case of virtual currencies specifically, as will be discussed in the sections that follow.

5.1 Implementation of the FATF Recommendations

The FATF publishes a comprehensive framework of measures for countries to implement in order to combat money-laundering and terrorist financing, as well as the financing of proliferation of weapons of mass destruction.[102] Many of these recommendations are applicable to, or can be interpreted in the context of, virtual currencies.

The FATF Recommendations are intended as an international standard, which countries should implement through measures adapted to their own particular circumstances. The document sets out the essential measures that countries should have in place to:

- Identify the risks, and develop policies and domestic coordination.
- Pursue money-laundering, terrorist financing and the financing of proliferation of weapons of mass destruction.
- Apply preventative measures for the financial sector and other designated sectors.
- Establish powers and responsibilities for the competent authorities (e.g. investigative, law enforcement and supervisory authorities) and other institutional measures.
- Enhance the transparency and availability of beneficial ownership information of legal persons and arrangements.
- Facilitate international cooperation.

Full detail on each of the recommendations, further reading and other references can be found in the FATF recommendations.

[102] "International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation – The FATF Recommendations", FATF-GAFI, February 2012. (Source: http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf)

5.2 Reporting

Frauds and money-laundering on the Internet often involve the use of large volumes of small transactions using both willing and unwilling money mules. This technique presents challenges from an investigative point of view since each individual transaction is very small and awareness of the fact that these individually small transactions can form part of a much larger criminal network is relatively low. Even when suspicious transactions are identified, the collation of a large volume of low value transactions and the subsequent identification of the true nature of the criminal activity can be difficult.

In the case of virtual currencies, the lack of regulation of virtual currency service providers means that there is often very limited, or no, reporting obligations on those organisations. Additionally, in the case of decentralised virtual currencies where there is no central administrating authority upon which a reporting obligation could be placed, there are significant technical obstacles to a formal structure for reporting of suspicious activity.

Several studies cite reporting, or other techniques for enhancing knowledge of criminal tools and techniques as an example of good practice.[103], [104] This can also include gathering of operational data to assist with detection and investigation of Internet crimes.

Numerous examples can be found of cooperation for the purposes of gathering and collating information specifically relating to the use of Internet services to commit crime, including laundering funds. These include:

- The Internet Crime Complaint Centre (IC3) in the United States.[105]
- MELANI in Switzerland.[106]
- The National Fraud Reporting Centre in the UK.[107]

The purpose of these initiatives is to allow various stakeholders, either members of the public, businesses or other victims of crime on the Internet to report to a central location. The central location can then analyse the reported activity to identify patterns or other intelligence that could be helpful in initiating of progressing an investigation.

---

[103] Chapter 8 of "Comprehensive Study on Cybercrime", UN Office on Drugs and Crime, February 2013 (draft).

[104] Section 4.1 of "Criminal money flows on the Internet: methods, trends and multi-stakeholder counteraction.", Council of Europe Global Project on Cybercrime and MONEYVAL, March 2012. (Source: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/reports-presentations/MONEYVAL_2012_6_Reptyp_flows_en.pdf)

[105] http://www.ic3.gov/

[106] http://www.melani.admin.ch

[107] http://www.actionfraud.org.uk/home

The intelligence that can be gathered through such reporting initiatives could, in principle, also be helpful in the detection and investigation of laundering crime proceeds on the Internet, including through the use of virtual currencies.

One example of a case where such reporting would be helpful is in cases where known suspect accounts with traditional financial services are used to fund virtual currency accounts. In such cases, knowledge of which virtual currency accounts were funded, and where those funds were subsequently transferred to, would help to close gaps in knowledge that may be introduced in the first place by the use of virtual currencies.

5.3 Public Awareness

There are many ways in which criminals exploit the ignorance of members of the public. Some examples include:

- Phishing emails/websites purporting to be from a financial institution tricking a customer into providing the criminal with their banking credentials. This exploits a lack of customer awareness of the fact that banks do not communicate with their customers in this way.
- Spam emails containing malware exploits a lack of customer awareness that they should not open attachments from people they do not know.
- Job offers and other inducements to become money mules exploiting customer naiveté with attractive, "too good to be true" jobs.

In these and other cases, effective and on-going programmes of public awareness can help to combat these techniques.

In the case of virtual currencies, awareness of the lack of protection, including the dangers of the irreversible nature of virtual currency transactions would be important. Mule recruitment activity relating to the use of virtual currencies could also be treated in a similar way.

5.4 Harmonised Legal Framework

A harmonised legal framework based on the adoption of international instruments is often cited as an important countermeasure against many forms of crime, including crimes on the Internet.[108, 109]

[108] Recommendation 36 in "International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation – The FATF Recommendations", FATF-GAFI, February 2012. (Source: http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf)

[109] Section 4.4 of "Criminal money flows on the Internet: methods, trends and multi-stakeholder counteraction.", Council of Europe Global Project on Cybercrime and MONEYVAL, March 2012. (Source:

The inherently international nature of most virtual currencies, and the consequent need for cross-border investigations and cooperation in cases of laundering crime proceeds is important to bear in mind in this context.

Harmonised legal frameworks are important for a variety of reasons including facilitating cross-border investigations, and therefore constitute an important countermeasure in the case of virtual currencies.

Harmonized legal frameworks are, first of all, important for formal international cooperation modalities, be it police-to-police cooperation or mutual legal assistance, which are based on the principle of dual criminality. Dual criminality seeks to ensure that the criminal conduct is similarly criminalized in both requesting and requested jurisdictions, and is an absolute prerequisite for such cooperation to take place.

Secondly, harmonized legal frameworks contribute to crime prevention, so that criminalization of offences or other incorporation of illegal acts into the law is evenly implemented across jurisdictions in order to prevent "safe havens" for criminals. Such concerns are particularly valid for illegal use of virtual currencies, both in the sense of cybercrime and money-laundering offences, since online environment is highly conducive to transnational nature of criminal activity.

Finally, harmonized legal frameworks are an important element in compliance with international monitoring by either money-laundering (such as FATF, MONEYVAL) or cybercrime (such as the Council of Europe Cybercrime Committee) institutions. Harmonization in this context is important for further development of the law in these areas enabling, in a longer term, increased efficiency of national authorities in preventing and suppressing the relevant offences.

5.5 Specialised Units

5.5.1 Specialised Units for Financial Investigations

Financial investigations are investigations into the financial affairs related to criminal conduct, the goal of which is to identify and document the movement of money during the course of criminal activity. A financial investigation involves the collection, collation and analysis of all available information with a view towards assisting in the prosecution of crime and in the deprivation of the proceeds and instrumentalities of crime. A financial investigation can be used as

http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/reports-presentations/MONEYVAL_2012_6_Reptyp_flows_en.pdf)

an instrument to reveal undiscovered predicate offences and to identify other people and companies involved in criminal activity[110].

In line with FATF Recommendation 30 there should be designated law enforcement authorities that have responsibility for ensuring that money-laundering, predicate offences and terrorist financing are properly investigated through the conduct of a financial investigation. Interpretive Note to Recommendation 30 requires a 'parallel financial investigation' which refers to conducting a financial investigation alongside, or in the context of, a (traditional) criminal investigation into money-laundering, terrorist financing and/or predicate offence(s). Law enforcement investigators of predicate offences should either be authorised to pursue the investigation of any related money-laundering and terrorist financing offences during a parallel investigation, or be able to refer the case to another agency to follow up with such investigations.

Thus, numerous models for the structure and role of specialised financial investigation units are possible and they may not be enforcement authorities, *per se*. In any case the central role in financial investigations normally resides with Financial Intelligence Units (FIU) that serve as a national centre for the receipt and analysis of: (a) suspicious transaction reports received from banks and other designated reporting entities; and (b) other information relevant to money-laundering, associated predicate offences and terrorist financing, and for the dissemination of the results of that analysis.

Recommendation 30 also supports the use of multi-disciplinary groups in financial investigations. The assembling of multi-disciplinary groups to conduct financial investigations is well-understood best practice[111]. Such groups may consist of financial investigators, experts in financial analysis, forensic accountants, forensic computer specialists, prosecutors and asset managers. Experts from other agencies may also be appointed or seconded such as from a regulatory authority, FIU, tax authority, auditing agency, inspector general or even from the private sector. Further discussion of inter-agency cooperation modalities can be found in Section 5.6.

In the case of virtual currencies, specialised financial investigative units can draw on their experience investigating laundering crime proceeds using more traditional methods. This knowledge can be effectively combined with the

[110] Paragraphs 14 and 15 of "FATF Report – Operational Issues: Financial Investigations Guidance", FATF-GAFI, June 2012. (Source: http://www.fatf-gafi.org/media/fatf/documents/reports/Operational%20Issues_Financial%20investigations%20Guidance.pdf)

[111] "FATF Report – Operational Issues: Financial Investigations Guidance", FATF-GAFI, June 2012. (Source: http://www.fatf-gafi.org/media/fatf/documents/reports/Operational%20Issues_Financial%20investigations%20Guidance.pdf)

expertise of specialised cybercrime units (discussed in the next section) to map this knowledge into the domain of virtual currencies.

5.5.2 Specialised Cybercrime Units

Specialised cybercrime units are a key element of the response to cybercrime. Specialised units in this case include both specialist law enforcement units but also specialised prosecutors[112].

The types and roles of specialised cybercrime units can vary, but predominantly they are to:

- Investigate and/or prosecute offences against computer data and systems
- Investigate and/or prosecute offences committed by means of computer data and systems
- Carry out computer forensics with respect to electronic evidence in general

There has been a trend in recent years towards a separation of responsibilities from the units responsible for the investigation of cyber- and other technology related crime and the units responsible for the gathering and examination of electronic evidence. This has arisen from the fact that in a number of countries, unmanageable backlogs of cases built up that required analysis of electronic evidence by a small group of investigators ostensibly responsible for cybercrime investigations. This led to the acknowledgement that an increasing number of crimes of all types involve some component of electronic evidence and therefore the forensic analysis of electronic evidence is nowadays increasingly integrated into mainstream forensic structures.

The function of specialised units will depend on the legislation that provides the legal basis for the unit, the department to which the unit is attached, internal structure of the authority and many other factors, but some common patterns can be observed:

- Units that investigate crimes committed against computer data and systems or by means of computer data and systems. These units may also have an internal computer forensic capability.

[112] Chapter Five of the UNODC Comprehensive Study on Cybercrime; see also "Specialised cybercrime units – good practice study", Prepared jointly by the CyberCrime@IPA project of the Council of Europe and the European Union, Global Project on Cybercrime of the Council of Europe and the European Union Cybercrime Task Force, November 2011. (Source: http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/Octopus2011/2467_HTCU_study_V30_9Nov11.pdf)

- Units that are responsible only for collecting and analysing electronic evidence.
- Units that coordinate investigative activities or gather intelligence but do not have an investigative function themselves.
- Units that are competent to investigate a specific crime.

In investigations involving the use of virtual currencies, there are many aspects that will be similar with other cybercrime investigations, so the technical expertise of specialised cybercrime investigators and forensic experts will be extremely helpful to ensure that the required evidence is gathered, and gathered correctly.

5.6 Inter-agency cooperation (public-public cooperation)

Depending on the specific details of each particular country, different agencies/authorities may be responsible for financial investigations, confiscation of proceeds, measures against money-laundering, cybercrime, forensic analysis and so on. Effective cooperation between these agencies to detect and investigate cases involving laundering of crime proceeds on the Internet, is an important condition for success.

In the case of virtual currency investigations, which have features in common with both cybercrime investigations and investigations of laundering crime proceeds on the Internet using other techniques, inter-agency cooperation will also be important.

Structures for inter-agency cooperation can be categorised as formal or informal. Formal arrangements, where there is a permanent infrastructure or arrangement (such as a Memorandum of Understanding) put in place to facilitate the cooperation. Equally important and much less well understood and appreciated are the informal arrangements that frequently exist between agencies.

Some examples of ways in which countries have implemented inter-agency cooperation are:

- Drawing together of expertise from multiple agencies to identify investigative challenges.
- Analyse representative cases by carrying out checks with national police authorities.
- Describe enforcement approaches from the view of the police and the supervisory authority.
- Establishing information sharing systems whereby agencies can be made aware of previous or on-going investigations into the same person

and/or legal entities. This helps to avoid replication, and promote cross-fertilisation.
- Establishing policies and procedures that promote the sharing of information/intelligence.
- Establishing a process whereby disputes are resolved in the best interest of the investigation.
- Competent authorities establishing written agreements such as Memoranda of Understanding or similar to formalise these processes.

Case Study: Focal Point for Reporting

Consider as an example of formal cooperation, the establishment of a focal point for the reporting of crimes. The importance of reporting as a countermeasure has already been discussed in Section 5.2.

Members of the public can often have difficulty knowing where and how to report crime. Reports from members of the public can be extremely important in identifying large-scale crimes on the Internet. This is because, considering the laundering typology mentioned in Module 2, a large number of small transfers are made using mule accounts that the amounts involved in individual crimes may be small.

Once the crime has been reported it is possible for the reporting point to identify crime patterns that may not otherwise have been identified. As well as this, it is possible for the reporting point to forward the reported crime to the appropriate unit for investigation.

Several examples of this model exist in practice.

One such example is the US Department of Justice website for directing members of the public to the appropriate authorities to report computer hacking, fraud and other Internet-related crime[113].

Another example is the Internet Crime Complaint Center (IC3)[114]. This is a partnership between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C). Its mission is to serve as a vehicle to receive, develop and refer criminal complaints regarding the rapidly expanding arena of cybercrime. This gives members of the public of cybercrime a way to alert authorities of suspected criminal or civil violations. It also provides law enforcement and regulatory agencies at

[113] http://www.justice.gov/criminal/cybercrime/reporting.html
[114] http://www.ic3.gov/default.aspx

federal, state and local level with a central referral mechanism for complaints involving Internet related crimes.

Case Example: Secondments to FIU

In *Korea*, a number of agencies have seconded a number of officials to the FIU. These secondees are responsible for leading the analysis of Suspicious Transaction Reports relating to their area of specialism, and identifying those which should be investigated by law enforcement agencies. In 2012 these compromised nine secondees from the public prosecutor's office, eight from the police, seven from the tax administration, seven from the customs administration, one from the Financial Supervisory Service and one from the Bank of Korea. For the period of their secondment to the FIU, these officials cannot directly access information held by their own agency, but must access information through the usual FIU gateway.

The *Spanish* tax administration has also seconded six of its officers to the FIU, to assist in analysing Suspicious Transaction Reports. As in Korea, seconded officials in Spain may share their skills and experience, but are not able to access tax information which, if required, must be obtained through normal channels using the FIU's dedicated point of contact within the tax administration.

The *Netherlands* tax administration has seconded a number of its officials to work as liaisons in the FIU. These staff work alongside FIU personnel in analysing Unusual Transaction Reports, but have direct access to tax administration databases to support them in this.

In *Greece*, personnel are seconded to the FIU from each of the agencies represented on the FIU's Board. These trained and experienced specialists work in analysing Suspicious Transaction Reports, with access to their respective agencies' databases.

The *Portuguese* tax and customs administration has personnel assigned to a liaison group located within the FIU.

In the *United States*, all large federal agencies, including the tax administration, have officials posted to the FIU, to act as liaisons in facilitating the sharing of information, typologies and trends.

The *United Kingdom* tax administration has a small team embedded in the FIU since the mid-1990s, in order to fully exploit Suspicious Transaction

Report data in the execution of its tax administration, law enforcement and other functions.

In *Belgium*, three officials from the police work as liaisons within the FIU.

In *Finland*, the Asset Recovery Office is located within the FIU. The Asset Recovery Office is mainly staffed by personnel from the Finnish police, but also includes one official from the tax administration and one from the Enforcement Authority. In addition, 17 multi-agency regional groups have been established across Finland to trace the proceeds of crime, comprising 38 officials from the police, 20 from the tax administration and 19 officials from the Enforcement Agency.[115]

Case Study: National Inter-Agency Cooperation

The Netherlands Financial Expertise Centre (FEC) is a joint project between supervisory, investigation, intelligence and prosecution authorities involved in regulating or monitoring activity in the financial sector. Partners in the FEC are the National Tax and Customs Administration, the Fiscal Intelligence and Investigation Service (FIOD, which is structurally part of the NTCA), the National Police, the General Intelligence and Security Service, the Public Prosecution Service, the Netherlands Financial Markets Authority and De Nederlandsche Bank, with the Ministry of Finance and Ministry of Security and Justice as observers. The mission of the FEC is to monitor and strengthen the integrity of the financial sector, and tackle issues of financial integrity throught inter-agency co-operation. This entails sharing information and building a knowledge centre belonging to and for the benefit of participating agencies, containing the knowledge and expertise needed to safeguard the integrity of the financial sector. Risks that the FEC focuses on include money-laundering, property fraud, identity fraud including skimming from bank accounts, mortgage fraud, investment fraud, and cyber crime including phishing scams.[116]

[115] Page 72 of "Effective Inter-Agency Cooperation in Fighting Tax Crimes and Other Financial Crimes", OECD 2nd Annual Forum on Tax and Crime, June 2012.

[116] Page 25 of "Effective Inter-Agency Cooperation in Fighting Tax Crimes and Other Financial Crimes", OECD, Second Edition, 2013.

Case Study: International Coordination and Analysis

In 2013 the European Commission officially commenced operations of the European Cybercrime Centre (EC3) at Europol[117]. The purpose of the centre is to act as a focal point in the EU's fight against cybercrime, contributing to faster reactions in the event of online crimes. The role of EC3 is to support Member States and the European Union's institutions in building operational and analytical capacity for investigations and cooperation with international partners.

The mandate of EC3 is to tackle the following areas of cybercrime:

- That committed by organised groups to generate large criminal profits such as online fraud.
- That which causes serious harm to the victim such as online child sexual exploitation.
- That which effects critical infrastructure and information systems in the European Union.

Investigations into online crimes can often involve hundreds of victims at a time, and suspects in many different parts of the world. This requires law enforcement authorities to adopt a coordinated and collaborative approach across borders, together with public and private stakeholders. The EC3 aims to provide a collaborative approach in cooperation with:

- EU member states
- Key EU stakeholders
- Non-EU countries
- International organisations
- Internet governance bodies and service providers
- Companies involved in Internet security and the financial sector
- Academic experts
- Civil society organisations
- Computer Security Incident Response Teams (CSIRTs)[118] and the CERT-EU.

[117] https://www.europol.europa.eu/ec3

[118] CSIRTs (Computer Security Incident Response Teams) are the key specialist groups that are instrumental in protection of national critical information infrastructures through a variety of methods, mostly focusing on prevention, handling and mitigation of consequences of cyber-security incidents.

5.7 Public-private cooperation and information exchange

Public-private cooperation and information exchange has been highlighted the single measure with arguably the strongest impact on the prevention and control of criminal money flows on the Internet. The problem addressed by such sharing is the lack of use of existing information, held by domestic financial institutions and law enforcement authorities. There are also issues relating to public-private cooperation and information exchange where the private sector organisations are multinational service providers.

Many examples of public-private cooperation and information exchange can be found and most relate to national cooperation and information exchange[119] but public-private cooperation can be considered much more broadly.

In the first instance, it is important to define what is meant by the terms "public", "private" and "cooperation".

There are many different components of the public service that may be interested in cooperating with the private sector. For example, law enforcement authorities, prosecution authorities, judges, financial regulators, supervisory authorities, FIUs, other regulatory authorities, customs officials, military agencies, intelligence agencies, and so on. The nature and extent of the engagement that is possible, and the requirements needed to facilitate that engagement will depend on the type of public agency concerned.

