Emerging Financial Technologies, Money Laundering and Terrorist Financing: A Typology of Virtual Currencies

IEWG Stream 3

Egmont Plenary, Buenos Aires, Argentina – March 2018

Acknowledgments

FINTRAC would like to thank the following colleagues, member FIUs and observers for their contribution to this report.

National Crime Agency (NCA)
United Kingdom

Cel voor Financiële Informatieverwerking – Cellule de Traitement des Informations Financières (CTIF-CFI)
Belgium

Finanspolisen Rikskriminalpolisen (FIPO)
Sweden

Office for Prevention of Laundering of Proceeds derived from Criminal Activity (Control Service) (KD)
Latvia

National Bureau of Investigation – Criminal Intelligence
Finland

Australian Transaction Reports and Analysis Centre (AUSTRAC)
Australia

Suspicious Transaction Reporting Office (STRO)
Singapore

New Zealand Police Financial Intelligence Unit (NZ-Police FIU)
New Zealand

General Inspector of Financial Information (GIFI)
Poland

HM Government of Gibraltar – Ministry of Commerce
Gibraltar Financial Intelligence Unit (GFIU)
Gibraltar

Agence National d'Investigation Financière du Gabon (ANIF)
Gabon

Wolfsberg Group Member

The Bank of Tokyo-Mitsubishi UFJ
Japan

Cellule de Renseignement financier (CRF)
Luxembourg

The Federal Financial Monitoring Service of the Russian Federation (Rosfinmonitoring)
Russian Federation

Financial Crimes Enforcement Network (FinCEN)
United States

Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)
Canada

The Egmont Group of Financial Intelligence Units

The Egmont Group is a united body of 156 Financial Intelligence Units (FIUs). The Egmont Group provides a platform for the secure exchange of expertise and financial intelligence to combat money laundering and terrorist financing (ML/TF). The Egmont Group continues to support the efforts of its international partners and other stakeholders to give effect to the resolutions and statements by the United Nations Security Council, the G20 Finance Ministers, and the Financial Action Task Force. The Egmont Group is able to add value to the work of member FIUs by improving the understanding of ML/TF current and emerging risks amongst its stakeholders.

Table of Contents

Executive Summary

This report highlights money laundering and terrorist financing risks, trends, methods, indicators and typologies in the area of virtual currencies. The purpose of the report, which FINTRAC produced as part of the Egmont Group's Information Exchange Working Group Stream 3 – Virtual Currencies project, is to familiarize financial intelligence units (FIUs) with this growing technology and the challenges it presents.

The report reviews past work and current literature on virtual currencies and provides an overview of four key concepts: virtual currency ATMs, virtual currency exchanges, virtual currency wallets, and mixers and tumblers. Initial coin offerings (ICOs) are also further explored. For each, the report covers associated risks, and provides overall indicators related to the use of virtual currencies and initial coin offerings.

Among the findings of the report, which features numerous case studies from the 15 contributing FIUs, along with the Bank of Tokyo Mitsubishi UFJ (member of the Wolfsberg Group) and the Ministry of Commerce of Gibraltar, are the following:

- Bitcoin continues to be the most prevalent virtual currency used for illicit activities, with other common ones including Ethereum, Monero and Litecoin
- In most jurisdictions, there has been a sharp increase in SAR/STR reporting related to virtual currencies, in particular Bitcoin, in the last three years
- Certain attributes of virtual currencies (e.g., anonymity) and mechanisms to conduct transactions involving virtual currencies (e.g., VCEs and virtual currency ATMs) allow individuals to circumvent the traditional financial system, obfuscate the origin or destination of funds, and avoid the scrutiny of reporting entities
- Some of the risks identified by FIUs include the role virtual currencies increasingly plays in laundering proceeds of crime, the challenge associated with tracing illicit virtual currency transactions, the lack of regulation of virtual currencies and virtual currency businesses, and virtual currency exchanges operating without licensing
- FIUs have indicated that there have been few prosecutions of cases involving virtual currencies, due in part to the fact that criminal proceedings are often not pursued
- FIUs have indicated that it is important to build a good working relationship between FIUs, virtual currency exchanges, reporting entities and law enforcement agencies for greater information sharing since the virtual currency industry is currently largely unregulated

Finally, the report sets out a number of other operational concerns and best practices for FIUs in the area of virtual currencies, and outlines issues identified by FIUs for further discussion.