Similarly, there are many private sector organisations with which public agencies may have in interest in cooperating with in the context of cybercrime, and virtual currencies specifically. Broadly, these can be divided into two categories: national and international corporations. With the international nature of the Internet, cybercrime and laundering crime proceeds on the Internet, international organisations can be in possession of information with can be critical to investigate cases of laundering crime proceeds. Examples of these organisations would be cloud and other Internet service providers (Microsoft, Amazon, Yahoo!, Facebook, Skype, Google, etc.), Internet payment service providers (PayPal, etc.), international financial organisations (Visa, Mastercard, Amex, etc.)

Within a national context, there are also important private sector organisations that can offer important information to investigations. The main examples in

[119] Section 4.7 of "Criminal money flows on the Internet: methods, trends and multi-stakeholder counteraction.", Council of Europe Global Project on Cybercrime and MONEYVAL, March 2012. (Source: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/reports-presentations/MONEYVAL_2012_6_Reptyp_flows_en.pdf)

this category are typically financial institutions, telecommunications providers and Internet service providers.

The nature of the cooperation will also depend on the parties intending to cooperate but common cooperation techniques include operational support, sharing technical knowledge and sharing intelligence, enabling and supporting compliance reporting and investigations.

To make a public-private cooperation effective, there must be a compelling business justification for all parties concerned. For public sector organisations the justification can be built from facilitating increased successful civil and criminal convictions or gathering operational intelligence. For private sector organisations the justifications can be reduction of fraud, sharing the cost of fraud prevention at an industry level, brand protection and corporate responsibility.

Case Study: Working with Financial Institutions

The Irish Banking Federation is the representative body for all financial institutions in Ireland. The IBF established a high-tech crime forum as a national public-private cooperation initiative to manage threats to the retail banking sector by cyber- and high-tech crime. The high tech crime forum meets four times per year to exchange information, hear about current and emerging threats, identify projects to be carried out at an industry level and to sponsor research and other initiatives.

The members of the forum include:

- Representatives from all of the online retail banks operating in Ireland.
- Law enforcement representatives from cybercrime unit
- Law enforcement representatives from credit card fraud unit
- Representatives from the Internet Service Providers Association of Ireland (ISPAI)
- Representatives from the Irish Payment Services Organisation (IPSO)
- Representatives from academia (UCD Centre for Cybercrime Investigation)

There have been a number of successful initiatives carried out by the high tech crime forum, some of which are summarised here:

- *Information exchange*:
  - Every bank reports on the types and amounts of cybercrime seen since the last meeting.
  - Internet service providers share information about observed

threats, trends and other relevant incidents.
    - The payment services organisation share information about payment card crime.
    - Law enforcement share information about emerging international trends.
- *Incident management and reporting centre*: The members of the high tech crime forum observed that it was very difficult to gain access to accurate information on the scale of the threat of cybercrime faced by financial institutions in Ireland. The members of the group launched a project to study this issue and based on the findings from the project agreed to collectively invest in infrastructure to which they would all report anonymous cybercrime incident data. This data would then be collated to provide accurate statistics and trends to the members about the number and amount of cybercrime incidents, including the reported losses.
- *Simulation exercises*: The members of the high tech crime forum agreed to conduct several simulated major cybercrime incidents. The purpose of these incidents was to investigate the effectiveness of internal response procedures in the financial institutions and how to structure coordination at an industry level, should that be required.
- *Operational support*: The high tech crime forum provided expertise to individual financial institutions and law enforcement in specific cases involving particularly technical cases.[120]

Case Study: Cooperation with Internet Service Providers

In January 2010, leading Georgian Internet Service Providers representing absolute majority of the telecommunications market have entered into the "Memorandum of Understanding between the Law Enforcement Agencies and Internet Providers based on the principles of cooperation in the field of cybercrime" with the Ministry of Internal Affairs. The document was the result of year-long negotiations between the Internet industry and the Government of Georgia in the framework of Project on Cybercrime implemented by the Council of Europe. The Memorandum is maintained by the Georgian National Communications Commission, which is an official registrar of the agreement.

The conclusion of the Memorandum was preceded by discussions between

[120] "Banks band together to tackle high-tech crime", Silicon Republic, August 2006. (Source: http://www.siliconrepublic.com/business/item/6595-banks-band-together-to-tack)

parties on the necessary changes to legislation, including preservation of stored computer data, as well as changes in the Law on Electronic Communications, as a result of which the principle of absolute subscriber confidentiality has been revoked.

The Memorandum recognizes the need to balance the privacy of individual users with the threats to information security, and inevitability of cooperation to achieve such balance. ISPs are regarded as equal parties in combating cybercrime along law enforcement authorities.

The Memorandum implements a number of important principles of cooperation, such as:

- Principle of minimum interference, so that cooperation activities have minimum effect on quality of Internet service and lead to Internet service disruption only in exceptional cases.
- Contact points are being devised and available 24/7 from both law enforcement and ISPs to enhance cooperation.
- Regular exchange of information and experience takes place (mostly through a yearly Cyber-Security Forum).
- Only written requests represent a basis for cooperation.
- Confidentiality of such communications is respected by both sides.
- Reasonable time is accorded to respond to requests – in practice rarely above 3 days.
- Where requested information cannot be provided by ISPs, written explanations are presented to law enforcement as to the relevant reasons.[121]

The Memorandum of Understanding is an enforceable and living document that is being actively used and referenced in cybercrime investigations.

5.8 Training

Training and awareness raising at all levels within the criminal justice system, including law enforcement, prosecutors and judiciary. Various projects, including this training manual, have been carried out to help provide the required training expertise and awareness raising material.

Some of the challenges highlighted are the absence of experienced practitioners to serve as trainers and also the integration of the required training into either initial or in-service training of the relevant professionals.

[121] The text of the Memorandum is available at the Council of Europe website: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20project%20balkan/June%2011_Duress_Cooperation_LEA_ISP/2215_MoU_Cooperation%20LEA-ISP_eng.pdf.

Case Study: Knowledge Sharing

In *Austria*, regular meetings and training sessions are held including officers from different agencies. This enables staff to develop and maintain personal contacts and have proved effective in improving the efficiency of joint working and information sharing. Inter-agency meetings to share strategic information relating to trends in financial crime, guidance on investigative techniques and best practice in managing cases, as well as cross-agency training sessions and conferences are also used in the Czech Republic, Luxembourg, the Netherlands, New Zealand and the Slovak Republic.[122]

Case Study: Cybercrime Training

In 2007, the European Cybercrime Training and Education Group[123] was established at Europol to coordinate cybercrime training initiatives and manage training material that had been developed through a number of EU projects. The aims of the group are to:

- Support international activities to harmonise cybercrime training across international borders.
- Share knowledge, expertise and find training solutions to issues identified.
- Promote standardisation of methods and procedures for training programmes and cooperation with other international organisations.
- Collaborate with academic partners to establish recognised academic qualification in the field of cybercrime and work with universities that have already created such awards making them available across international borders.
- Collaborate with industry partners to establish frameworks whereby their existing and future efforts to support law enforcement by the delivery of training, harmonised into an effective programme that makes best use of available resources.
- Support international partners by providing training material and trainers to support their efforts to train law enforcement on

[122] Page 74 of "Effective Inter-Agency Cooperation in Fighting Tax Crimes and Other Financial Crimes", OECD 2nd Annual Forum on Tax and Crime, June 2012.
[123] http://www.ecteg.eu/index.html

cybercrime issues globally.

A large number of technical courses have been developed, strictly for law enforcement use. The list of courses is:

- Linux as an Investigative Tool (part 1)
- Linux as an Investigative Tool (part 2)
- Applied NTFS Forensics
- Core Skills in Mobile Phone Forensics
- Internet Investigations
- Network Investigations
- Malware Analysis and Investigations
- Forensic Scripting using BASH
- Introductory Open Source IT Forensics and Network Investigation Course
- Live Data Forensics
- Macintosh Forensics Course
- Network Forensic Intermediate Course
- Solid State and other Storage Media Forensic Course
- Vista and Windows 7 Forensics
- Data Mining and Databases
- Intermediate Mobile Phone Forensics

Self Assessment

Question 1: Describe, from the perspective of substantive criminal law, interrelation between money-laundering and cybercrime in cases where virtual currencies are used.

Question 2: What can be an example of an offence of illegal access in relation to virtual currencies?

Question 3: Describe how use of online anonymizers (proxies) can be used as an element of crime in data interference offences, when such offences compromise the personal data of virtual currency users.

Question 4: Explain how the use of decentralized virtual currencies could be used to prove an element of "layering" in money-laundering charges?

Question 5: Explain possible correlations between computer-related fraud and money-laundering through the use of virtual currencies.

Question 6: Which CSIRT data can be used for financial investigators in money-laundering cases involving virtual currencies?

Question 7: What is the legal basis and requirements for interception of content data in cases involving virtual currencies?

Question 8: Explain procedural differences (in terms of law and practice) between expedited preservation of stored computer data versus search and seizure of computer data.

Question 9: Name at least three elements of the chain of custody of electronic evidence.

Question 10: Describe national institutions whose expert capacity might be useful in virtual currency-related investigations.

Question 11: Describe investigative indicators that may suggest the use of virtual currencies for the purposes of laundering crime proceeds.

Question 12: Discuss the types of evidence that may be gathered through forensic analysis of a suspect's computer that may provide information about the laundering of crime proceeds through virtual currencies. Use as a concrete example a Bitcoin wallet.

Question 13: Describe the information that may be available from virtual currency central administering authorities and/or virtual currency exchanges and the available options for gathering this information.

Question 14: Discuss how public-private partnership can be an effective countermeasure against the laundering of crime proceeds using virtual currencies. Use a case study to illustrate the points made.

Question 15: Discuss how inter-agency cooperation (public-public cooperation) can be an effective countermeasure against the laundering of crime proceeds using virtual currencies. Use a case study to illustrate the points made.

Basic Manual on the Detection And Investigation of the Laundering of Crime Proceeds Using Virtual Currencies

Module 4
Seizure of Virtual Currencies

1 Summary

The purpose of this module is to present legal requirements, procedures, tools and techniques for the seizure of virtual currencies.

2 Learning Objectives

By reading this module you will:

- Know the legal and institutional frameworks required both nationally and internationally to effect seizure of virtual currencies as proceeds or instrumentalities of crime.

- Be aware of procedural powers and extent of competencies, as well as institutions that are relevant in the process of seizure of assets in cases involving virtual currencies both at national and international level.

- Be aware of the techniques of seizure of virtual currencies as well as issues pertaining to prospective confiscation of such items.

3 Introduction

While previous parts of this Manual have dealt with money-laundering and cybercrime aspects of virtual currencies and offered solutions for law enforcement in dealing with virtual currency-related offences in the framework of traditional criminal justice administration – that is, investigating and prosecuting a relevant criminal activity – this section of the Manual focuses on practical ways in which proceeds and instrumentalities of such crime can be seized in order to effect their confiscation in favour of the State.

Seizure of proceeds or instrumentalities means application of procedures that prohibit transfer, conversion, disposition or movement of criminally obtained property which allows the competent authority or court to take control of the specified property.[1] Seizure of crime proceeds or instrumentalities of crime is an effective tool that is equally beneficial for the prevention (no further criminal use of the property is possible), investigation (property under control may not be moved or converted into another property) and administration of justice (indirect compensation of efforts against organized crime[2] and overall chilling effect on organized crime). Seizure of the proceeds/instrumentalities of crime can be equally efficient in virtual currency-related offences of money-laundering, bringing together all three elements of prevention, investigation and administration of justice in a coherent manner.

Seizure, freezing or confiscation of proceeds or instrumentalities of crime are complex processes both in terms of law and procedure. It only comes naturally that their application to virtual currencies is even more complex, due to the features of such currencies that have been extensively discussed in this Manual (anonymity, traceability and trans-jurisdictional transactions being just a few examples). In this context, while focusing on the seizure of the proceeds or instrumentalities of crime in the context of virtual currencies, this Module will only address such proceeds or instrumentalities in the form of centralized or decentralized virtual currencies; for example, seizure of malware that is used for hacking Bitcoin wallets belonging to individual users will not be addressed here.

Last but not least, the current Module is not intended to serve as a guide to confiscation of proceeds of virtual currency-related offences or their confiscation as instrumentalities of crime, focusing solely on issues of seizure of such assets. In fact, it can be argued that, once proper seizure procedures are applied, confiscation of virtual currency or its relative value would not be

[1] Financial Action Task Force, Glossary of FATF Recommendations, (Source: http://www.fatf-gafi.org/pages/glossary/s-t/).
[2] FATF Recommendation 38.

entirely different to confiscation of other forms of property, especially monetary instruments. In this respect, the corresponding sections of the Manual on International Cooperation for the Purposes of Confiscation of Proceeds of Crime, published by the United Nations Office on Drugs and Crime in 2012,[3] can be used as guidance for the confiscation of already seized assets or their corresponding value.

[3] https://www.unodc.org/documents/organized-crime/Publications/Confiscation_Manual_Ebook_E.pdf.

4 Definitions

Seizure of proceeds or instrumentalities of crime can be defined as prohibition of the transfer, conversion, disposition or movement of property on the basis of an action initiated by a competent authority or a court under a freezing mechanism. In contrast to "freezing", which means temporarily prohibiting the transfer, conversion, disposition or movement of property,[4] a seizure is effected by a mechanism that allows the competent authority or court to **take control** of specified property. The seized property remains the property of the natural or legal person(s) that holds an interest in the specified property at the time of the seizure, although the competent authority or court will often take over possession, administration or management of the seized property.[5]

There are also several important definitions that are particularly relevant in the context of seizure of crime proceeds, namely:

- **"Proceeds"** refers to any property derived from or obtained, directly or indirectly, through the commission of an offence. Such proceeds may consist of any type of property, whether corporeal or incorporeal, movable or immovable, and legal documents o documents that give title to or interest in such property;[6]
- **"Instrumentalities"** means any property used or intended to be used, in any manner, wholly or in part, to commit any criminal offence(s).[7]

These two definitions are directly relevant to the nature of virtual currencies, whether centralized or decentralized, due to their use as a means of electronic payment. Virtual currencies, due to the possibilities of anonymity of transactions (a case more applicable to decentralized currencies), can be used to conceal the criminal origin of the money used to purchase/exchange into such currencies; while investment into bitcoins can bring further proceeds in the form of more bitcoins being mined or their value increased through inflation of exchange rates.[8] Therefore, in the course of investigation and adjudication of offences that involve the use of virtual currencies - especially money-laundering offences - it would be challenging to draw a line between proceeds of crime and its instrumentalities. On a practical level, however, these designations will have no significant effect on the procedures or techniques used for seizure, since these will be essentially the same.

[4] UNODC, "Manual on International Cooperation for the Purposes of Confiscation of Proceeds of Crime", p. 2.
[5] Financial Action Task Force, Glossary of FATF Recommendations, (Source: http://www.fatf-gafi.org/pages/glossary/s-t/).
[6] Article 1(d, e) of the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances.
[7] Article 1(c) of the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism
[8] http://www.coindesk.com/price/.

5 Legal requirements and procedures

Identification, freezing/seizure and confiscation of crime proceeds are legal procedures that are increasingly recognized as particularly efficient measures in combating organized crime. Application of any of these procedures requires solid legal grounds to be present. The purpose of this section is, therefore, to give a brief overview of both international and national regulations and standards that need to be utilized and applied in the context of seizure of crime proceeds and instrumentalities.

5.1 International standards

This section of the Manual will present an overview of international regulatory framework for the seizure of crime proceeds. Understanding these standards, besides purely theoretical value, is important for knowing the basis for international cooperation, as well as basic standards applicable in this regard.

The approach to crime prevention and administration of justice in the form of measures enabling confiscation of proceeds of crime was spearheaded by the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, which enables seizure, freezing and confiscation of proceeds – or property of corresponding value – from drug-related crime, as well as reversal of burden of proof with regard to the lawfulness of the property.[9]

These principles were taken further by the 2000 United Nations Convention against Organized Crime and its Protocols, not only extending the above-noted possibilities for seizure and confiscation to most prevalent forms of organized crime, but also adding regulations for the member states in terms of international cooperation modalities for the purposes of seizure and confiscation, as well as management of seized assets.[10]

The United Nations Convention against Corruption, adopted in 2003, contains provisions similar in scope and content, extending seizure, freezing and confiscation to corruption-related offences as defined under the Convention, and introducing a new chapter on asset recovery .[11]

The need for efficient procedures for seizure, freezing and confiscation of crime proceeds and instrumentalities is also recognized by the Financial Task Force (FATF) Recommendations. In particular, they require confiscation of property laundered, proceeds from money-laundering or predicate offences,

[9] Article 5 of the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances.
[10] Articles 12-14 of the United Nations Convention against Transnational Organized Crime.
[11] Article 31 and Chapter V of the United Nations Convention against Corruption.

instrumentalities used in or intended for use in the commission of these offences, or property of corresponding value, without prejudicing the rights of bona fide third parties. Such measures should include the authority to: (a) identify, trace and evaluate property which is subject to confiscation; (b) carry out provisional measures, such as freezing and seizing, to prevent any dealing, transfer or disposal of such property; (c) take steps that will prevent or void actions that prejudice the State's ability to recover property that is subject to confiscation; and (d) take any appropriate investigative measures.[12] Most important of all, such measures may be taken (including confiscation) in the absence of a criminal conviction, i.e. before the competent court renders a final judgement on the merits of the criminal case.[13]

On a regional level applicable to the GUAM states, the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime Laundering of 1999, as supplemented by the 2005 Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism provide for similar tools and requirements as the documents noted above.[14]

5.2 National regulations and institutions

In order to allow for seizure and confiscation of the proceeds of crime, national jurisdictions need not only establish legal rules and requirements for relevant procedures under their law, but also to devise competent authorities that are able to effectively implement these powers.

From a substantive law perspective, all of the GUAM states criminalize legalization of proceeds of crime in their legislation.[15] With the exception of Ukraine,[16] an all-crime approach is used by these jurisdictions in relation to predicate offences, meaning that proceeds and instrumentalities of any crime can be subject to freezing, seizure and confiscation.

[12] FATF Forty Recommendations, recommendation 3 "Provisional measures and confiscation" (Source: http://www.fatf-gafi.org).

[13] More information on internationally applicable standards and instruments in the area of seizure of crime proceeds and instrumentalities can be found in UNODC compilation "An Overview of the UN Conventions and Other International Standards Concerning Anti-Money-laundering and Countering the Financing of Terrorism" (Source: https://www.imolin.org/pdf/overview_of_UN_conventions_2013.pdf).

[14] Sections 3 and 4 of noted Conventions.

[15] Article 193^1 of the Criminal Code of Azerbaijan; Articles 194 and 194^1 of the Criminal Code of Georgia; Article 243 of the Criminal Code of Moldova; and Article 209 of the Criminal Code of Ukraine.

[16] Article 209 of the Criminal Code of Ukraine envisages a minimum threshold of sentence (crimes punishable by deprivation of liberty or fine in excess of 3000 minimum wages) as well as exceptions for tax evasion offences (Articles 212 and 212^1 of the Criminal Code).

In the context of the GUAM states, procedures for seizure of criminal profits or crime instrumentalities are predominantly addressed by the criminal procedure framework.[17] While none of these provisions contain any prohibitive or restricting criteria that may limit their application to virtual currencies as proceeds or instrumentalities of crime, several observations are particularly relevant here:

- In the light of varying terms in which seizure of property is addressed and differing definitions of property, the nature of virtual currencies shall be taken into account while pursing seizure. Namely, all of the noted jurisdictions provide for seizure of instrumentalities of crime, while application of seizure proceedings to the proceeds of crime may be conditional on specific offences listed or the criteria of gravity;
- There are varying degrees of judicial involvement in the issues of seizure of property, including approval of an already conducted seizure in exigent circumstances, which has a direct effect on the expediency of the proceedings – an important concept in relation to electronic evidence;
- Some states refer to civil procedures applicable in cases of seizure of property, thus calling the need for specialized civil procedure knowledge that may not be readily available to the law enforcement agency effecting seizure procedures;
- All of the jurisdictions noted allow for seizure before conviction; therefore, the standard of proof required for seizure of criminal proceeds is below the standard required for the court decision on the merits of the case.

Another relevant issue is institutional authority to enforce seizure in criminal cases involving the use of virtual currencies. In the current state of affairs, the relevant functions in the GUAM states are assigned to law enforcement, which may use any criminal procedure action available under the Code of Criminal Procedure provided they have an investigative jurisdiction over the case; for the purposes of this manual these will be the units investigating legalization of illegal proceeds.[18]

However, it is generally agreed that dealing with the proceeds and instrumentalities of crime requires specialist knowledge, and the context of virtual currencies may require even further specialization that may not be

[17] Article 249 of the Criminal Procedure Code of Azerbaijan; Article 151 of the Criminal Procedure Code of Georgia; Article 203-204 of the Criminal Procedure Code of Moldova; Article 100 of the Criminal Procedure Code of Ukraine.

[18] Department for Combating Corruption at the General Prosecutor's Office of Azerbaijan; Anti-Corruption Department of the Chief Prosecutor's Office of Georgia; Service on Prevention and Combating Money-laundering at the National Anti-Corruption Center of Moldova; and the Financial Investigations Department at the Ministry of Revenue and Duties of Ukraine, with investigative actions also performed by the Ministry of Internal Affairs and/or State Security Service.

available within law enforcement itself. In such cases, expert examinations and reports of such examinations[19] may be necessary for effecting seizure of crime proceeds and instrumentalities, especially where motions for such actions need to be sanctioned by the judge.

5.3 Jurisdictional issues

Virtual currencies operate and thrive in the online environment that blurs national borders and elevates e-commerce into an international phenomenon. It comes as no surprise that, in this light, one of the most challenging features for recovery of crime proceeds in virtual currency-related offences is applicable jurisdiction, as well as the requirements for international cooperation that such determination is set to create.

It must be noted from the outset that there are no cases reported as of yet that involve seizure or confiscation of virtual currencies in an international context. Therefore, the following suggestions are based upon the general foundations for establishing jurisdiction in terms of seizure of virtual currency as crime proceeds/instrumentalities.

First of all, jurisdictional aspects of seizure of crime proceeds and instrumentalities bring forth the differences between centralized and decentralized virtual currencies. In cases of centralized virtual currencies, e.g. in-game currencies, exchange tokens are treated as licences to access certain features or services offered by an administrating authority, and thus remain, both technically and legally, under the control of the company issuing such tokens.[20] For the purposes of seizure of assets, it means that the jurisdiction where the administrating authority of the virtual currency is incorporated is, unless specifically regulated otherwise, a jurisdiction for the purposes of seizure and confiscation of crime proceeds.

Decentralized virtual currencies, especially crypto-currencies, render a different picture in this context. For example, bitcoins themselves do not exist in any form, even as a digital file; in fact, there are only records of transactions between different addresses, with balances that increase and decrease.[21] Therefore, if treated as proceeds or instrumentalities of crime, bitcoins cannot be thought of physically "residing" on a specific medium or even in a specific place. However, as they are transactions between individual users' Bitcoin addresses, bitcoins have an intrinsic connection to specific addresses over which specific users exercise effective control. Thus, in terms of jurisdictional

[19] Chapter XXXV of the Criminal Procedure Code of Azerbaijan; Article 144-146 of the Criminal Procedure Code of Georgia; Articles 142-153 of the Criminal Procedure Code of Moldova; Articles 242-245 of the Criminal Procedure Code of Ukraine.
[20] http://lindenlab.com/tos#tos4.
[21] http://www.coindesk.com/information/how-do-bitcoin-transactions-work/.

approach, under the public international law, territorial jurisdiction over proceeds or instrumentalities of crime in cases of crypto-currencies will be tied to the location of the wallet. In other words, the physical location of the hardware on which the wallet containing virtual currency is operational should be considered as the jurisdiction for the purposes of freezing, seizure and confiscation of the crime proceeds and instrumentalities.

A particular challenge to establishing jurisdiction in cases involving virtual currencies is cloud computing (already discussed in module 2 of this Manual). Virtual currency wallets stored on the cloud infrastructure may be subject to regular migration of data from one server to another, crossing state borders with ease. In cybercrime investigations facing the same challenges, this is often called "loss of location".[22] However, unless a significant revision of public international law is undertaken, the principle of territoriality remains a point of departure for establishing jurisdiction; therefore, all efforts must be made, through international cooperation modalities, to determine the location of a wallet as data residing on a specific server infrastructure in a specific jurisdiction.

[22] See, for instance, Council of Europe, Discussion Paper "Cloud Computing and cybercrime investigations: Territoriality vs. the power of disposal?", p. 5 (Source: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/internationalcooperation/2079_Cloud_Computing_power_disposal_31Aug10a.pdf).

6 Procedures and tools for seizure

The purpose of this section is to focus on existing approaches and techniques for the seizure of crime proceeds and instrumentalities that can be potentially relevant in terms of virtual currencies. To this end, practical procedures and considerations relevant to seizure and prospective confiscation will be described.

Similar to the approach employed throughout this Manual, procedural options for the seizure of crime proceeds and instrumentalities comprise activities aimed at detection of such proceeds (asset tracing) and actual seizure of such assets through available legal procedures. While this division may seem superficial on the surface, the practical considerations of virtual currencies as proceeds and instrumentalities of crime highlight the distinctions between these approaches, not least from an institutional standpoint.

The approaches and procedures listed in this section are structured in a certain order that attempts to apply the logic of criminal investigations to the context of virtual currencies. However, due to the new and untested nature of the issues of this very context, the sequence of actions and techniques provided herein is for general guidance only.

6.1 Step 1: Initiating financial investigations

A financial investigation involves the collection, collation and analysis of all available information with a view towards assisting in the prosecution of crime and in the deprivation of the proceeds and instrumentalities of crime.[23] The major goal of a financial investigation is to identify and document the movement of money during the course of criminal activity. The link between the origins of the money, beneficiaries, when the money is received and where it is stored or deposited, can provide information about, and proof of criminal activity.[24] In this respect, financial investigation is a process that is mostly parallel to the main criminal proceedings – be it cybercrime, fraud or money-laundering – and allows investigators to focus solely on the proceeds and instrumentalities of crime.

Financial investigations thus require specialized knowledge that may not be always available at regular law enforcement agencies. To address this, national jurisdictions can revert to multiple solutions:

[23] FATF Report, "Operational Issues - Financial Investigations Guidance", FATF/OECD 2012, p. 6.
[24] FATF Report, "Operational Issues - Financial Investigations Guidance", FATF/OECD 2012, p. 3.

- Creation of joint investigative groups by the prosecutor, with the coordination and division of tasks ensured by supervisory prosecution authority;
- Involving financial transaction experts into ongoing investigations, retaining full control of the criminal investigation by the requesting law enforcement agency;
- Separating the crime proceeds investigation from the core criminal investigation and ensuring feedback between the investigative authorities.

Whichever of these options is used, distinctive features of financial investigations should be kept in mind. One such feature, and a consideration of financial investigations, is the comparably relaxed standard of proof compared to criminal cases (i.e. money-laundering cases). Proof of criminal origin of the property and its proceeds does not require a proof beyond reasonable doubt, making the conduct of such proceedings different from mainstream criminal investigations.

Financial investigations focusing on virtual currencies as proceeds and instrumentalities of crime are still a relative novelty. Therefore, there are no tried and tested approaches in terms of dealing with virtual currencies; the following sections are thus an attempt to provide guidance as to most relevant investigative techniques that can be used in tracing, taking control of and managing virtual currencies.

6.2 Step 2: Asset tracing

Tracing assets or, to put it another way, following the trail of the money is an important part of financial investigations in order to establish the criminal origin of the proceeds or to determine crime instrumentalities. In asset investigations focusing on virtual currency, this can be deemed as the preparatory stage, which helps to determine the object of freezing or seizure, before such objects are actually seized.

Asset tracing, as any criminal or financial intelligence activity, relies on specific indicators – "red flags" – that may help and guide the investigator in determining the criminal nature of the proceeds/property in question. In fact, the red flags referenced to and discussed in the Module 3 of this Manual are relevant not only in terms of actual investigations, but also for the identification of transactions in virtual currencies. These red flags are:

- Large number of bank accounts held by the same virtual currency administrator or virtual currency exchange company (sometimes in different countries) apparently being used as flow-through accounts

(may be indicative of layering activity), without a business rationale for such a structure;
- Virtual currency administrator or virtual currency exchange company located in one country but holding accounts in other countries where it does not have a significant customer base (unexplained business rationale which could be suspicious);
- Back and forth movement of funds between bank accounts held by different virtual currency administrator or virtual currency exchange companies located in different countries (may be indicative of layering activity as it does not fit the business model);
- The volume and frequency of cash transactions (sometimes structured below reporting threshold) conducted by the owner of a virtual currency administrator or virtual currency exchange company do not make economic sense;
- Virtual currency systems that lack appropriate registration and/or transparency or are known to be popular with notable criminal groups.

As can be seen from these indicators, these are directed at the points of contact of the virtual currencies with the established financial institutions - that is, central administrators, currency exchanges, virtual currency payment processors, hosting services, merchant service companies, etc. One should bear in mind that virtual currency transactions operate beyond established financial institutions, and the anonymity of such transactions, reliance on cryptography, as well as absence of official record-keeping is going to make tracing of crypto-currencies an arduous, if not impossible, task. Even where such currencies, such as Bitcoin, keep an open, transparent ledger of all transactions available as open-source information (known as the Blockchain),[25] linking a specific transaction to individual users (wallets) may require information from other sources.

In this light, there are several other options in which assets can be traced in the virtual currencies context:

6.2.1 Option 1: Financial intelligence

Financial Intelligence Unit (FIU) should be considered as primary partner for law enforcement in identifying and tracing crime proceeds and instrumentalities due to direct access to financial information concerning suspected proceeds of crime and potential financing of terrorism. Financial intelligence offered by FIU is one of the keys to the effective investigation and confiscation of profits from crime.[26]

[25] https://blockchain.info/.
[26] UNODC Manual on International Cooperation for the Purposes of Confiscation of Proceeds of Crime, p. 24.

One of the major functions of a national FIU is to process and provide information that can be used for financial intelligence purposes. Among these, STRs (suspicious transaction reports) and analysis provided on these reports by the FIU is of particular value and relevance.

In cases of centralized virtual currencies, management of exchange tokens or in-game assets will be mostly performed by the administrating authority through the in-house channels that are removed from the traditional financial system of the state. Therefore, availability and value of STRs from central administrators will be usually linked with the degree of state regulation on virtual currencies and where such entities are obliged to file STRs to a national FIU.

In contrast to central administrating authorities, cases of decentralized currencies - in particular, crypto-currencies - STRs that focus on the red-flagged transactions performed by virtual currency exchanges would be particularly useful source of intelligence in financial investigations on proceeds and instrumentalities of crime.

Generally, law enforcement need to be familiar with the structure, role and authority of the financial intelligence unit in their own jurisdiction.[27] In addition to obtaining suspicious transaction reports, many financial intelligence units are authorized to collect and maintain reports on currency and large cash transactions, making financial intelligence units the central holders of significant financial data.[28]

6.2.2 Option 2: Monitoring of transactions

Information and intelligence necessary for financial investigations could be also obtained through monitoring or production orders.

“Monitoring order” means an order issued by the competent authority and directed at a financial institution, requiring disclosure to an authorized person of information concerning transactions carried out through an account held with the institution by a person named in the order. Such an order may require the financial institution to make the disclosure immediately after a transaction has been made; or on suspicion that a transaction is about to be made; or the order may direct the financial institution to refrain from completing or effecting the transaction for a specified period.[29]

---

[27] For more information concerning relevant authorities, functions and competence of FIUs, please consult the publication of the International Monetary Fund/World Bank “Financial Intelligence Units: An Overview“ (Source: http://www.imf.org/external/pubs/ft/FIU/fiu.pdf)

[28] UNODC Manual on International Cooperation for the Purposes of Confiscation of Proceeds of Crime, p. 44.

[29] UNODC Manual on International Cooperation for the Purposes of Confiscation of Proceeds of Crime, p. 3.

In the context of GUAM states, monitoring orders may be issued by both law enforcement and FIUs (with the exception of Azerbaijan). Law enforcement has the general power to monitor any account for suspicious activity related to money-laundering, terrorism financing, all predicate offences for money-laundering and any other criminal offence by virtue of the provisions of the criminal procedure legislation.[30] FIUs, on the other hand, also have the power to monitor bank accounts for suspicious activities, usually for all types of offences; the legal framework for this authority is laid down either by specialized anti-money-laundering legislation or the law on operative and detective activities.[31] The factors that can trigger the use of monitoring orders are: a request from a foreign authority (including FIUs), an internal analysis, an STR received from a reporting entity or a request from the prosecutor's office.

"Production order" means a judicial order addressed to a specified person to produce for the inspection of an authorized person any document that identifies or locates any property subject to forfeiture or confiscation or that determines the value of the property or benefit derived by a defendant from criminal conduct.[32]

In short, the purpose of such orders is to compel the person or entity named in the order to turn over information or copy thereof within a specified time. In terms of virtual currencies, such orders will be significantly different in application to cases of centralized and decentralized virtual currencies:

- Administrating authorities of centralized currencies can receive and process such orders directly and can be compelled to turn over such information;
- Since there is no centralized authority in cases of decentralized crypto-currencies, exchangers may be addressed by monitoring or production orders that may indicate specific customers and/or their accounts that need to be monitored and reported.

[30] MONEYVAL Research report, "The postponement of financial transactions and the monitoring of bank accounts", Council of Europe 2013, pp. 40-41 (Source: http://www.coe.int/t/dghl/monitoring/moneyval/Typologies/MONEYVAL(2013)8_Postponement.pdf)
[31] MONEYVAL Research report, pp. 38-39.
[32] UNODC Manual on International Cooperation for the Purposes of Confiscation of Proceeds of Crime, p. 4.

Case Study: Targeting Bitcoin Currency Exchange for Money-laundering

US Prosecutors arrested Charlie Shrem, a prominent 24-year-old advocate for Bitcoin, at John F. Kennedy International Airport in New York in January 2014. He is charged in connection with a money-laundering conspiracy that allegedly funnelled more than $1 million of the currency to users of the online black market site Silk Road. Another man, Robert Faiella, was also arrested in what the Manhattan U.S. Attorney's office said was a conspiracy to help Silk Road customers anonymously purchase everything from narcotics to forged passports.

Mr. Shrem ran Bitinstant, a New York exchange for buying and selling bitcoins that was one of the first to register with the Treasury Department. The company has attracted a high-profile investment of $1.5 million from Winklevoss Capital in 2013.

Prosecutors allege Shrem and Faiella sold more than $1 million of the digital currency to users of the Silk Road website. According to the complaint, Mr. Faiella, 52 years old, ran an "underground" Bitcoin exchange on the Silk Road website that sold the currency to users from December 2011 until October 2013. After receiving an order, Mr. Faiella allegedly obtained the currency from a New York City-based company, where Mr. Shrem was the chief executive officer, and then sold it back to users at a mark-up.

The company, which wasn't named in the complaint, allowed users to anonymously exchange cash for bitcoins. Mr. Shrem was also the chief compliance officer at the company, according to the complaint, and responsible for ensuring the company was in line with money-laundering laws.

According to the complaint, Mr. Shrem filled Mr. Faiella's orders for a fee, despite knowing that currency was going back to Silk Road users who could then use it buy narcotics and other contraband. Mr. Shrem gave Mr. Faiella discounts on bulk orders, concealed the orders from the other co-founder of his company and failed to file suspicious activity reports with authorities as required by federal law, according to the complaint. Prosecutors also said that Mr. Shrem personally bought drugs on Silk Road.

"Bitcoins are not inherently illegal and have known legitimate uses, but they are also known to be used to facilitate illicit transactions and to launder criminal proceeds, given the ease with which can be used to move money anonymously," an agent of the Internal Revenue Service, which investigated

the case, wrote in the complaint.

Both men are charged with one count of conspiracy to commit money-laundering and one count of operating an unlicensed money transmitting business. Mr. Shrem is also charged with one count of wilful failure to file a suspicious activity report. Mr. Faiella faces up to 25 years in prison, while Mr. Shrem faces up to 30 years in prison.[33]

6.2.3 Option 3: Disclosure of financial records

Disclosure of financial records is another avenue for the use of production orders, offering particularly valuable source of information for tracing proceeds and instrumentalities of crime. Anti-money-laundering requirements on banking and non-banking businesses require them to keep specific information about accounts and activity of their customers, which can be extracted and used a source of intelligence for identification of assets in question.

In terms of virtual currencies, such enquiries, as already noted above, should be directed to currency exchangers who are supposed to abide by the anti-money-laundering requirements, including record-keeping. Information about customers and their transactions in exchange of virtual currencies should be requested in compliance with the applicable data protection standards, and used solely for the purposes of investigation.

Wire transfers are frequently used for exchange of fiat money into decentralized virtual currencies such as Bitcoin and vice versa.[34] This, as well as other payment methods that are used by currency exchangers, would be another potentially valuable, documented source of information to focus on in terms of identifying proceeds and instrumentalities of crime.

6.3 Step 3: Taking control of assets

Once crime proceeds or instrumentalities are identified, they can be subject to seizure proceedings. Seizure, as noted above, implies taking control of specified property, with the competent authority taking over possession, administration or management of the seized property.

Although there is relevant experience in terms of seizing and confiscation of electronic money or accounts (intangible assets) that can be used as an analogy, virtual currencies, in absence of state regulation, operate beyond the realm of

[33] The Wall Street Journal, "Two Charged in Alleged Bitcoin-Laundering Scheme" (Source: http://online.wsj.com/article/BT-CO-20140127-709257.html)
[34] http://www.coindesk.com/information/how-can-i-buy-bitcoins/.

established financial institutions and transactions. When talking about seizure of virtual currencies as proceeds/instrumentalities of crime, differences between centralized and decentralized currencies lead to different approaches that may work in such cases.

6.3.1 Option 1: Seizing centralized currency items

For centralized currencies, assets in the form of virtual currency remain under the full control of the administrating authority. Therefore, seizure of these assets may be served upon legal companies in charge of asset administration, making it easier for law enforcement to seek and obtain compliance with their legitimate requests.

At the same time, there certainly are considerations as to the seizure of centralized currency items. Where systems such as WebMoney or now defunct e-Gold process assets that can be seized as virtual currency and then converted into monetary value, computer game assets, such as upgrades to virtual characters' clothing or battleships, would be of very little actual value to law enforcement and the state. Therefore, a value-based recovery – that is, a method of confiscation that enables imposition of a pecuniary liability (such as a fine, usually in multiples of the profit or benefit derived from the crime), which is realizable against any asset of the individual[35] – can be used instead to avoid these and other potential difficulties in management of such assets.

Case Study: Massive-Multiplayer Online Items

The Chinese company Shanda Interactive has been ordered to pay RMB 5,000 and apologize to a gamer of its in-house developed MMORPG "The World of Legend" for taking away his virtual assets.

The gamer surnamed Zhang discovered six virtual items, worth more than RMB1,500, missing from his game account on November 22, 2006 and contacted Shanda regarding the disappearance. Shanda said that the company had taken the items in accordance with a police investigation regarding the sale of stolen virtual items. According to the report, Shanda failed to follow police instruction and return the items after the investigation ended.[36]

Although the case discussed here is entirely unconnected with the money-laundering and crime proceeds context, it shows that the law enforcement

[35] UNODC Manual on International Cooperation for the Purposes of Confiscation of Proceeds of Crime, p. 5.

[36] MMOsite, "Game Company Forced to Pay for Seized Virtual Item", (Source: http://news.mmosite.com/content/2007-12-30/20071230222432466,1.shtml).

and the judiciary have relevant tools at their disposal when it comes to seizure and confiscation of virtual assets, and can apply value-based approach where efficiency of investigation is concerned.