1. Introduction

This report highlights money laundering and terrorist financing (ML/TF) risks, trends, methods and typologies in the area of virtual currencies. The report has several purposes:

- to familiarize financial intelligence units (FIUs) and law enforcement agencies with key concepts, trends and methods related to virtual currencies, including virtual currency ATMs, virtual currency exchanges, mixers and tumblers, and initial coin offerings
- to enhance understanding of how virtual currencies are used for ML/TF
- to propose indicators and typologies to recognize red flags and the use of virtual currencies to conduct illicit activities
- to connect the use of virtual currencies to conduct illicit activity—especially ML/TF—to dark net and other activities that may present risks for and lead to vulnerabilities in the financial system

Methodology

To produce this report, FINTRAC gathered and analyzed data submitted by FIUs and other stakeholders in response to a questionnaire. FINTRAC circulated the survey as part of the Egmont Group's Information Exchange Working Group (IEWG) Stream 3 virtual currencies project, following the launch of the questionnaire in Macau (July 2017) and the follow up conducted in Buenos Aires, (October 2017). Of the 17 contributing members, 15 are FIUs. The other two contributors are the Bank of Tokyo Mitsubishi UFJ, member of the Wolfsberg Group, and the Ministry of Commerce of Gibraltar. FINTRAC also reviewed publications by the Financial Action Task Force, the Egmont Group, law enforcement agencies, FIUs, government regulators, media and academia on virtual currencies.

2. Overview of Previous Work on Virtual Currencies

The Egmont Group and the Financial Action Task Force have published a multitude of reports and updates to inform FIUs, delegations and member states on the current trends and associated risks of virtual currencies. The following section provides a brief review of this work.

Financial Action Task Force (FATF)

Virtual Currencies: Key Definitions and Potential AML/CFT Risks (June 2014)[1]

This report proposes key definitions and vocabulary to clarify what a virtual currency is and offers a classification of the various types of virtual currencies based on their business models and methods of operations. The report also identifies the participants in typical virtual currency systems. In addition, the report outlines some of the uses and potential risks associated with virtual currencies (e.g., anonymity risks linked to decentralization, global reach and complex infrastructure that involve several entities, the lack of clarity with regards to supervision and enforcement, and the rapidly evolving nature of virtual currencies). The report also cites law enforcement actions involving virtual currencies, for example Liberty Reserve, Silk Road, and Western Express International.

Guidance for a Risk-Based Approach: Virtual Currencies (June 2015)[2]

This report builds on the report described above on the risk matrix and the best practices contained in the *Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet Based Payment Services report (June 2013)*[3]. Its intent is to explain the application of the risk-based approach to AML/CFT measures in the virtual currencies context, to identify the entities involved in virtual currencies payment products and services (VCPPS), and to clarify the application of relevant FATF Recommendations to convertible virtual currency exchanges. The report also provides an overview of various jurisdictions' regulatory approach and offers potential solutions to compliance challenges such as customer identification and verification, transaction monitoring requirements and the development of third-party digital identity systems to facilitate AML/CFT compliance.

RTMG Internal Review of Past Reports on VCs and Identification of New Emerging Risks, Threats and Vulnerabilities (Paris, February 2017)[4]

This paper identifies new ML/TF risks associated with virtual currencies as detailed in the above publications. The report discusses the changing virtual currencies landscape, which includes the growing number of players and technological advancements, and a growing market capitalization. The paper also outlines a set of outcomes for consideration by FATF RTMG members.

[1] Refer to http://www.fatf-gafi.org/publications/methodsandtrends/documents/virtual-currency-definitions-aml-cft-risk.html.
[2] Refer to http://www.fatf-gafi.org/publications/fatfgeneral/documents/guidance-rba-virtual-currencies.html.
[3] Refer to http://www.fatf-gafi.org/publications/fatfrecommendations/documents/rba-npps-2013.html.
[4] Refer to FATF/RTMG (2017)8. Update on Virtual Currencies (February 2017) – JT03408521.