6.3.2 Option 2: Seizing decentralized crypto-currencies

Crypto-currencies, in contrast to centralized virtual currencies, operate without any coordinating or centralized structure. Therefore, seizure orders need to be served upon individual users, while object of seizure would be virtual currency contained in the addresses/wallets associated with the user.

Theoretically, taking control of the virtual currency wallet can be done in two different ways. First would be to compel the user to surrender his/her credentials associated with the wallet to the seizing authority. The pros of such approach may include the possibility of further intelligence and investigative activities, since, at the level of transactions, ownership of the wallet is not visible due to anonymity; however, the cons far outweigh the pros in this regard:

- In the current state of affairs, availability of legal powers to compel the user to submit his/her confidential data is largely dependent on the legal system of the state. While, in the context of the GUAM states, refusal to provide login information may be interpreted as tampering with evidence attracting separate criminal charges, the lack of expediency in this approach and volatility of electronic evidence may work against the interest of the investigation;
- The lack of guarantees that, even if credentials for a wallet are handed over to the state, no copies have been made by the offender or crime associates that would allow to those individuals to regain control of the seized assets.

Therefore, the viable option at the moment is taking control over virtual currencies by using the regular transaction mechanisms to transfer the currency to the account (wallet) of the law enforcement authority. Naturally, there would be a number of steps involved in this process:

- Determining the amount of virtual currency items, wallets or both to be seized;
- Securing suspect's cooperation or exercising control over the wallet through other means permitted by law, so that the required sum can be transferred to a government-controlled wallet, pending liquidation upon forfeiture;
- Conformation of receipt duly recorded; or
- Where cooperation or control over the wallet is not viable:

- Determine the value of virtual currency to be seized in local currency based on exchange rate;
- Apply value-based recovery procedures.

Needless to say, value-based recovery can be used from the initial steps of the process, especially where direct seizure and control of virtual currency is not viable due to either security or asset management considerations.

One of the additional arguments in favour of transferring virtual currencies or their value to state accounts is that, in the absence of more detailed information, this seems to be a preferred method in those very few cases that have used seizure and confiscation of virtual currencies. Namely, in the already noted Silk Road case, the US Government appears to manage the largest Bitcoin wallet in the world comprised of currency seized from the mastermind of the Silk Road.[37]

Case Study: Seizure of Bitcoins in Drug-Related Crime

The US Drug Enforcement Administration has posted an official notice stating that it seized bitcoins from an individual for purchasing a controlled substance. According to Let's Talk Bitcoin, this may, in fact, be the first time a law enforcement agency has seized bitcoins.

The DEA notice shows that, among many other people, a Mr. Eric Daniel Hughes (AKA Casey Jones) had 11.02BTC, with a value of $814.22 USD, on April 12th, earlier this year. The digital money was taken in forfeiture as the individual was in violation of the Controlled Substances Act (21 U.S.C. §§ 801 et seq.), in the district of South Carolina.

The notice is a general release, detailing all of the forfeitures by US citizens in violation of the Controlled Substances Act, of which Mr Hughes is one of many. As such, there are no details in the notice as to how the bitcoins were actually seized. There is no indication the Bitcoin protocol was compromised. "Seizure" is probably a word used to imply that money was received in the process of a Silk Road sting operation, rather than actually seized from the Bitcoin user's wallet" said Andreas M. Antonopoulos, a

[37] International Business Times, "World's Biggest Bitcoin Wallet Owned by U.S. Government", (Source: http://www.ibtimes.com/worlds-biggest-bitcoin-wallet-owned-us-government-1514100).

security expert and Let's Talk Bitcoin contributor.

The Bitcoin address referenced in the notice, 1ETDwGUC1QcjYuehFr3u1FD3MvDaUs7SFy, can be seen on the blockchain receiving 11.02 BTC on April 12th 2013, which matches the DEA notice.[38].

6.4 Step 4: Management of assets

One of the challenges for law enforcement is the management of the items seized, where control of the assets is handed over to the state. Naturally, since the ownership of the property, pending confiscation decision, rests with the original owner, diligent care must be taken of the seized assets.

Virtual currencies, whether centralized or decentralized, represent the least of such challenges since, as digital items, they do not physically deteriorate. However, virtual currencies, especially decentralized crypto-currencies, are susceptible to very significant fluctuations in exchange rates,[39] which may be a concern for law enforcement from the perspective of pending confiscation in favour of the state. The differences in value at the time of asset tracing stage and the actual seizure may require a review of the amount and value of virtual currencies to be seized, although, in the view of open availability of the exchange rate data, this should not require expert review and support.

Where assets are seized as instrumentalities of crime, one of the issues is the preventive nature of the seizure, meaning that the instrumentalities of crime must be taken out of circulation. Although no cases have been reported as to the seizure of centralized or decentralized virtual currencies as instrumentalities of crime, there still may be the need to place the seized virtual currency (wallet contents) on removable hardware in order to take it "off the grid".

Similar logic would also apply to bitcoins that are seized as proceeds of crime and transferred to the wallet operated by the competent authority. It would be advisable, in these cases, to take the wallet and its contents "off the grid" by creating local files and storing those safely on removable and/or secure storage.[40] The reasons for this, besides the wish to protect seized property from manipulation through transactions and mining, is that virtual currencies, as digital items, may be inadvertently altered or lost through mismanagement,

[38] CoinDesk, "Bitcoins seized by Drug Enforcement Agency" (Source: http://www.coindesk.com/bitcoins-seized-by-drug-enforcement-agency/).
[39] http://www.coindesk.com/price/; http://dogepay.com/; http://www.ltc-charts.com/
[40] https://en.bitcoin.it/wiki/How_to_set_up_a_secure_offline_savings_wallet.

disruptions in service, or be compromised by means of a cyber-attack. These and other necessary security tips can be taken from the Bitcoin network itself.[41]

6.5 Features of international investigations

Financial investigations often reach beyond domestic borders; therefore, it is important that competent authorities have timely focus on both formal and informal international cooperation efforts and ensure they are maintained for the duration of the case. Establishing early contact aids practitioners in understanding the foreign legal system and potential challenges in obtaining additional leads and in forming a common strategy. It also gives the foreign jurisdiction the opportunity to prepare for its role in providing co-operation.[42]

Taking into account the trans-border nature of the Internet which serves as an exclusive platform for the operation of virtual currencies, international cooperation will be an essential element of financial investigations into virtual currency-related offences. To this end, both formal and informal cooperation modalities must be employed efficiently and, most importantly, in an expeditious manner due to volatility of electronic evidence and traces of crime proceeds.

Financial investigators can avail themselves of a multitude of cooperation modalities, such as:

- Cooperation through dedicated international cooperation networks targeting proceeds of crime, such as the Camden Asset Recovery Inter-Agency Network (CARIN),[43] the Stolen Asset Recovery Initiative (StAR), which is a partnership between the World Bank Group and the United Nations Office on Drugs and Crime (UNODC),[44] or more specialized networks for asset recovery, such as the Global Focal Point Network on Asset Recovery, a joint project of the StAR Initiative and Interpol focusing on proceeds of corruption;[45]

- Use police-to-police cooperation modalities, especially 24/7 contact points under the Council of Europe Convention on Cybercrime, G8 Network of High Tech Crime Units national contacts or Interpol contact points, who can provide both intelligence or execute data preservation and other investigative requests directly, without the need for lengthy mutual legal assistance procedures;

[41] http://www.coindesk.com/information/how-to-store-your-bitcoins/.
[42] FATF Report, "Operational Issues - Financial Investigations Guidance", FATF/OECD 2012, p. 31.
[43] http://www.assetrecovery.org/kc/node/baf520a5-fe6d-11dd-a6ca-f1120cbf9dd3.6
[44] http://star.worldbank.org/star/
[45] http://www.interpol.int/Crime-areas/Corruption/International-asset-recovery

- Make contact with FIUs in foreign jurisdictions, requesting access to STRs or other intelligence information or analysis, through the national FIU by means of the Egmont Secure Web[46] or other, bilateral modalities; and

- Engage in formal procedures with central authority (Prosecutor's Office) for transmitting mutual legal assistance requests to foreign jurisdiction.

In relation to the last option, without going into unnecessary detail on the legally complex mutual legal assistance practicalities, additional difficulty with utilizing mutual legal assistance requests for the seizure of centralized or decentralized virtual currencies is the lack of legal regulation for such currencies (already discussed in this Manual, Module 1), leaving their status in the financial system of the requested state open to interpretation. It has to be kept in mind that mutual legal assistance is a highly formalized process that relies on exact definitions and clear procedures, and is often prejudiced by the lack of understanding or willingness of the requested state to deal with the issues that may be alien to its legal system.

[46] http://www.egmontgroup.org/membership

Self Assessment

Question 1: What are the differences between crime proceeds and instrumentalities?

Question 2: What are the differences between freezing and seizure of crime proceeds and instrumentalities?

Question 3: Describe the need for expert assistance for identification and seizure of crime proceeds and instrumentalities.

Question 4: Explain how applicable jurisdiction will be determined in international investigations of decentralized virtual currencies as crime proceeds?

Question 5: List at least two “red flags” for the tracing of crime proceeds involving virtual currency exchanges.

Question 6: Explain the relevance of suspicious transaction reports (STRs) for identification of crime proceeds or instrumentalities in the context of virtual currencies.

Question 7: Please describe the process of seizure (taking control) of decentralized virtual currency.

Question 8: List at least two modalities for international cooperation in financial investigations.

Basic Manual on the Detection And Investigation of the Laundering of Crime Proceeds Using Virtual Currencies

Annex 1
Bibliography

This annex assembles the list of key publications referenced throughout the body of the manual.

Domestic Legislation

- **Azerbaijan**
  - "Criminal Code of Azerbaijan"
  - "Criminal Procedure Code of Azerbaijan"
  - "Law of Azerbaijan on Operative-Detective Activity"
- **Georgia**
  - "Criminal Code of Georgia"
  - "Criminal Procedure Code of Georgia"
- **Moldova**
  - "Criminal Code of Moldova"
  - "Criminal Procedure Code of Moldova"
  - "Moldovan Law on Combating Cybercrimes"
  - "Moldovan Law on Special Detective Activities"
- **Ukraine**
  - "Criminal Code of Ukraine"
  - "Criminal Procedure Code of Ukraine"

United Nations

- "International Convention for the Suppression of the Financing of Terrorism "
  - http://www.un.org/law/cod/finterr.htm
- "UNCITRAL Model Law on Electronic Commerce"
  - https://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model.html
- "UNCITRAL Model Law on International Credit Transfers"
  - https://www.uncitral.org/pdf/english/texts/payments/transfers/ml-credittrans.pdf
- "United Nations Convention against Corruption"
  - http://www.unodc.org/documents/treaties/UNCAC/Publications/Convention/08-50026_E.pdf

- "United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances"
  - http://www.unodc.org/pdf/convention_1988_en.pdf

- "United Nations Convention against Transnational Organized Crime"
  - http://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf

- "UNODC Comprehensive Study on Cybercrime"
  - Prepared by UNODC for the consideration of the open-ended intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime, according to the methodology agreed on by the expert group.
  - http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

- "UNODC Manual on International Cooperation for the Purposes of Confiscation of Proceeds of Crime"
  - https://www.unodc.org/documents/organized-crime/Publications/Confiscation_Manual_Ebook_E.pdf

- "UNODC Toolkit to Combat Trafficking in Persons"
  - http://www.unodc.org/documents/human-trafficking/Toolkit-files/08-58296_tool_3-5.pdf

- "UNODC Overview of the UN Conventions and Other International Standards Concerning Anti-Money Laundering and Countering the Financing of Terrorism"
  - http://www.imolin.org/pdf/overview_of_UN_conventions_2013.pdf

International, Regional and National Stakeholders

- **Asian Development Bank**

  - "Manual on Countering Money Laundering and the Financing of Terrorism"
    - https://www.unodc.org/tldb/pdf/Asian-bank-guide.pdf

- **Commonwealth of Independent States (CIS)**
  - "Agreement on Cooperation in Combating Offences related to Computer Information"
    - https://cms.unov.org/documentrepositoryindexer/GetDocInOriginalFormat.drsx?DocID=5b7de69a-730e-43ce-9623-9a103f5cabc0

- **Council of Europe**
  - "Convention on Cybercrime"
    - http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm
  - "Criminal money flows on the Internet: methods, trends and multi-stakeholder counteraction"
    - http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/reports-presentations/MONEYVAL_2012_6_Reptyp_flows_en.pdf
  - "Cybercrime training for judges and prosecutors: a concept"
    - http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Training/2079_train_concept_4_provisional_8oct09.pdf
  - "Discussion paper "Cloud Computing and Cybercrime Investigations: Territoriality vs. the power of disposal?""
    - http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/internationalcooperation/2079_Cloud_Computing_power_disposal_31Aug10a.pdf
  - "Electronic Evidence Guide: A basic guide for police officers, prosecutors and judges"
    - http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Electronic%20Evidence%20Guide/default_en.asp
  - "Explanatory Memorandum to the Council of Europe Convention on Cybercrime"
    - http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm
  - "Financial Investigations and Confiscation of Proceeds from Crime"
    - http://www.coe.int/t/dghl/cooperation/economiccrime/specialfiles/CARPO-ManualFinInv_eng.pdf

- "Judicial training: Introductory course on cybercrime and electronic evidence for judges and prosecutors"
  - http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/basic%20training%20for%20judges/Cyber_JudTrain_Basic_course_Manual_V_1_0.pdf

- "Law Enforcement Challenges in Transborder Acquisition of Electronic Evidence from "Cloud Computing Providers""
  - http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/reports-presentations/2079_reps_IF10_reps_joeschwerha1a.pdf

- "MONEYVAL Research report, "The postponement of financial transactions and the monitoring of bank accounts""
  - http://www.coe.int/t/dghl/monitoring/moneyval/Typologies/MONEYVAL(2013)8_Postponement.pdf

- "Specialised cybercrime units – good practice study"
  - http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/Octopus2011/2467_HTCU_study_V30_9Nov11.pdf

- "Strategic Priorities for the Cooperation against Cybercrime in the Eastern Partnership Region"
  - http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/CyberCrime@EAP/2523_EAP_Strat_Priorities_V7%20ENG.pdf

- "Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism"
  - http://conventions.coe.int/Treaty/en/Treaties/Html/141.htm

- **European Central Bank**

  - "Virtual Currency Schemes"
    - http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf

- **European Parliament**
  - "Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures"
    - http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:31999L0093
  - "Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market"
    - http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:en:HTML
  - "Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions"
    - http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009L0110&from=EN
  - "Directive 2011/83/EU on Consumer Rights"
    - http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32011L0083&rid=1
- **Financial Action Task Force (FATF)**
  - "FATF Report "Virtual Currencies – Key Definitions And Potential AML/CFT Risks"
    - http://www.fatf-gafi.org/topics/methodsandtrends/documents/virtual-currency-definitions-aml-cft-risk.html
  - "FATF Report – Operational Issues: Financial Investigations Guidance"
    - http://www.fatf-gafi.org/media/fatf/documents/reports/Operational%20Issues_Financial%20investigations%20Guidance.pdf
  - "Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services"

        - http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf

    - "Money Laundering Using New Payment Methods"
        - http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20using%20New%20Payment%20Methods.pdf

    - "Report on New Payment Methods"
        - http://www.fatf-gafi.org/media/fatf/documents/reports/Report%20on%20New%20Payment%20Methods.pdf

- **Financial Crimes Enforcement Network (FinCEN), United States Department of the Treasury**

    - "Guidance: Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies"
        - http://www.fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html

- **International Monetary Fund**

    - "Financial Intelligence Units: An Overview"
        - http://www.imf.org/external/pubs/ft/FIU/fiu.pdf

- **International Telecommunication Union (ITU)**

    - "The ITU Toolkit for Cybercrime Legislation"
        - http://www.cyberdialogue.ca/wp-content/uploads/2011/03/ITU-Toolkit-for-Cybercrime-Legislation.pdf

- **League of Arab States**

    - "Convention on Combating Information Technology Offences"
        - https://cms.unov.org/DocumentRepositoryIndexer/GetDocInOriginalFormat.drsx?DocID=3dbe778b-7b3a-4af0-95ce-a8bbd1ecd6dd

- **Organization for Economic Cooperation and Development (OECD)**

    - "Effective Inter-Agency Cooperation in Fighting Tax Crimes and Other Financial Crimes"

- http://www.oecd.org/ctp/crime/EffectiveInterAgencyCooperationinFightingTaxCrimes.pdf

- **Shanghai Cooperation Organization**
  - "Agreement on Cooperation in the Field of International Information Security"
    - http://www.fidh.org/en/Terrorism/Agreement-Between-the-Member (unofficial translation)

Basic Manual on the Detection And Investigation of the Laundering of Crime Proceeds Using Virtual Currencies

Annex 2
Glossary

1 Glossary of Terms

Please note that the definitions of terms provided in this glossary are for informational purposes only and are only applicable in the context of this manual.

Administrating Authority
See Centralised Virtual Currency

Bitcoin
A decentralised, peer-to-peer payment network that is powered by its users with no central authority or middlemen.

Block Chain
A public ledger of transactions maintained by certain types of decentralised virtual currencies (e.g. Bitcoin)

Centralised Virtual Currency
Centralised virtual currencies have a single administrating authority (administrator) i.e. a third party that controls the system. An administrator issues the currency; establishes the rules for its use; maintains a central payment ledger; and has authority to redeem the currency (withdraw it from circulation). The exchange rate for a convertible virtual currency may either be floating - i.e. determined by market demand for the virtual currency - or pegged - i.e. fixed by the administrator at a set value, such as gold or a basket of currencies.

Closed Virtual Currency
See non-convertible virtual currency

Computer-related Fraud
An assimilative offence that tailors traditional fraud offences to the environment of information and communications technology.

Computer Security Incident Response Team
Computer Security Incident Response Teams are specialist groups that mostly focus on prevention, handling and mitigation of consequences of cyber-security incidents.

Consumer Protection
The set of rules protecting the rights of consumers entitling them to a reasonable standard of goods and services received, and protecting them from unfair and unjust business practices.

Content Data
The communication content of the communication i.e. the meaning or purport of the communication, or the message or information being conveyed by the communication.

Convertible Virtual Currency
Convertible virtual currency has an equivalent value in real currency and can be exchanged back-and-forth for real currency.

Crypto Currencies
See decentralised virtual currencies

CSIRT
See Computer Security Incident Response Team

Currency Exchangers
See virtual currency exchange

Cybercrime
A concept that denotes both offences against computer data and systems, namely, offences against confidentiality, integrity and availability of data and systems, as well as offences committed by means of computer data and systems.

Data Interference
The offence of data interference aims to protect integrity and proper functioning or use of stored computer data or computer programs against damaging, deletion, deterioration, alteration or suppression of computer data without right.

Decentralised Virtual Currencies
Decentralised virtual currencies are distributed, open-source, peer-to-peer digital currencies that have no central administrating authority and no central monitoring or oversight.

Digital Currency
Digital currency is a digital representation of either virtual currency (non-fiat) or e-money (fiat).

Digital Representation
A representation of something in the form of digital data. A physical object such as a flash drive or a computer hard drive may contain a digital representation of a virtual currency but ultimately, the digital data itself, not the medium on which it is stored is the virtual currency.

Discretionary Prosecution
A concept that refers to the application of public interest standards to specific criminal cases in order to decide whether to initiate or continue prosecution or to divert the perpetrator into alternative solutions.

E-Commerce
Any form of business transaction between individuals and entities that uses electronic communications in place of physical exchange of goods or services.

E-Gold
A virtual currency established in 1996 that allowed users to open an account with a value denominated in grams of gold (or other precious metals) and the ability to make instant transfers of value to other E-Gold accounts. Shut down by the US courts in 2007.

E-Money
See electronic money

Electronic Evidence
Information generated, stored or transmitted using electronic devices that may be relied upon in court.

Electronic Money
A digital representation of fiat currency used to electronically transfer value denominated in fiat currency. Electronic money is a digital transfer mechanism for fiat currency - i.e. it electronically transfers value that has legal tender status.

Fiat Currency
The coin and paper money of a country that is designated as its legal tender, circulates and is customarily used and accepted as a medium of exchange in the issuing country.

Financial Intelligence Unit
Financial Intelligence Units are specialised supervision agencies that receive reports of suspicious transactions from financial institutions and other persons and entities, analyse them, and disseminate the resulting intelligence to local law enforcement agencies and foreign Financial Intelligence Units to combat money-laundering.

FIU
See Financial Intelligence Unit

Freezing
Temporarily prohibiting the transfer, conversion, disposition or movement of property. Contrast with seizure, which allows a competent authority or court to take control of the specified property.

Illegal Access
The basic offence of threats to and attacks against the security (i.e. confidentiality, integrity and availability) of computer systems and data.

Instrumentalities
Any property used or intended to be used, in any manner, wholly or in part, to commit any criminal offence(s).

Integration
The final stage of a money-laundering scheme which represents the return of the funds to the legal economy. See also money-laundering, placement and layering.

Layering
The second stage of a money-laundering scheme which usually consists of a series of transactions to conceal the origin of the funds. See also money-laundering, placement and integration.

Liberty Reserve
A virtual currency established in 2006 that operated until 2013, allowing users to register and transfer money with to other users with only a name, email address and date of birth.

Linden Dollars
A convertible, centralised virtual currency for use in the online virtual world "Second Life"

Misuse of Devices
The intentional commission of specific legal acts regarding certain devices or access data to be misused for the purpose of committing offences against the confidentiality, integrity and availability of computer systems or data.

Money-laundering
The process by which criminals disguise the original ownership and control of the proceeds of criminal conduct by making such proceeds appear to have derived from a legitimate source.

Monitoring Order
An order issued by the competent authority, directed at a financial institution, requiring disclosure to an authorised person of information concerning

transactions carried out through an account held with the institution by a person named in the order.

New Payment Methods
An expression used by the FATF to refer to prepaid cards, mobile payments and Internet payment services.

Non-convertible Virtual Currency
Non-convertible virtual currency is specific to a particular virtual domain or world such as a Massively Multiplayer Online Role-Playing Game (MMORPG) or Amazon, and cannot be exchanged for fiat currency under the rules governing its use.

Open Virtual Currency
See convertible virtual currency

Placement
The first stage of a money-laundering scheme which represents the initial entry of the funds into the financial system. See also money-laundering, layering and integration.

Predicate Offence
An offence whose proceeds may become the subject of any money-laundering offence.

Preservation
The concept that data, which already exists in stored form, be protected from anything that would cause its current quality or condition to change or deteriorate. Preservation does not necessarily mean that the data will be rendered inaccessible, so that legitimate users, depending on the exact specifications of the order, may still access the data.

Proceeds
Refers to any property derived from or obtained, directly or indirectly, through the commission of an offence.

Production Order
Used by law enforcement to compel a person to provide specified stored computer data, or a service provider offering its service to submit subscriber information.

Seizure
Application of procedures that prohibit the transfer, conversion, disposition or movement of criminally obtained property which allows the competent authority or court to take control of the specified property.

System Interference
The offence of intentional hindering of the lawful use of computer systems including telecommunications facilities by using or influencing computer data.

Technological Neutrality
The concept that technologies can be used for both legitimate and illegitimate purposes and therefore the core technology itself cannot be considered illegal due to the potential for its criminal use.

Virtual Currency
A virtual currency is a digital representation of value that can be traded on the Internet as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but does not have legal tender status in any jurisdiction.

Virtual Currency Exchange
An organisation that offers to buy or sell, or facilitate the buying and selling, of virtual currency in exchange for either fiat currency or other virtual currencies.

Virtual Machine
Software that allows a user to execute an operating system as an application on their computer.

WebMoney
A virtual currency established in 1998 that is based on providing its users with the ability to control individual property rights stored by other participants of the system. WebMoney has almost 25 million users at the time of writing.

Basic Manual on the Detection And Investigation of the Laundering of Crime Proceeds Using Virtual Currencies

Annex 3
Examples and Analysis Pertaining to the GUAM Countries

This annex provides a brief insight into the legal aspects of virtual currencies in the GUAM states, addressing related legal and institutional frameworks of money-laundering and cybercrime. These are grouped into relevant topics of general regulation of virtual currencies, aspects of money-laundering, and cybercrime regulations in respective states.

1 Regulation of virtual currencies

None of the GUAM states have adopted direct regulations related to centralized or decentralized virtual currencies. There is nothing extraordinary in this, since, at the time of writing of this Manual, only a handful of states worldwide are taking the very first steps in an attempt to address some issues raised by virtual currencies. This does not mean, however, that the lack of regulation with regard to virtual currencies absolves their use for illegal purposes (including money-laundering) from all sorts of responsibility. As has been discussed throughout this Manual, analogies and interpretations of existing provisions on money-laundering and cybercrime can and should be used to address the challenges raised by use for virtual currencies for money-laundering purposes.

Similar to global trends in this area, the need for regulation of virtual currencies in the GUAM states will become an agenda item when the number of users and transactions in virtual currencies reaches a certain threshold to become a concern. However, as the following case study demonstrates, virtual currencies can attract attention from policy makers and financial regulators even in cases where such, rather hypothetical, thresholds are yet to be met.

Case Study: Bitcoin status and regulation in Ukraine

In response to queries from Ukraine-based news source AIN.UA,[1] the National Bank of Ukraine (NBU) has issued its first formal legal guidance to its native Bitcoin community.

Most notably, the NBU has indicated that Bitcoin payment systems and payment infrastructure services must register with the agency and abide by existing laws related to the management of electronic money. The topic of whether Bitcoin businesses necessitate unique laws is being debated around the world, and as such, Ukraine's decision to use existing laws gives it a unique position on the global stage.

AIN.UA published the full comments it obtained from the NBU, which

[1] http://ain.ua/.

amount to a few paragraphs of direction, as well as a link to an existing payment systems and money-laundering law – "On Payment Systems and Funds Transfer in Ukraine" – which lies at the centre of the new guidance.[2]

Pursuant to Article 9 of the law, the NBU stated that Bitcoin businesses have the right to perform services only after registering with the government, suggesting that those that have not are in violation of current law.

Article 9 also requires payment service providers to:

- Enact a procedure for settling instances when it fails to perform services;
- Establish an organizational structure and formal channels to resolve member disputes;
- Provide information about the transfer of money to enhance consumer protection.

Further, the NBU cited Article 15 of the Act, which requires those with "the intention to issue electronic money"[3] to coordinate rules for its use consistent with current regulation.

While NBU officials did provide some legal clarifications for the wider virtual currency community, they also followed in the footsteps of other European nations that have issued warnings to citizens regarding Bitcoin's price volatility and lack of consumer protections. Said the bank: "We emphasize that all the risks associated with the use of so-called … crypto-currency … bear calculations." With this statement, Ukraine joins other European and Asian nations that have recently decided to increase consumer awareness of the risks of virtual currencies.[4]

[2] Full text of the guidance in response to AIN.UA query can be found at the following address: http://ain.ua/2014/02/14/513124 (in Russian only).
[3] Electronic money in this quotation should be interpreted as meaning "digital currencies" per the definitions provided in Module 1.
[4] CoinDesk, "Ukraine to Regulate Bitcoin Businesses Under Existing Laws" (Source: http://www.coindesk.com/ukraine-regulate-bitcoin-businesses-existing-laws/)

2 Money-laundering regulatory framework

All of the GUAM states are parties to key international instruments that require states to undertake efforts in preventing and combating money-laundering, including the United Nations Convention against Organized Crime, the United Nations Convention against Corruption, the United Nations Convention against illicit traffic in narcotic drugs and psychotropic substances and, in a regional context, the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism. The GUAM states are also part of the FATF global network, subject to monitoring of compliance with International Standards on Combating Money-laundering and the Financing of Terrorism & Proliferation (FATF Recommendations). Similarly, in a European context, the GUAM states' compliance with anti-money-laundering standards is ensured by the Council of Europe Committee of Experts on the Evaluation of Anti-Money-laundering Measures and the Financing of Terrorism (MONEYVAL).

2.1 Substantive law

Money-laundering definitions in the GUAM states are provided by the specialized legislative acts adopted with an aim of preventing legalization of illegal proceeds. Definitions contained in the Law of the Republic of Azerbaijan on the Prevention of the Legalization of Criminally Obtained Funds or Other Property and the Financing of Terrorism, the Law of Georgia on Facilitating the Prevention of Illicit Income Legalization, the Law of Moldova on the Prevention and Combating Money-laundering and Financing of Terrorism, and the Law of Ukraine on Prevention and Counteraction to Legalization (Laundering) of the Proceeds of Crime or Terrorist Financing conform to the internationally accepted definitions of money-laundering that can be used in cases involving illegal use of virtual currencies.

From a substantive criminal law perspective, all of the GUAM states criminalize legalization of proceeds and instrumentalities of crime in their legislation. Articles 193[1] and 194 of the Criminal Code of Azerbaijan, ''Legalization of funds or other property, knowing that such funds or other property is the proceeds of crime'' and "Acquisition, possession, use or disposition of funds or other property, knowing, at the time of receipt, that such funds or other property is the proceeds of crime", Articles 194 and 194[1] of the Criminal Code of Georgia, "Legalization of illegal proceeds" and "Use, procurement, possession or disposition of property obtained from the legalization of illegal income", Article 243 of the Criminal Code of Moldova, "Money-laundering", and Article 209 of the Criminal Code of Ukraine, "Legalization (laundering) of criminally obtained money and other property", provide substantive law framework for addressing such offences in terms of necessary elements of crime, as well as possible sanctions.

The situation differs in relation to predicate offences. With the exception of Ukraine, the GUAM states use an all-crimes approach in relation to predicate offences, meaning that proceeds and instrumentalities of any crime can be subject to freezing, seizure and confiscation. In case of Ukraine, Article 209 of the Criminal Code of Ukraine envisages a minimum threshold of sentence (crimes punishable by deprivation of liberty or fine in excess of 3000 minimum wages) as well as exceptions for tax evasion offences (Articles 212 and 212[1] of the Criminal Code). Putting this into the terms of cybercrime often being the predicate offence in virtual currency-related investigations, this is not a major concern, since all of the acts under Chapter 16 "Criminal Offenses Related to the Use of Electronic Computing Machines (Computers), Systems and Computer Networks and Telecommunication Networks" of the Criminal Code of Ukraine envisage deprivation of liberty as a possible option for sentencing.

2.2 Procedural regulations

Besides the general criminal procedure framework available for investigation of all criminal offences, and the related procedural actions (such as witness testimony, search and seizure, production of documents, etc.), financial investigations into money-laundering, as well as detection and seizure of illegal proceeds and instrumentalities of crime, are based on application of specific procedural powers that can be also relevant in the context of virtual currency-related investigations.

In terms of criminal intelligence in money-laundering cases involving virtual currencies, the importance of using suspicious transaction reports from national FIUs has been noted in this Manual. Definitions of suspicions transactions are provided, correspondingly, by Article 7 of the Law of the Republic of Azerbaijan on the Prevention of the Legalization of Criminally Obtained Funds or Other Property and the Financing of Terrorism, Article 2(h) of the Law of Georgia on Facilitating the Prevention of Illicit Income Legalization, Article 5 of the Law of Moldova on the Prevention and Combating Money-laundering and Financing of Terrorism, and Article 11 of the Law of Ukraine on Prevention and Counteraction to Legalization (Laundering) of the Proceeds of Crime or Terrorist Financing.

Monitoring of transactions, as an investigative tool in financial investigations of money-laundering, is provided by Articles 2-9 of the Law of the Republic of Azerbaijan on the Prevention of the Legalization of Criminally Obtained Funds or Other Property and the Financing of Terrorism, Articles 5-10 of the Law of Georgia on Facilitating the Prevention of Illicit Income Legalization, Article 4-6 of the Law of Moldova on the Prevention and Combating Money-laundering and Financing of Terrorism, and Section II of the Law of Ukraine on Prevention and Counteraction to Legalization (Laundering) of the Proceeds of Crime or Terrorist Financing. This is the procedural power specific to the FIUs.

Monitoring orders may be also issued by law enforcement. Article 124^1 of the Criminal Procedure Code of Georgia and Article 132^4 of the Criminal Procedure Code of Moldova provide investigative agencies with the power to monitor financial transactions in the course of investigation; in the criminal procedure legislation of Azerbaijan and Ukraine, there are no comparable provisions for law enforcement.

Production and disclosure of financial records falls within the general power of law enforcement to request and obtain evidence in the form of document or information from any state agency, private entity or an individual. In the context of virtual currencies, either specialized production orders for electronic evidence (Article 136 of the Criminal Procedure Code of Georgia and Chapter 15 of the Criminal Procedure Code of Ukraine) or general production orders (Chapter XXXI of the Criminal Procedure Code of Azerbaijan and Article 126 of the Criminal Procedure Code of Moldova) can be used to secure financial records in the course of virtual currency-related investigations.

In the context of the GUAM states, procedures for seizure of criminal profits or crime instrumentalities are predominantly addressed by the criminal procedure framework.

Article 249 of the Criminal Procedure Code of Azerbaijan provides for the grounds that can be used for seizing illegally obtained property; although such seizure is a predominantly judicial procedure, in case of exigent circumstances, such as imminent destruction or other loss of control over such property, investigator's substantiated motion may provide legal grounds for effecting seizure.

Article 151 of the Criminal Procedure Code of Georgia provides for strictly judicial procedure for the arrest of illegally obtained property. This provision introduces the specific possibility for the use of civil law procedures for the purposes of arrest, provided those procedures are generally compliant with the Criminal Procedure Code.

Articles 203-209 of the Criminal Procedure Code of Moldova provide for the grounds and procedures for the seizure of illegally obtained property. Both judicial warrant and ex officio procedures can be used in this respect. There are also detailed provisions related to the enforcement of warrants and management of seized property.

Chapter 17 of the Criminal Procedure Code of Ukraine addresses seizure of illegal proceeds in the framework of general regulations pertaining to seizure of property in the criminal proceedings.

Where expert examinations and reports of such examinations are necessary for proper performance of procedural actions noted above, Chapter XXXV of the Criminal Procedure Code of Azerbaijan, Articles 144-146 of the Criminal Procedure Code of Georgia, Articles 142-153 of the Criminal Procedure Code of Moldova and Articles 242-245 of the Criminal Procedure Code of Ukraine may be used as a legal groundwork for securing expert support in virtual currency-related investigations.

2.3 Institutional framework

In terms of money-laundering investigations and especially financial intelligence, specialized agencies for money-laundering investigation, such as Financial Intelligence Units, are naturally key players from an institutional standpoint. In this regard, Financial Monitoring Service under the Central Bank of the Republic of Azerbaijan, Financial Monitoring Service of Georgia, Office for Prevention and Fight against Money-laundering of the National Anticorruption Centre of the Republic of Moldova and the State Financial Monitoring Service of Ukraine provide expertise in prevention and investigation of money-laundering offences.

In terms of actual seizure of crime proceeds and instrumentalities, relevant functions in the GUAM states are assigned to law enforcement tasked with investigation of legalization of illegal proceeds, such as Department for Combating Corruption at the General Prosecutor's Office of Azerbaijan, Anti-Corruption Department of the Chief Prosecutor's Office of Georgia, Service on Prevention and Combating Money-laundering at the National Anti-Corruption Centre of Moldova, and the Financial Investigations Department at the Ministry of Revenue and Duties of Ukraine, with investigative actions also performed by the Ministry of Internal Affairs and/or State Security Service of Ukraine.

With regard to international cooperation in money-laundering, all of the noted GUAM state FIUs are part of the Egmont Group of Financial Intelligence Units and can therefore avail themselves of the data exchange and investigative assistance opportunities offered by this network. On the other hand, law enforcement units investigating legalization of illegal proceeds can use both 24/7 contact points for the purposes of police-to-police cooperation in cybercrime cases, or local Interpol contacts for similar and other assistance modalities in police-to-police cooperation. Where juridical cooperation is required, central authorities for mutual legal assistance in criminal cases can be involved to handle processing of such requests (international departments of the Ministries of Justice or Chief/General Prosecutor's Office in all GUAM states, depending on the stage of the criminal proceedings).

3 Cybercrime regulatory framework

All of the GUAM states are parties to the 2001 Council of Europe Convention against Cybercrime, which is a regional treaty addressing criminalization of cybercrime offences, procedural actions aimed at their investigation, and institutional capacities and international cooperation modalities required to fight cybercrime across national borders. Compliance of the GUAM states with the requirements of the Convention is performed by the Cybercrime Convention Committee (T-CY) through regular and thematic reporting.

3.1 Substantive law

Cybercrime offences that can be predicate or auxiliary to money-laundering committed through the use of virtual currencies are mostly incorporated into the legislation of the GUAM states; however, there are some differences in addressing different offences by the GUAM jurisdictions.

The offence of illegal access, as a basic offence of threats to and attacks against the security (i.e. the confidentiality, integrity and availability) of computer systems and data, is fully criminalized by Azerbaijan, Georgia and Moldova. Illegal access is addressed, correspondingly, by the Article 271 of the Criminal Code of Azerbaijan, Article 284 of the Criminal Code of Georgia and Article 259 of the Criminal Code of Moldova. However, no direct analogy is found in the substantive criminal law of Ukraine.

Data interference, an offence against integrity and the proper functioning or use of stored computer data or computer programs, such as damaging, deletion, deterioration, alteration or suppression of computer data, is incorporated in the provisions of Article 286 of the Criminal Code of Georgia, Article 260^2 of the Criminal Code of Moldova and Articles 361 and 362 of the Criminal Code of Ukraine. No separate offence of data interference is available in the criminal legislation of Azerbaijan.

Similarly, an offence of system interference, meaning intentional hindering of the lawful use of computer systems including telecommunications facilities by using or influencing computer data, is criminalized under Article 286, p. 2 of the Criminal Code of Georgia, Article 260^3 of the Criminal Code of Moldova and Articles 361 and 363^1 of the Criminal Code of Ukraine. Criminal law of Azerbaijan, at the moment, does not provide for a separate definition of system interference.

Misuse of devices, that is, illegal act of misuse of devices and data for the purpose of committing offences against the confidentiality, the integrity and availability of computer systems or data, is properly criminalized by all GUAM states. Corresponding provisions can be found in Article 271^6 of the Criminal

Code of Azerbaijan, Article 285 of the Criminal Code of Georgia, Article 260^4 of the Criminal Code of Moldova and Article 361^1 of the Criminal Code of Ukraine.

3.2 Procedural actions

Electronic evidence is a key concept for investigation of crimes involving computer systems and data, and is thus important for investigation of money-laundering offences. In the GUAM states, the criminal procedure acts do not incorporate electronic evidence as a separate, standalone category of evidence, but rather interpret electronic evidence to be a part of the concept of "documents" or "information" that can be used as admissible evidence in criminal proceedings.

Regarding specific procedural actions aimed at investigation of cybercrime offences, real-time collection of traffic data is provided by Article 137 of the Criminal Procedure Code of Georgia and Article 263 of the Criminal Procedure Code of Ukraine. This procedure is notably missing from the criminal procedure framework of Azerbaijan and Moldova.

Interception of content data aims to assimilate traditional options for the collection of content data in respect of telecommunications (e.g., telephone conversations) into the environment of information technology. In the context of the GUAM states, interception procedures are provided either by laws on Operative-Detective Activity (Section 10 of the Law of Azerbaijan on Operative-Detective Activity and Article 18 of the Moldovan Law on Special Detective Activities) or incorporated into the mainstream criminal procedure legislation (Article 138 of the Criminal Procedure Code of Georgia and Articles 258 and 264 of the Criminal Procedure Code of Ukraine).