RTMG Internal Review of Past Reports on VCs and Identification of New Emerging Risks, Threats and Vulnerabilities (Buenos Aires, October 2017)[5]

This report builds on the 2014 report and the 2015 FATF guidance, both noted above, and includes information and comments from 20 delegations. The paper identifies areas of work for FATF RTMG beyond the previously identified ML/TF risks associated with virtual currency payment products and services. The report also provides examples of virtual currency uptake and outlines risk mitigation experiences in various jurisdictions.

The Egmont Group

Virtual Currencies Paper (FIU Poland for Egmont's IEWG – January 2016)[6]

This paper identifies the risks, typologies, trends and methods in the area of misuse of digital currencies (in particular virtual currencies) for ML/TF purposes. The report includes an annex which includes cases of interest provided by contributing member FIUs.

[5] Refer to FATF/RTMG (2017)32. Virtual Currencies Update (October 2017) – JT03419767.
[6] Refer to Virtual Currencies Paper, IEWG, Egmont – General Inspector of Financial Information (GIFI), Poland.

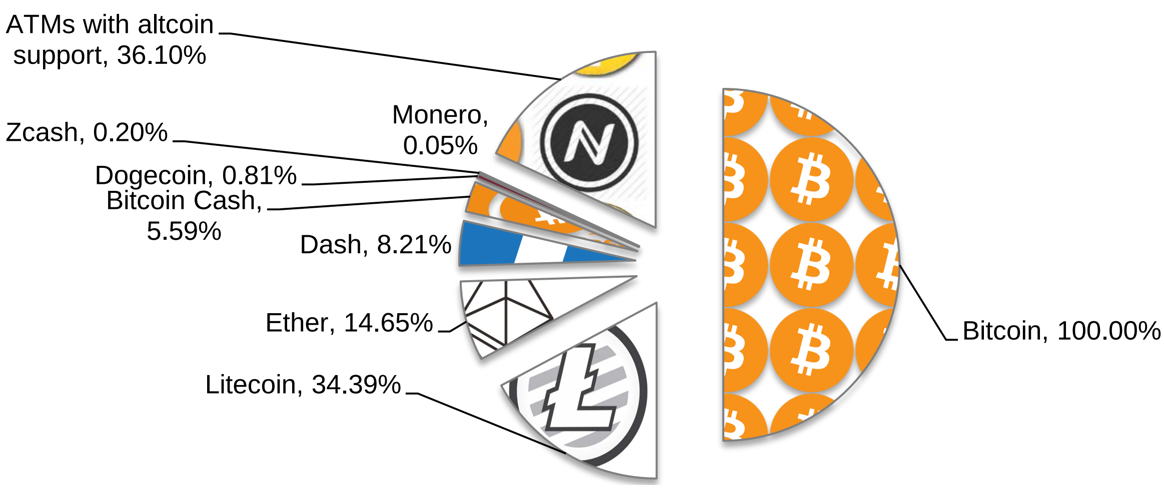
3. Key Concepts and Risks Related to Virtual Currencies

Virtual Currency ATMs

ATMs allow users to buy or sell Bitcoin, for example, using cash and to upload funds to their wallet. While ATMs offer an easy way to purchase coins or deposit funds, they have also been used in fraudulent activities or to launder proceeds of illicit activities.

The rate of installation of virtual currency ATMs has increased significantly over the last three (3) years. North America (75.23%) and Europe (19.14%) have the most installations of ATMs and Tellers in 2018. The figure below shows the number of ATMs around the world that accept Bitcoin (also known as BTMs) and other cryptocurrencies globally. In addition to Bitcoin (BTC), some of the other main cryptocurrencies accepted are Ethereum/Ether (ETH), Litecoin (LTC), Dash (DSH), Bitcoin Cash (BCH), Dogecoin (DOGE), Zcash (ZEC) and Monero (XMR). Appendix 1 provides the breakdown of ATM/BTM installations by contributing member FIUs and by continent.