In contrast, preservation of stored computer data, as well as partial disclosure of data so preserved, is only available under Article 7 of the Moldovan Law on Combating Cybercrime and is not an approach shared by other GUAM states. However, in practice, preservation procedures can be substituted by search and seizure of electronic evidence in exigent circumstances, something that is widely available across most GUAM jurisdictions (Article 243 p. 3 of the Criminal Procedure Code of Azerbaijan, Article 120 of the Criminal Procedure Code of Georgia, and Article 125 p. 4 of the Criminal Procedure Code of Moldova), with the exception of Ukraine that allows only judicial warrants for search and seizure (Article 234 of the Criminal Procedure Code of Ukraine).

Production orders, used in a cybercrime context to compel a person to provide specified stored computer data, or to require service provider offering its services in the territory of the Party to submit subscriber information, are available under Article 136 of the Criminal Procedure Code of Georgia and Chapter 15 of the Criminal Procedure Code of Ukraine. In cases of Azerbaijan and Moldova, general criminal procedure provisions on production of

documents and other evidence can be used to an equal effect (Chapter XXXI of the Criminal Procedure Code of Azerbaijan and Article 126 of the Criminal Procedure Code of Moldova).

3.3 Institutional framework

Cybercrime investigations, per the requirements under the Council of Europe Convention against Cybercrime, rely on centralized, specialized investigative units to perform detection and investigation cybercrime, as well as preliminary investigative analysis of electronic evidence in cybercrime cases. All of the GUAM states operate such units at their police forces.

In Azerbaijan, cybercrime investigations are handled by Department of Combating Crimes in Communications and IT of the Ministry of National Security of the Republic of Azerbaijan. Georgian cybercrime investigations are performed by the Division for Combating Cybercrime of the Central Criminal Police Department at the Ministry of Internal Affairs of Georgia. Cybercrime detection and investigation in Moldova is undertaken by the Direction of Prevention and Combating of Cybernetic, Information and Transnational Offences of the Ministry of Internal Affairs of Moldova. Ukraine investigates cybercrime offences under the investigative competence of the Department for Combating Cybercrime of the Ministry of Internal Affairs of Ukraine.

With regard to international cooperation in cybercrime matters, all of the investigative units noted above incorporate 24/7 contact point for the purposes of police-to-police cooperation in cybercrime cases, in compliance with the requirements of the Convention on Cybercrime. Where juridical cooperation is required, central authorities for mutual legal assistance in criminal cases are set up to handle the processing of such requests (international departments of the Ministries of Justice or Chief/General Prosecutor's Office in all GUAM states, depending on the stage of the criminal proceedings).

4 Conclusions

In the absence of directly applicable regulations on the illegal use of virtual currencies, in particular, for money-laundering purposes, the GUAM states have to rely on existing provisions of their legislation on money-laundering and cybercrime, and to adapt them to the context of virtual currencies. In all fairness, no other nations have introduced similarly direct regulations on virtual currencies, and the advanced state of money-laundering and cybercrime regulations in the GUAM states should, at least theoretically, allow them to apply existing provisions to new and emerging challenges presented by virtual currencies.

However, several considerations with regard to implementation of cybercrime provisions in criminal law framework of the GUAM states – from both substantive and procedural points of view – need to be addressed. Although cybercrime offences may be standalone acts that have no relation to money-laundering activities, relevance of cybercrime investigations as offences that can be predicate or auxiliary to money-laundering has been highlighted throughout this Manual. Even if this approach remains largely unexplored in practice in the GUAM states, having a coherent legal framework prepared for challenges presented by technology cannot be understated.

Correct interpretation of legal terms is important; however, even more important is an understanding in all state agencies and departments involved, in one way or another, of the cross-cutting issues of money-laundering and cybercrime in the context of virtual currencies. As with any form of technically and legally complex situations, the key to understanding and addressing challenges presented by virtual currencies is cooperation between national stakeholders. And, since virtual currencies operate in a borderless online environment, international cooperation is going to play an increasingly important role in investigating money-laundering by use of virtual currencies. Having already established national authorities for investigation of money-laundering and cybercrime, as well as making available national contact points for international investigative cooperation as well as mutual legal assistance, the GUAM states are institutionally well-equipped for offering and implementing such cooperation.

Basic Manual on the Detection And Investigation of the Laundering of Crime Proceeds Using Virtual Currencies

Annex 4
List of Designated Agencies in the GUAM Countries

This annex assembles the list of relevant designated agencies in the GUAM countries with regard to the detection and investigation of laundering crime proceeds through virtual currencies. The list of contacts is organized alphabetically by the GUAM member states.

1 Azerbaijan

Financial Intelligence Unit

Financial Monitoring Service
The Central Bank of the Republic of Azerbaijan
40 Bul-Bul Avenue, AZ1014,
Baku, Republic of Azerbaijan
Tel.: +994 12 598 19 46;
Fax: +994 12 493 03 88; +994 12 493 03 67;
E-mail: office@fiu.az

Money-laundering Investigations

Department for Combating Corruption
General Prosecutor's Office of Azerbaijan
30A Kaverochkin Street, AZ1007
Baku, Republic of Azerbaijan
Tel: +994 12 441 92 52
Fax: n/a
E-mail: kaliyev@prosecutor.gov.az

Units for seizure of crime proceeds/instrumentalities

Department for Combating Corruption
General Prosecutor's Office of Azerbaijan
30A Kaverochkin Street, AZ1007
Baku, Republic of Azerbaijan
Tel: +994 12 441 92 52
Fax: n/a
E-mail: kaliyev@prosecutor.gov.az

Prosecution service

Office of Prosecutor General of the Republic of Azerbaijan
7 Nigar Rafibeyli Str., AZ1001
Baku, Republic of Azerbaijan
Tel: +994 12 492 55 40
Fax: n/a

E-mail: info@prosecutor.gov.az

National contact for Mutual Legal Assistance

Pre-trial:
International Legal Department
Prosecutor General's Office of the Republic of Azerbaijan
7, Nigar Rafibeyli St., AZ370001
Baku, Republic of Azerbaijan
Tel: +994 12 492 61 98; +994 12 492 17 70; +994 12 492 87 51
Fax: +994 12 493 00 20
E-mail: intlaw@azeri.com

Trial stage:
International Cooperation Department
Ministry of Justice of the Republic of Azerbaijan
1 İnshaatchılar ave., AZ1073
Baku, Republic of Azerbaijan
Tel: +994 12 430 01 67
Fax: +994 12 510 29 40
E-mail: international@justice.gov.az

Cybercrime/High-tech crime unit

Department of Combating Crimes in Communications and IT
Ministry of National Security of the Republic of Azerbaijan
2 Parliament Ave, AZ1006
Baku, Republic of Azerbaijan
Tel: +994 12 493 76 22
Fax: +994 12 493 76 22
E-mail: secretoffice@mns.gov.az

24/7 contact point under the Convention on Cybercrime

Department of Combating Crimes in Communications and IT
Ministry of National Security of the Republic of Azerbaijan
2 Parliament Ave, AZ1006
Baku, Republic of Azerbaijan
Tel: +994 12 493 76 22
Fax: +994 12 493 76 22
E-mail: secretoffice@mns.gov.az

Interpol contact point

Bureau of Interpol in Azerbaijan
4 Firdovsi Mammadov, Narimanov, AZ1008
Baku, Republic of Azerbaijan
Phone: +994 12 498 09 23, +994 12 590 99 26
Fax: +994 12 598 37 77
E-mail: n/a

Computer Security Incident Response Team (CSIRT)

CERT-AZ
Drogal Lane, Block 702, AZ1010
Baku, Republic of Azerbaijan
Phone: +994 12 493 20 57
E-mail: reports@cert.az

Personal data protection office

Commissioner for Human Rights (Ombudsman)
40, U. Hajibayov Street, Government House, II Door, AZ 1000
Baku, Republic of Azerbaijan
Tel: +994 12 498 23 65
Faxm: ombudsman@ombudsman.gov.az

2 Georgia

Financial Intelligence Unit

Financial Monitoring Service of Georgia
2 Sanapiro Street, 0105 Tbilisi, Georgia
Tel: +995 32 229 67 00
Fax: +995 32 229 67 00
E-mail: info@fms.gov.ge

Money-laundering Investigations

Anti-Corruption Department
Chief Prosecutor's Office of Georgia
24 Gorgasali Street, Tbilisi 0114 Tbilisi, Georgia
Tel: +995 32 240 51 36
Fax: n/a
E-mail: btkhelidze@justice.gov.ge

Units for seizure of crime proceeds/instrumentalities

Anti-Corruption Department
Chief Prosecutor's Office of Georgia
24 Gorgasali Street, 0114 Tbilisi, Georgia
Tel: +995 32 240 51 36
Fax: n/a
E-mail: btkhelidze@justice.gov.ge

Prosecution service

Chief Prosecutor's Office of Georgia
24 Gorgasali Street, Tbilisi 0114 Tbilisi, Georgia
Phone: +995 32 240 53 44
Fax: n/a
E-mail: presscenter@pog.gov.ge

National contact for Mutual Legal Assistance

Both pre-trial and trial stages:
International Legal Department
Chief Prosecutor's Office, by delegated authority of the Ministry of Justice of Georgia
24 Gorgasali Street, 0114 Tbilisi, Georgia
Tel: +995 32 240 51 43
Fax: +995 32 240 51 42

E-mail: ichilingarashvili@justice.gov.ge

Cybercrime/High-tech crime unit

Division for Combating Cybercrime
Central Criminal Police Department
Ministry of Internal Affairs of Georgia
38 Kakheti Highway, 0135 Tbilisi, Georgia
Tel: +995 32 241 87 59
Fax: +995 32 241 87 76
E-mail: international@mia.gov.ge

24/7 contact point under the Convention on Cybercrime

Division for Combating Cybercrime
Central Criminal Police Department
Ministry of Internal Affairs of Georgia
38 Kakheti Highway, 0135 Tbilisi, Georgia
Tel: +995 32 241 87 59
Fax: +995 32 241 87 76
E-mail: datogabekhadze@mia.gov.ge

Interpol contact point

National Central Bureau of Interpol
Ministry of Internal Affairs of Georgia
38 Kakheti Highway, 0135 Tbilisi, Georgia
Tel: +995 32 241 13 98
Fax: +995 32 241 13 98
E-mail: interpol@mia.gov.ge

Computer Security Incident Response Team (CSIRT)

CERT-GOV-GE
Data Exchange Agency
Ministry of Justice of Georgia
2 St. Nicholas Street, 0102 Tbilisi, Georgia
Tel: +995 32 291 51 40
Fax: +995 32 291 51 40
E-mail: cert@dea.gov.ge

Personal data protection office

Office of the Personal Data Protection Inspector
15 Apakidze Str., 0102 Tbilisi, Georgia

Tel: +995 32 242 10 00
Fax: n/a
E-mail: office@pdp.ge

3 Moldova

Financial Intelligence Unit

Office for Prevention and Fight against Money-laundering
National Anticorruption Centre of the Republic of Moldova
198 Ştefan cel Mare Ave., Chişinău 2004
Republic of Moldova
Tel: +373 22 257 317
Fax: +373 22 257 317
E-mail: spcsb@cna.md

Money-laundering Investigations

Office for Prevention and Fight against Money-laundering
National Anticorruption Centre of the Republic of Moldova
198 Ştefan cel Mare Ave., Chişinău 2004
Republic of Moldova
Tel: +373 22 257 317
Fax: +373 22 257 317
E-mail: spcsb@cna.md

Units for seizure of crime proceeds/instrumentalities

Office for Prevention and Fight against Money-laundering
National Anticorruption Centre of the Republic of Moldova
198 Ştefan cel Mare Ave., Chişinău 2004
Republic of Moldova
Tel: +373 22 257 317
Fax: +373 22 257 317
E-mail: spcsb@cna.md

Prosecution service

Office of the Prosecutor General of the Republic of Moldova
26 Banulescu-Bodoni Street, Chişinău 2005
Republic of Moldova
Phone: +373 212 042, +373 212 348
Fax: n/a
E-mail: proc-gen@gov.md

National contact for Mutual Legal Assistance

Pre-trial:
International Legal Department

Prosecutor General's Office of the Republic of Moldova
26, Metropolit Banulescu-Bodoni St., Chisinau 2005
Republic of Moldova
Tel: +373 22 221 470; + 373 22 225 589; + 373 22 221 335
Fax: + 373 22 221 335
E-mail: proc-gen@gov.md

Trial stage:
International Legal Department
Ministry of Justice of the Republic of Moldova
82 31 August 1989 Street, Chisinau 2012
Republic of Moldova
Tel: + 373 22 201 438; +373 22 201 455
Fax: + 373 22 201 410
E-mail: sirku@justice.gov.md

Cybercrime/High-tech crime unit

Direction of Prevention and Combating of Cybernetic, Information and Transnational Offences
Ministry of Internal Affairs of Moldova
14 Bucuriei Street, Chisinau 2004
Republic of Moldova
Tel: +373 22 577 216
Fax: n/a
E-mail: Iurdan-ana@mail.ru

24/7 contact point under the Convention on Cybercrime

Direction of Prevention and Combating of Cybernetic, Information and Transnational Offences
Ministry of Internal Affairs of Moldova
14 Bucuriei Street, Chisinau 2004
Republic of Moldova
Tel: +373 22 577 216
Fax: n/a
E-mail: Iurdan-ana@mail.ru

Interpol contact point

Interpol National Central Bureau
International Police Cooperation Centre
Ministry of Internal Affairs of Moldova
75 Stefan cel Mare Street, Chisinau 2004
Republic of Moldova

Tel: +373 22 255 404
Fax: n/a
E-mail: igp@mai.gov.md

Computer Security Incident Response Team (CSIRT)

Cyber Security Centre CERT-GOV-MD
Centre of Special Telecommunications
State Chancellery of the Republic of Moldova
1 Piaţa Marii Adunări Naţionale, Chisinau 2033
Republic of Moldova
Tel: +373 22 820 900
Fax: +373 22 250 522
E-mail: info@cert.gov.md

Personal data protection office

National Center for Personal Data Protection
48, Serghei Lazo Str., Chisinau 2004
Republic of Moldova
Tel: +373 22 820 801
Fax: +373 22 820 807
E-mail: centru@datepersonale.md

4 Ukraine

Financial Intelligence Unit

The State Financial Monitoring Service of Ukraine
Ministry of Finance of Ukraine
Biloruska 24, Kyiv 04655, Ukraine
Tel: +380 44 594 16 52
Fax: +380 44 594 16 52
E-mail: sdfm@sdfm.gov.ua

Money-laundering Investigations

General Financial Investigations Division
Ministry of Revenue and Duties of Ukraine
8 Lviv Square, Kiyv 04655, Ukraine
Tel: +38 044 247 34 99
Fax: +38 044 247 36 03
E-mail: Kabmin_doc@minrd.gov.ua

Division for Combating legalisation of the proceeds of organised groups and criminal organisations
Ministry of Internal Affairs of Ukraine
Bohomoltsa 10, Kiyv 01601, Ukraine
Tel: +380 44 256 03 33
Fax: +380 44 256 16 33
E-mail: n/a

Units for seizure of crime proceeds/instrumentalities

General Financial Investigations Division
Ministry of Revenue and Duties of Ukraine
8 Lviv Square, Kiyv 04655, Ukraine
Tel: +380 44 247 34 99
Fax: +380 44 247 36 03
E-mail: Kabmin_doc@minrd.gov.ua

Prosecution service

Office of the Prosecutor General of the Ukraine
Riznytska 13/15, Kiyv 01011, Ukraine
Phone: +380 44 200 78 49
Fax: n/a
E-mail: jnt@gp.gov.ua

National contact for Mutual Legal Assistance

Pre-trial:
International Legal Department
Prosecutor General's Office of Ukraine
Reznitska 13/15, Kyiv 01011, Ukraine
Tel: +380 44 200 78 84
Fax: +380 44 280 28 51
E-mail: indep@gp.gov.ua

Trial stage:
International Department
Ministry of Justice of Ukraine
Horodetskogo 13, Kyiv 01001, Ukraine
Tel: +380 44 279 68 79
Fax: +380 44 270 54 53
E-mail: itex@minjust.gov.ua

Cybercrime/High-tech crime unit

Department for Combating Cybercrime
Ministry of Internal Affairs of Ukraine
Bohomoltsa 10, Kiyv 01601, Ukraine
Tel: +380 44 374 37 13
Fax: +380 44 374 37 00
E-mail: request@cybercrime.gov.ua

24/7 contact point under the Convention on Cybercrime

Department for Combating Cybercrime
Ministry of Internal Affairs of Ukraine
Bohomoltsa 10, Kiyv 01601, Ukraine
Tel: +380 44 374 37 13
Fax: +380 44 374 37 00
E-mail: request@cybercrime.gov.ua

Interpol contact point

Ukrainian Bureau of Interpol
Ministry of Internal Affairs of Ukraine
Bohomoltsa 10, Kiyv 01601, Ukraine
Tel: +380 44 256 12 53
Fax: +380 44 226 20 57
E-mail: interpol@mvs.gov.ua

Computer Security Incident Response Team (CSIRT)

CERT-UA
State Service of Special Communication and Information Protection of Ukraine
Melnikova 83b, block 2, Kiyv 04119, Ukraine
Tel: +380 44 281 88 25
Fax: +380 44 489 31 33
E-mail: cert@cert.gov.ua

Personal data protection office

State Service of Ukraine on Personal Data Protection
Maryny Raskovoi 15, Kyiv 02660, Ukraine
Tel: +38 044 517 68 00
Fax: +38 044 517 68 00
E-mail: info@zpd.gov.ua

Basic Manual on the Detection And Investigation of the Laundering of Crime Proceeds Using Virtual Currencies

Annex 5
Sample Answers to Self-Assessment Questions

This annex contains sample answers to the self-assessment questions contained within the modules of the training course. The sample answers below contain bullet lists of the key points that should be covered in an answer to that question.

1 Module 1: Introduction to Virtual Currencies

Question 1: Using the definitions adopted by the FATF, define the terms "virtual currency", "electronic money" and "digital currency", explaining clearly the difference between each term.

- Definitions below are based on those adopted by the FATF. Other definitions are possible.
- Definition of the term "virtual currency"
  "A virtual currency is a digital representation of value that can be traded on the Internet and functions as (1) a medium of exchange; (2) a unit of account; and/or (3) a store of value, but does not have legal tender status in any jurisdiction."
- Clarification of the term "digital representation" in the context of the above definition.
- Definition of the term "electronic money"
  "Virtual currency is also distinct from e-money, which is a digital representation of fiat currency used to electronically transfer value denominated in fiat currency. E-money is a digital transfer mechanism for fiat currency – i.e., it electronically transfers value that has legal tender status."
- Definition of the term "digital currency"
  "Digital currency is a digital representation of either virtual currency (non-fiat) or e-money (fiat)."

Question 2: Describe the characteristics that differentiate a convertible virtual currency from a non-convertible virtual currency. Provide an example from each category.

- Definition of convertible/open virtual currency versus non-convertible/closed virtual currency
- Provide examples of convertible and non-convertible virtual currencies
  - Convertible: Bitcoin, WebMoney, Second Life Linden Dollars
  - Non-convertible: World of Warcraft Gold
- Note that secondary trade in non-convertible virtual currencies is also possible.
- Mention the fact that convertible/non-convertible is not a primary categorisation of virtual currencies for investigative purposes due to the

fact that secondary trade in virtual currencies makes many *du jure* non-convertible virtual currencies into *de facto* convertible virtual currencies.

Question 3: Describe the characteristics that differentiate a centralised virtual currency from a decentralised virtual currency. Provide an example from each category.

- Definition of centralised versus decentralised virtual currency.
- Briefly describe features of centralised and decentralised virtual currencies
    - Centralised: Central administrating authority controls the currency
    - Decentralised: distributed, open-source, math-based, peer-to-peer digital currencies with no central monitoring or oversight.
- Provide examples of centralised and decentralised virtual currencies
    - Centralised: Second Life Linden Dollars, PerfectMoney, WebMoney and World of Warcraft gold
    - Decentralised: Bitcoin, LiteCoin, Ripple

Question 4: When considering virtual currencies it is important to be aware of the interface between virtual currencies and the traditional financial system. In this context, discuss the role virtual currency exchanges play. Focus in particular on the range of possible funding sources from which virtual currencies can be acquired.

- Trading of fiat currency for virtual currency typically takes place on a virtual currency exchange.
- Many funding sources are possible including other virtual currencies, bank transfer, money remittance provider, payment card, cash and Internet payment services such as PayPal.
- Other novel models such as paying for virtual currency with SMS (text messages) also exist.
- The lack of regulation of the trade of virtual currencies introduces risks that virtual currencies do not properly identify the sources of funding used to acquire the virtual currencies.

Question 5: Aside from virtual currency exchanges, give three examples of interfaces between the traditional financial system and virtual currencies that are relevant to the issue of laundering crime proceeds through the use of virtual currencies.

- Cash
    - Cash has always been attractive in the laundering of crime proceeds.

  - In recent times, the growing popularity of virtual currencies, particularly Bitcoin, mean that new business models have emerged.
  - For example, Bitcoin ATMs are available in a number of countries.
  - Virtual currency exchanges that facilitate trading bitcoins for cash also exist.
- Payment Cards
  - Prepaid cards can act as an alternative to a variety of traditional banking products, including making and receiving payments from third parties, cross-border remittances, and so on.
  - Payment cards can act as a funding source for virtual currencies.
  - Prepaid cards can also be designed to provide absolute anonymity.
- Money Remittance Providers
  - Previous studies have indicated that the use of money remittance providers is a common technique for laundering crime proceeds, particularly criminal money derived from cybercrime.
  - Money remittance providers could be used in laundering via virtual currencies through the use of mule accounts.
  - There are also virtual currency exchanges that will directly accept money remittances to fund virtual currency purchases.

Question 6: Explain the reasons why some virtual currencies might be an attractive payment method for legitimate merchants.

- Once confirmed, Bitcoin transactions are irreversible and therefore there is no possibility of chargebacks or other fraud losses that are possible with payment cards.
- The fees associated with processing bitcoins are lower than payment card acquiring fees.
- There is a growing ecosystem of merchant support services to assist businesses to configure and accept Bitcoin payments.

Question 7: Explain what is meant by the term cryptocurrency.

- A cryptocurrency is a virtual currency that relies on the principles of cryptography to ensure reliability and integrity.
- For example, bitcoins are a convertible, decentralised virtual currency, and also a cryptocurrency.
- Cryptocurrencies typically involve management and sharing of a public ledger of transactions, the integrity and chronological order of the transactions in the ledger are enforced by cryptography.

Question 8: Describe the operation of the Bitcoin network paying particular attention to the purpose of "mining".

- The Bitcoin network is fundamentally involved with the management and sharing of a public ledger known as the "block chain", which contains every transaction ever performed and is used to verify the validity of every transaction.
- Bitcoin addresses serve as a unique identifying value that is used to represent ownership of a particular Bitcoin.
- For Person A to send money to Person B, they broadcast a message to the Bitcoin network containing the sender address, the recipient address (their "receiving address") and the amount to transfer. Every node in the Bitcoin network that receives this message will update their copy of the ledger and then pass along the transaction message to other nodes.
- Transactions are assembled into groups, known as blocks, and the blocks are linked together to form the block chain.
- Transactions within a block are considered to have happened at the same time.
- The blocks are ordered by virtue of the fact that each block refers to the previous block in the chain.
- The process of building blocks and appending them to the block chain as described above is known as mining.
- Whoever solves the block and appends it to the block chain receives a reward of a set number of bitcoins, currently 25.
- Every four years the block reward is cut in half until eventually no more bitcoins will be released.
- A total of 21 million bitcoins will be created.
- Bitcoins can be subdivided into smaller units called Satoshi.
- In addition to the Bitcoin reward, miners also receive a transaction fee that can optionally be included with transactions.
- Most mining is performed not by individuals but rather by organised groups of miners, known as mining pools. The reward for computing blocks is divided amongst the members of the pool in proportion to the amount of computational effort each member provided to the pool.

Question 9: Explain how the Bitcoin network prevents "double spending" of Bitcoins.

- The Bitcoin network is fundamentally involved with the management and sharing of a public ledger known as the "block chain", which contains every transaction ever performed and is used to verify the validity of every transaction.
- Bitcoin addresses serve as a unique identifying value that is used to represent ownership of a particular Bitcoin.
- Double spending is a big issue in a peer-to-peer networks, like the Bitcoin network, because there is no guarantee that the order in which

transactions are received by any particular node in the network represents the order in which they were created.

- The problem can be defined as follows; what prevents Person A creating a transaction message sending bitcoins to Person B and simultaneously creating a second transaction message to send bitcoins to someone else, hence double spending the same bitcoins?
- The key technological advance of bitcoins is the technique by which this issue is resolved.
- Transactions are assembled into groups, known as blocks, and the blocks are linked together to form the block chain.
- Transactions within a block are considered to have happened at the same time.
- The blocks are ordered by virtue of the fact that each block refers to the previous block in the chain.
- Transactions that are not already in a block are called unconfirmed transactions.
- Any node in the network can collect a set of unconfirmed transactions, assemble them into a block and propose them as the next block in the chain.
- The proposed block must contain the solution to a complex mathematical problem that is computationally difficult to calculate. The Bitcoin network dynamically adjusts the difficulty of the mathematical problem so that a new block is added to the chain on average once every ten minutes.
- Although it is unlikely, it may occasionally happen that multiple nodes in the Bitcoin network may propose blocks at around the same time.
- In this case the block chain temporarily branches as different nodes in the network append different blocks to the block chain.
- This situation is resolved when the next block is added to the chain.
- The new block will, as mentioned previously, contain a reference to the previous block in the chain.
- It will be therefore be appended to one of the two possible branches in the block chain. At this point, one of the two branches is longer.
- The rule of the Bitcoin network is that nodes must switch to the longest available branch. The result is that very quickly the block chain will stabilise and all nodes will agree on all blocks that are a few back from the end of the chain.

Question 10: Explain how a user of the Bitcoin network proves ownership of a certain amount of Bitcoins to another user.

- The Bitcoin network is fundamentally involved with the management and sharing of a public ledger known as the “block chain”, which contains every transaction ever performed and is used to verify the validity of every transaction.

- Bitcoin addresses serve as a unique identifying value that is used to represent ownership of a particular Bitcoin.
- In order to construct a valid transaction message to transfer bitcoins, the sender of the bitcoins must prove that they are the current owner.
- Consider a situation where Person A is sending, for example, ten bitcoins to Person B. Person A must include in the transaction message references to previous transactions where they received more than the required ten bitcoins. These are referred to as the "inputs" to the transaction.
- Recall that each user of the Bitcoin network maintains a copy of the ledger ("block chain") that contains the history of all previous transactions.
  Person B can use the block chain to verify that the bitcoins referenced in Person A's transaction message indeed belong to Person A.

Question 11: Describe the correlation between principles of technological neutrality and the use of virtual currencies for illegal purposes.

- The principle of technological neutrality is one of the cornerstones of e-commerce regulations worldwide. Technological neutrality means that the technology in question can be used to further both legitimate and illegal ends, and that the technology in itself is "innocent". Illegal use of the technology is a result of human control and actions, and therefore responsibility lies on individual users, not the technology itself.
- Virtual currencies, both centralized and decentralized, represent technology that can be used for legitimate and illegitimate purposes alike.
- Legitimate uses of virtual currencies bring forward benefits for the users in terms of convenience, while contributing positively to the growth of e-commerce.
- Illegal uses of virtual currencies, on the other hand, may involve using technology for the commission of crimes of fraud and money-laundering or other offences of a similar nature, as well as for movement and concealment of illegal proceeds.
- Based on the principle of technological neutrality, virtual currencies are "innocent" of illegal uses performed by individual users, thus ruling out the logic for prohibition of such technology on account of the possibility for it to be used in criminal activities.

Question 12: Describe the possible "appeal" of virtual crypto-currencies for money-laundering purposes.

- In essence, one has to take into account the distinguishing features of virtual currencies that may be used to facilitate the commission of crime or concealment of its proceeds.
- The focus of this question is on decentralized crypto-currencies, thus excluding discussion of centralized ones.

- Crypto-currencies operate beyond established financial institutions – virtual currencies operate without the need to use common, established and thus thoroughly regulated and monitored channels of financial transactions, thus providing greater degree of being "off the grid" from money-laundering oversight institutions;
- Crypto-currencies ensure anonymity of transactions – once virtual currency, e.g. Bitcoin, is assigned to a specific wallet, its further transactions in the block-chain (a single online ledger of Bitcoin transactions) can be anonymized and no longer being able to be traced to individual holders of currency wallets;
- Crypto-currencies rely on cryptography – crypto-currencies base their value on the distributed network of calculations performed by miners in the solution of a cryptographic problem. This adds another layer of difficulty for the purposes of tracing and identification of illegal uses of virtual currencies.

Question 13: What is the difference between cybercrime offences against confidentiality, integrity and availability of computer systems/data, and content-related cybercrime offences?

- Cybercrime offences against confidentiality, integrity and availability of computer systems and data denote the actions directed against normal operations of computer system or the data such systems operate, and include the following offences:
    - Illegal access;
    - illegal interception;
    - Data interference;
    - System interference; and
    - Misuse of devices.
- In contrast to offences against confidentiality, integrity and availability of computer systems and data, content-related cybercrime offences can mean any criminal offence that is committed with the use of information technology and/or is greatly facilitated by such technology. One such example is the computer-related fraud, which denotes traditional fraud offence elements in conjunction with the use of computer systems and data.

Question 14: Mention at least two countries that have banned or restricted the use of Bitcoins, and elaborate on the reasons for such decisions.

- At the moment, China and Canada have moved to ban or restrict, correspondingly, the use of Bitcoin in their financial/banking systems. Additional research or interest on the topic may also put Russia and Denmark on the same list.

- Both of the states noted cite more or less common reasons for disallowing the use of bitcoins in their financial/banking systems. These reasons predominantly include the perceived risks of money-laundering, as well as, to some extent, on the volatility and speculative nature of crypto-currencies.
- Proper conclusion from these two examples is that bitcoins are not banned in the strict sense of the word, but rather temporarily denied recognition due to some of the features of virtual currencies that enhance money-laundering and financial stability risks.

2 Module 2: The Challenges Presented by Virtual Currencies

Question 1: Describe threats presented by virtual currencies that make them an attractive technique for laundering crime proceeds.

- Fast, Irreversible Transactions
  - The speed of transactions, in particular, the speed at which funds can be withdrawn or converted increases the complexity of monitoring and also adds difficulty when attempting to freeze funds.
  - The extent to which transactions can be reversed depends on the particular virtual currency being considered. Bitcoin transactions, for example, cannot be reversed.
- Anonymity by Design
  - Primarily a problem with decentralised virtual currencies, although not all decentralised virtual currencies are designed for anonymity.
  - The details of transactions are available but details associating transactions with real-world identities are not.
  - For centralised virtual currencies, it might be possible to recover details of parties to a transaction from either virtual currency exchanges of central administering authorities.
- Inadequate Transaction Records
  - Central administering authorities and virtual currency exchanges may retain transaction and customer records.
  - However there is typically no regulatory obligation on the exchanges and administrating authorities to retain such records, therefore the quality and accuracy of these records will vary.
  - Both intentionally poor record keeping and unintentionally poor record keeping are possible.
- Identifying that Virtual Currencies Have Been Used
  - Virtual currencies are relatively obscure (relative to cash, payment cards, etc.)
  - Therefore, knowing that virtual currencies have even been used can present a challenge.
  - Further, an appropriate legal basis for the detection of laundering funds through virtual currencies must also be available.
- Complex/Obfuscated Transaction Patterns
  - Virtual currency accounts can be effectively dissociated from real-world identities.
  - It is also possible for an individual to create a large volume of accounts.
  - These facts can be used to facilitate novel, complex layering transaction patterns.
- No funding limits

- In centralised virtual currencies, the administrating authorities may introduce funding limits, but these are typically a fraud management measure.
- With decentralised virtual currencies there are typically no funding limits.

Question 2: In the context of virtual currencies, discuss how criminals exploit the non-face-to-face nature of virtual currencies to launder crime proceeds.

- Most involvement with virtual currencies involves minimal, or zero, face-to-face contact. This can give rise to situations where the virtual currencies can be abused by criminals to launder crime proceeds.
- One category of exploitation that can take place involves the scenario where criminals gain control of the accounts of legitimate users and perform transactions.
- Two distinct cases where this is reported to take place:
  "In a number of cases NPM products were used to launder illicit proceeds gained from fraud following identity theft or from stealing money from bank accounts or credit/debit cards using computer hacking or phishing methods. Since the bank accounts or credit and debit cards were held in the names of legitimate customers, the criminals were able to use them as reference accounts for the funding of prepaid cards or IPS accounts. In such instances, the NPM providers could not detect that the transactions were actually not initiated by their legitimate customer, or detect any other suspicious activity."
  "In other cases, stolen or fake identities were used to create NPM accounts which were also used as transit accounts in the laundering of illegal proceeds, or to commit both criminal activities (e.g. fraud) and money laundering at the same time."
- The second category of exploitation of the non-face-to-face nature of NPM accounts revolves around the exploitation of the anonymous nature of some of these services.
  "In some jurisdictions e-money payment services can be used anonymously. It should also be noted that e-money circulates outside banks and, as such, outside the bank supervision system. Banks serve as agents, letting the money in or out of the e-payment systems, and in certain cases – as "issuers"/emitters of e-money."

Question 3: Describe how the regulatory and supervisory challenges relating to the administrating authorities of centralised virtual currencies present risks of laundering.

- The requirement for financial institutions to be regulated for compliance to anti-money-laundering best practice is well understood.

- By the definition used by the FATF, centralised virtual currency providers fall within the definition of financial institutions.
- In the case of decentralised virtual currencies, there is no financial institution providing a money or value transfer service. Nevertheless a value transfer service exists.
- An appropriate legislative basis for regulation of virtual currencies is required.
- As well as this, implementing supervisory oversight, particularly of decentralised virtual currencies, presents some significant practical challenges.

Question 4: List investigative challenges presented by virtual currencies and discuss possible ways in which those investigative challenges can be addressed.

- Lack of Knowledge
    - Limited awareness among investigators and prosecutors of the existence and capabilities of virtual currencies as well as the tools and techniques to effectively perform investigations involving virtual currencies.
- Reliance on Electronic Evidence
    - Most evidence relating to virtual currencies is likely to be electronic.
    - Electronic evidence must be appropriately managed and it must be authentic, admissible and relevant.
    - It can be difficult to trace electronic evidence, requiring specialist tools and expertise to gather and analyse.
    - Electronic evidence can be highly volatile.
    - Electronic evidence is particularly susceptible to alteration and therefore requires specialist techniques of preservation.
    - Electronic evidence may be copied which may present challenges in court in terms of positioning evidence as authentic.
- Legislative Loopholes
    - A major legislative loophole in the case of virtual currencies is the lack of regulation and directly applicable laws.
    - Appropriate legislation to support the admissibility of electronic evidence must also be in place.
- Regulatory/Supervisory Challenges
    - The requirement for financial institutions to be regulated for compliance to anti-money-laundering best practice is well understood.
    - By the definition used by the FATF, centralised virtual currency providers fall within the definition of financial institutions.

  - In the case of decentralised virtual currencies, there is no financial institution providing a money or value transfer service. Nevertheless a value transfer service exists.
  - An appropriate legislative basis for regulation of virtual currencies is required.
  - As well as this, implementing supervisory oversight, particularly of decentralised virtual currencies, presents some significant practical challenges.
- Prosecution and Adjudication of Offences
  - Appropriate gathering and management of electronic evidence.
  - Proper understanding of judges in criminal proceedings.
- National Cooperation Issues
  - Due to the unregulated nature of virtual currencies, offences that involve or are predicate to their illegal use can often lead to unclear or competing investigative jurisdictions of several agencies.
  - National cooperation is important for crime intelligence as well as prosecution offences that use or are committed against information technology.
  - The primary partners are law enforcement and FIUs, cybercrime units and financial investigators.
  - The primary challenge for such cooperation is that often criminal and financial investigators belong to different institutions in countries and use different methods for detection and investigation of offences. Financial investigators often rely on methods of criminal and intelligence and investigation techniques applicable to traditional, tangible forms of evidence. Cybercrime investigators are typically much more experienced dealing with electronic evidence.
  - There are increasing instances of cooperation between cybercrime units and national Computer Security Incident Response Teams (CSIRTs). CSIRTs are key groups that are instrumental in protection of national critical information infrastructures.
  - Public-private cooperation is also important at a national level. The cooperation with Internet Service Providers are a primary source of subscriber information, traffic data and other important electronic evidence in virtual currency investigations. Financial sector institutions are also important sources of evidence.
  - Challenges to public-private cooperation include legal obstacles (confidentiality of user data, lack of legal mechanisms for preservation or retention of data) and practical obstacles (unwillingness to cooperate with state authorities due to lack of agreements/memoranda, costs of specialised equipment for preservation or retention).

- International Cooperation Issues
    - Transnational nature of cybercrime, and virtual currencies in particular, are a distinguishing feature of these types of crimes.
    - International cooperation is often severely dependent on the availability and expediency of international cooperation between investigative agencies and criminal justice institutions of respective jurisdictions.
    - International cooperation is typically far more formalised than national cooperation modalities.
    - The lack of regulation of virtual currencies in various jurisdictions presents a challenge to international cooperation.
    - The length of time and complexity of the procedure of international cooperation, such as Mutual Legal Assistance (MLA) or other similar judicial proceedings also present a challenge, particularly considering the volatile nature of electronic evidence.
    - Similar challenges are relevant in the context of police-to-police cooperation. Several cooperation mechanisms are available (e.g. 24/7 contact points, INTERPOL contact points, G8 Network), such cooperation mechanisms are often under-utilised due to lack of knowledge of law enforcement or supervisory/regulatory authorities.
    - In terms of public-private cooperation, foreign companies may hold data that is relevant to investigations. Examples include social networks, email providers and so on. Particularly challenging in this respect is legally binding cooperation with parent companies of foreign origin. Some of the important data may be directly processed and/or held by a parent company or another entity in a different jurisdiction.

Question 5: List some specific features of electronic evidence that distinguish it from physical (traditional) evidence.

- Difficult traceability, that is, it is difficult to find and trace unless there is specialized knowledge of where to find such data within the specific systems and what other data may be connected to it;
- Necessity for specialist insight, meaning that specialized expert knowledge and experience is required to secure and extract information found in computer system, as well as knowledge of finance, taxation and/or money-laundering techniques and practices relevant in the context of virtual currency investigations;
- High volatility of evidence, so that existing data may be destroyed or rendered inaccessible in the standard course of operation of computer systems;
- Susceptibility to alteration, meaning that computer systems and devices constantly change and update the data through automatic procedures or

manual interference, therefore requiring understating of the temporal limitations and states of electronic evidence at different periods of time;
- Unlimited copying, that is, there are, as such, no copies of digital information - each copy is a precise, flawless copy of the original, making authenticity of electronic evidence difficult to prove.

Question 6: What are the legal grounds for admissibility of electronic evidence in criminal cases in your country?

- The answer would depend on a specific country in context, but at least one of the following would be applicable:
    - Electronic evidence is recognized as a separate category or type of evidence that can be directly admissible in criminal proceedings, without additional requirements compared to traditional evidence;
    - Electronic evidence can be introduced as admissible evidence in the form of the electronic document, provided that every country recognizes the admissibility of documents in the proceedings;
    - Electronic evidence is admissible on the account of being "information" that is also generally admissible in criminal proceedings.

Question 7: Describe the concept of discretionary prosecution and its applicability for investigations involving virtual currency.

- Discretionary prosecution is a concept that allows the prosecutor to dismiss charges in a specific criminal case due to the lack of public interest to press forward with the case. Such considerations may be manifold, including financial issues, age of the defendant, positions of the victim, gravity of the crime, or any other factor that helps to divert the offender from the criminal justice system.
- In many cases, there are alternatives to criminal prosecution that will be binding for the offender following such decisions – e.g. mediation with the victim, compensations of crime costs, obligation to undertake drug abuse treatment, etc.
- In virtual currency offences, there is often an element of cybercrime that may prove problematic for pursuing prosecution since cybercrime offences are usually less grave and there are legitimate grounds for the prosecutor to divert the offender from the criminal justice system.
- In order to address this, the charges of money-laundering – a more serious offence – should be pursued instead of focusing on cybercrime, thus negating the grounds for prosecutorial discretion.

Question 8: Explain the benefits that law enforcement can potentially reap from cooperation with financial intelligence units.

- Access to up-to-date knowledge and experience with money-laundering techniques and practices (general expertise);
- Use of FIU staff as experts in cases involving money-laundering by means of virtual currencies (specialized expertise);
- Access to intelligence information such as suspicious transaction reports (STRs);
- Sharing of knowledge of cybercrime offences in the financial sector and thus enhancing understanding of issues in view of cooperation.

Question 9: Provide a list of international police-to-police cooperation mechanisms that can be used in investigations involving virtual currencies.

- 24/7 points of contact under the Budapest Convention on Cybercrime are primary contacts in cases of cybercrime and offer direct assistance with preservations requests and other investigative actions on the request of similar contacts from other countries.
- G8 Network of high-tech crime units is open to all states beyond G7+ countries themselves and has responsibilities similar to 24/7 points of contact.
- Interpol contact points can be used for police-to-police cooperation for any criminal offences where there are no specialized contact points or the bilateral agreements allow for more efficient cooperation through such channels.

Question 10: What trends are likely to influence the use of virtual currencies as a technique for laundering crime proceeds?

- Increasing Number of Virtual Currencies
    - Since their inception, there have been an increasing number of virtual currencies.
    - The first cryptocurrency (Bitcoin) was established in 2009. In 2014 there are a total of 12 popular cryptocurrencies.
    - There is no reason to believe that other role-playing games/virtual worlds will not develop in-world (non-convertible) virtual currencies.
    - Large merchants (e.g. amazon.com) have begun introducing virtual currencies for in-app payments and purchasing other items on their websites.
- Increasing Availability of Virtual Currencies
    - With increasing availability of virtual currencies, an increasing number of business models, involving an increasing number of funding sources, will become available.

    - There are no inherent geographical limitations on the acquisition of any convertible virtual currency, once the anti-fraud requirements of the administering authority or virtual currency exchange are satisfied.
- Growing Complexity of Laundering Schemes
    - The dissociation of virtual currency accounts from real-world identities, combined with the ability of an individual to create an arbitrary number of accounts means that novel, complex layering transaction patterns are possible.
    - Virtual currencies can therefore act as an enabler for the creation of new laundering methodologies.
- Increasing Regulation of Virtual Currencies
    - Centralised administrators of virtual currencies and virtual currency exchanges may be regulated as financial institutions offering value transfer services.
    - It is expected that the trend towards increased regulation of these types of virtual currency providers will continue.

3 Module 3: Detection and Investigation of Laundering Crime Proceeds Through Virtual Currencies

Question 1: Describe, from the perspective of substantive criminal law, interrelation between money-laundering and cybercrime in cases where virtual currencies are used.

- Predicate offences: cybercrime offices of illegal access, data interception, computer-related fraud or other, similar offences can generate illegal profits from criminal activities, and such proceeds may require concealment and laundering.
- Auxiliary offences: cybercrime offences against computer systems and data facilitate money-laundering by creating favourable conditions for concealment of proceeds or their conversions into legitimate money, especially in cases where security of virtual currency wallets is compromised.
- Standalone offences: cybercrime offences against the proper operation of systems or data involved in the transaction of virtual currencies may be indicative of preparation of money-laundering offences, since hacked or infected systems can be vulnerable to misuse as money-laundering tools.

Question 2: What can be an example of an offence of illegal access in relation to virtual currencies?

- Illegal access to computer systems and data means unauthorized entry into the whole or any part of a computer system (hardware, components, stored data of the system installed, directories, traffic and content-related data), irrespective of the type of connection and method of communication. In the context of virtual currencies, such hacking offences may include the following targets:
    - Database of central administrating entity that manages accounts of game users as well as their transactions;
    - Bitcoin wallets or other forms of storage where currency may be stored;
    - Server infrastructure of the currency exchange with a view to gaining control of the exchange's transaction data.

Question 3: Describe how use of online anonymizers (proxies) can be used as an element of crime in data interference offences, when such offences compromise the personal data of virtual currency users.

- The offence of data interference implies unauthorized acts of manipulation of data, such as damaging, deletion, deterioration, alteration or suppression of computer data.

- The use of anonymizers or proxies, or any other solution that enhances anonymity, can be deemed as unauthorized action that aims to conceal the identity of the potential offender.
- Use of additional online anonymity tools beyond the technology of virtual currencies itself, in order to further enhance anonymity of decentralized virtual currency users, may be brought forward as an element of offence of data interference – in particular, as a proof of intent.

Question 4: Explain how the use of decentralized virtual currencies could be used to prove an element of "layering" in money-laundering charges?

- Layering, in terms of money-laundering, consists of a series of transactions designed to conceal the origin of the funds obtained from criminal activity.
- In the process of layering, the essential features of virtual currency, such as anonymity and difficult traceability of transactions, can be brought forward as an element of money-laundering offence in order to prove the deliberate choice of this alterative exactly for these features.
- In money-laundering prosecutions, focus on layering in terms of virtual currency use can be made a central argument for the proof of intent.

Question 5: Explain possible correlations between computer-related fraud and money-laundering through the use of virtual currencies.

- The offence of computer-related fraud is an assimilative offence that tailors traditional fraud offences to the environment of information and communications technology. In this respect, computer-related fraud has limited relevance in the context of money-laundering offences through the use of virtual currencies:
    - Computer-related fraud may be a predicate offence, where proceeds generated from fraudulent activity on the Internet can be converted into virtual currencies for the proposes of laundering;
    - Computer-related fraud may be an auxiliary offence that facilitates commission of money-laundering offences through manipulation of virtual currency users' data;
    - Users of virtual currency accounts or wallets may be fraudulently led into activities that constitute money-laundering.

Question 6: Which CSIRT data can be used for financial investigators in money-laundering cases involving virtual currencies?

- Computer incident reporting established by CSIRTs either through local sensor network or international databases, with the special focus on the traffic of financial sector institutions;

- Data on malware that is specifically targeted toward identity theft or breaches of privacy of financial information, including instances where traces of traffic generated by such malware include data or software used for management of centralized or decentralized virtual currencies;
- General intelligence information about hacker community and threats in national cyberspace, advanced intelligence about cybercrime rings, forums and other crime-related information exchange platforms.

Question 7: What is the legal basis and requirements for the interception of content data in cases involving virtual currencies?

- Interception of content data aims to assimilate traditional options for the collection of content data in respect of telecommunications (e.g., telephone conversations) into the environment of information technology. Therefore, in essence, the same requirements applicable to traditional interception/wiretapping powers should be listed in this regard:
    - Ongoing investigation into serious crime that may involve the use of virtual currencies;
    - Judicial order for the interception of data;
    - Prosecutorial oversight over the process.

Question 8: Explain procedural differences (in terms of law and practice) between expedited preservation of stored computer data versus search and seizure of computer data.

- Preservation of stored computer data allows for expeditious preservation of specified computer data, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification. Its defining features are:
    - It is a measure that is less intrusive into the private life of individuals;
    - Preserved data are retained under ownership and control of the owner, with the requirement that such data may not be adversely modified;
    - Confidentiality required for the holders of data with regard to existence and execution of the preservation order;
    - No specific requirements for specialized knowledge in order to request and effect preservation.
- Search and seizure procedures for computer data (i.e., electronic evidence) are, in essence, assimilative provisions that aim to harmonize already existing criminal procedural law powers for search and seizure of tangible objects, in terms of their application to computer systems and data. There are, however, some distinctive features in contrast to preservation of stored computer data:

- Greater invasion of privacy of an individual/business entity whose premises are being searched;
- Search and seizure are not performed confidentially and usually require attendance of person/representative of the entity searched;
- Data, objects and generally evidence are removed from the control of the owner into the custody of the state;
- Search and seizure of electronic evidence requires specialist knowledge in order to ensure integrity of seized evidence.

Question 9: Name at least three elements of the chain of custody of electronic evidence.

- Data integrity, so that computer data should be always kept from possible modifications by the use of techniques and methods (such as access only in "read mode", examination of a digital copy and not "original" evidence, imaging or recording of handling, etc.) that ensure maintaining authenticity of data.
- Audit trail, meaning that handling of the electronic evidence should be properly documented by use of standard checklists, reports, photos, records, notes from the crime scene and other formal paperwork requirements in order to prove authenticity of electronic evidence.
- Computer forensics specialist support is an important, albeit not overly mandatory, requirement that is conditioned by highly technical nature of computer environment, as well as high degree of specialization required for proper processing of certain types of electronic evidence.
- Legality of evidence, meaning that only the data that is relevant to the purposes of investigation is extracted and secured, and other personal data of confidential nature is sorted out and not processed without proper authorization; where such data may be necessary, court orders preserving such data may be necessary to further proceed with analysis of information.

Question 10: Describe national institutions whose expert capacity might be useful in virtual currency-related investigations.

- Computer Security Incident Response Teams (CSIRTs) can be used as experts for malware and network analysis in cases where virtual currencies are used.
- Financial Intelligence Units (FIUs) can be brought in for advanced expertise on financial crimes and money-laundering techniques, and as intelligence experts with knowledge of handling suspicious transactions.
- High-tech crime / cybercrime units usually have expert capacity in terms of procedural actions aimed at criminal intelligence in cybercrime-

related cases (preservation, interception, monitoring), as well as first-response electronic evidence handling and analysis.
- Central expert institutions within countries may be requested to provide expert examinations and produce reports on electronic evidence based on their qualifications and technical capabilities.
- Private sector expertise may be sought in cases where highly specialized expertise is required for processing of specific types of evidence (e.g. energy management systems or mobile communications).

Question 11: Describe investigative indicators that may suggest the use of virtual currencies for the purposes of laundering crime proceeds.

- The use of financial red flags/indicators
    - None specifically relating to virtual currencies available but ones that are applicable in more general cases of laundering crime proceeds on the Internet are also applicable in cases of virtual currencies.
    - Refer to and discuss red flags from FATF "Money-laundering Using New Payment Methods".
    - Refer to and discuss red flags from Council of Europe "Criminal Money Flows on the Internet"
- The presence of software associated with the use of virtual currencies
    - Bitcoin wallets
    - Software associated with the use of other virtual currencies
    - Software for accessing virtual worlds
- Browsing history containing virtual currency related websites
- Remote storage services (e.g. dropbox)
    - Can be used for storage of virtual currency and/or credentials
- Credential storage software
    - Can be used for storage of virtual currency and/or credentials
- Virtual machines
    - May be used to conceal the use of virtual currencies in a virtual environment
    - Many virtual machine environments support encryption of virtual machine hard drives
- Mobile devices
    - Much virtual currency software that is available for PCs is also available for mobile devices
    - Browsing history indicating the use of virtual currencies may also be found on mobile devices

Question 12: Discuss the types of evidence that may be gathered through forensic analysis of a suspect's computer that may provide information about the laundering of crime proceeds through virtual currencies.

- There may be evidence in the form of credentials, visits to websites, emails, etc. that establish the suspect's relationship with a virtual currency administrator or virtual currency exchange.
- It may be possible to gather evidence to demonstrate a suspect's possession of particular virtual currency value.
- In the case of Bitcoin, it may be possible to identify particular Bitcoin addresses that are in the control of the suspect. Bitcoin addresses can subsequently be investigated to determine from which other addresses value was transferred to the suspect address and to which other addresses value was transferred by the suspect address.
- The IP address of the computer at a particular time may be associated with known suspect transactions or other financial activity.
- Evidence of the use of remote storage services, upon which virtual currency value may be stored.
- Passwords or other credentials that may be used to unlock virtual currency accounts or value.

Question 13: Describe the information that may be available from virtual currency central administering authorities and/or virtual currency exchanges and the available options for gathering this information.

- Subscriber and transaction information as well as communication with the suspect may be available from virtual currency central administrating authorities and/or currency exchanges.
- Options for gathering information
    - Direct contact with administrating authorities based on terms of service or privacy policy.
    - Police-to-police cooperation via local law enforcement.
    - Mutual legal assistance

Question 14: Discuss how public-private partnership can be an effective countermeasure against the laundering of crime proceeds using virtual currencies. Use a case study to illustrate the points made.

- Has been highlighted as the single measure with arguably the strongest impact on the prevention and control of criminal money flows on the Internet.
- Most initiatives relate to national cooperation and information exchange.
- A complex issue depending on which aspect of the public sector, which aspect of the private sector and what nature of cooperation is being considered.
- National private sector organisations can offer important information to investigations. Examples are financial institutions, ISPs, telecoms providers.

- Internationally information may be available from large multinational service providers. Examples are social networks, web-based email providers, etc.

Question 15: Discuss how inter-agency cooperation (public-public cooperation) can be an effective countermeasure against the laundering of crime proceeds using virtual currencies. Use a case study to illustrate the points made.

- Interagency cooperation may be formal or informal.
- Formal arrangements involve permanent infrastructure or arrangements (e.g. MOU) to facilitate the cooperation.
- Informal arrangements also frequently exist in practice between various agencies.
  Some examples of ways in which countries have implemented inter-agency cooperation are:
  - Drawing together of expertise from multiple agencies to identify investigative challenges.
  - Analyse representative cases by carrying out checks with national police authorities.
  - Describe enforcement approaches from the view of the police and the supervisory authority.
  - Establishing information sharing systems whereby agencies can be made aware of previous or on-going investigations into the same person and/or legal entities. This helps to avoid replication, and promote cross-fertilisation.
  - Establishing policies and procedures that promote the sharing of information/intelligence.
  - Establishing a process whereby disputes are resolved in the best interest of the investigation.
  - Competent authorities establishing written agreements such as Memoranda of Understanding or similar to formalise these processes.

4 Module 4: Seizure of Virtual Currencies

Question 1: What are the differences between crime proceeds and instrumentalities?

- Crime proceeds means any property derived from or obtained, directly or indirectly, through the commission of an offence. Such proceeds may consist of any type of property, whether corporeal or incorporeal, movable or immovable, and legal documents or documents that give title to or interest in such property;
- Instrumentalities means any property used or intended to be used, in any manner, wholly or in part, to commit any criminal offence(s).
- Virtual currencies can be both the proceeds and instrumentalities of crime, especially in cases involving money-laundering.

Question 2: What are the differences between freezing and seizure of crime proceeds and instrumentalities?

- Freezing of crime proceeds and instrumentalities means temporarily prohibiting transfer, conversion, disposition or movement of property, while still retaining the property in question under the owner's legal and effective control.
- Seizure of proceeds or instrumentalities of crime is also a prohibition of the transfer, conversion, disposition or movement of property on the basis of an action initiated by a competent authority or a court that allows such authorities to take control of specified property.
- Although seized property remains the property of the natural or legal person(s) that holds an interest in the specified property at the time of the seizure, the competent authority or court will often take over possession, administration or management of the seized property.

Question 3: Describe the need for expert assistance for identification and seizure of crime proceeds and instrumentalities.

- Securing proceeds and instrumentalities of crime requires specialist knowledge, and the context of virtual currencies may require even further specialization that may not be available within law enforcement itself.
- Formal financial expert examinations and reports of such examinations may be necessary to be used for effecting seizure of crime proceeds and instrumentalities.
- Expert involvement is particularly relevant where investigative actions for securing proceeds/instrumentalities of crime require judicial approval.

Question 4: Explain how applicable jurisdiction will be determined in international investigations of decentralized virtual currencies as crime proceeds?

- Decentralized virtual currencies constitute transactions between individual users' wallets.
- Territorial jurisdiction over proceeds or instrumentalities of crime in the case of decentralized crypto-currencies will be tied to the location of the wallet: that is, physical location of the hardware where the wallet containing the virtual currency resides. This is going to be the jurisdiction for the purposes of freezing, seizure and confiscation of the crime proceeds and instrumentalities.
- Determining the location of the virtual currency wallet is a subject of investigative and intelligence actions that would point at least to the jurisdiction in which relevant hardware is located.

Question 5: List at least two "red flags" for the tracing of crime proceeds involving virtual currency exchanges.

- Large number of bank accounts held by the same virtual currency exchange company (sometimes in different countries) apparently used as flow-through accounts (may be indicative of layering activity).
- Virtual currency exchange company located in one country but holding accounts in other countries (unexplained business rationale which could be suspicious).
- Back and forth movement of funds between bank accounts held by different virtual currency exchange companies located in different countries (may be indicative of layering activity as it does not fit the business model).
- The volume and frequency of cash transactions (sometimes structured below reporting threshold) conducted by the owner of virtual currency exchange company do not make economic sense.

Question 6: Explain the relevance of suspicious transaction reports (STRs) for identification of crime proceeds or instrumentalities in the context of virtual currencies.

- Suspicious transaction reports (STRs) are primary tools for financial intelligence used by financial intelligence units.
- Availability and value of STRs from central administrators will be usually linked with the degree of state regulation on virtual currencies and where such entities are obliged to file STRs to a national FIU.
- In cases of decentralized crypto-currencies, STRs that focus on virtual currency exchanges would be particularly useful source of intelligence in financial investigations of proceeds and instrumentalities of crime.

- Particularly relevant are STRs that target "red-flagged" transactions or currency exchanges.

Question 7: Describe the process of seizure (taking control) of decentralized virtual currency.

- The viable option for taking control over virtual currencies is using regular transaction mechanisms to transfer the currency to the account (wallet) of the law enforcement authority, which would take the following steps:
- Determining the amount of virtual currency items, wallets or both to be seized;
- Securing suspect's cooperation or exercising control over the wallet through other means permitted by law, so that the required sum can be transferred to a government-controlled wallet, pending liquidation upon forfeiture;
- Confirmation of receipt duly recorded; or
- Where cooperation or exercising control over the wallet is not viable:
    - Determine the value of virtual currency to be seized in local currency based on exchange rate;
    - Apply value-based recovery procedures.
- Value-base recovery can be used from the initial steps, in cases where direct seizure and control of virtual currency is not viable due to either to security or asset management considerations.

Question 8: List at least two modalities for international cooperation in financial investigations.

- Cooperation through dedicated international cooperation networks targeting proceeds of crime, such as the Camden Asset Recovery Inter-Agency Network (CARIN), the Stolen Asset Recovery Initiative (StAR), or more specialized networks for asset recovery such as the Global Focal Point Network on Asset Recovery.
- Use of police-to-police cooperation modalities, especially 24/7 contact points under the Convention on Cybercrime, G8 Network High Tech Crime Units or Interpol contacts, who can provide intelligence, execute preservation and carry out other investigative requests directly, without the need for lengthy mutual legal assistance procedures.
- Contact with foreign FIUs requesting access to STRs or other intelligence information or analysis through the national FIU with the use of the Egmont Secure Web or other, bilateral modalities.
- Engagement in formal procedures with central authority (Prosecutor's Office) for transmitting mutual legal assistance requests to foreign jurisdictions.

UNODC
United Nations Office on Drugs and Crime