Global Percentage of Virtual Currency ATMs by Cryptocurrency[7]



Source: as of January 5, 2018. Based on data from www.coinatmradar.com

Some FIUs have reported that criminals and criminal organizations are using BTMs and virtual currency ATMs for laundering proceeds of crime, and that they eventually cashed out the coins in other jurisdictions and/or outside of the banking system.

One FIU indicated that, on average, a kiosk operator[8] with eight (8) branch locations throughout a large metropolitan area conducted USD 565,000 in business in one month. The total number of revenue per kiosk terminal (BTM) was of USD 70,625 per month. This FIU also noted that law enforcement in their jurisdiction observed that most Bitcoin ATMs require only limited forms of identifying information to conduct the exchange transaction, despite regulatory requirements for this type of activity. It is also important to note that virtual currency ATMs/BTMs are not accessible through VC service providers such as Coinbase.

[7] As at January 5, 2018, the number of ATM/BTM totaled 4,011.
[8] Virtual currency ATMs and Bitcoin ATMs are also referred to as kiosks. The term kiosk refers to a Bitcoin or virtual currency ATM. A kiosk operator refers to an individual controlling a kiosk through a corporate registration.

One FIU indicated that a company had made regular cash deposits to its bank account explaining that the funds came from BTM machines located in two major cities in its jurisdiction and in many gaming centres. This company itself was not subject to the jurisdiction's AML/CFT framework or reporting obligations but enacted rules that limit cash deposits above a certain amount to people that have been appropriately identified beforehand. The FIU noted that anyone could use a BTM machine to anonymously convert cash into bitcoins if this activity were not correctly regulated and supervised.

Another FIU noted that they received multiple reports describing Bitcoin ATM that is consistent with structuring, where transactions are conducted to avoid Currency Transaction Report (CTR) reporting thresholds or transaction limits put in place by operators. Some operators limit users to less than USD 10,000 per day, likely to avoid having to file CTRs.

Box 1 – How a Bitcoin ATM/Kiosk Works

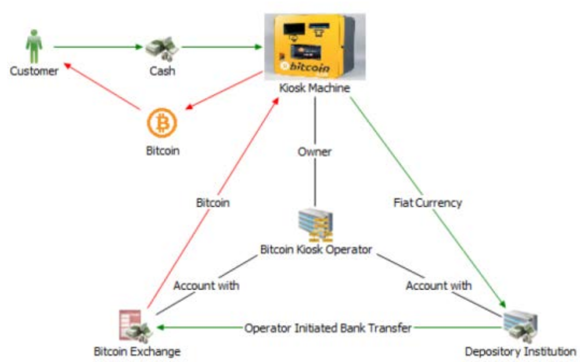
A typical cash deposit to a Bitcoin ATM involves the following steps:

1. Upon arriving at a kiosk, a user typically submits a mobile phone number in order to complete two-factor authentication (2FA) that the mobile phone number belongs to the individual at the kiosk.

2. The user chooses to scan his or her existing Bitcoin wallet Quick Response (QR) code or requests that the kiosk generates a new Bitcoin address.

3. The user then inserts cash or a credit card into the machine and the machine credits the selected customer wallet with bitcoin. This could include the wallet of a third-party not present at the kiosk.

4. A cash withdrawal from a Bitcoin wallet using an ATM works in the same manner, but with the user selecting to credit bitcoin to the kiosk from the provided wallet in return for cash. To effect transactions, the kiosk operator[9] may supply the cash and bitcoin or use a depository institution and bitcoin exchange.



Source: United States (FinCEN)

[9] Operators usually charge a fee for each transaction that generally varies between five (5) and 21 per cent.

Risks Associated with Virtual Currency ATMs

The following are some of the risks associated with virtual currency ATMs:

- Virtual currency ATMs/BTMs remain largely unsupervised or unregulated
- Transactions involve a simple two-step method to turn physical cash into virtual currency funds that are uploaded onto a virtual currency wallet;
- Transactions using virtual currency ATMs or BTMs are not insured
- Depending on the amount of virtual currency purchased, the fees associated with purchasing virtual currencies may result in a customer not actually receiving any virtual currency[10]
- Organized crime and street level drug dealers have used local virtual currency ATMs to launder proceeds of crime
- Virtual currencies have been used in multiple scams in which victims unknowingly sent funds to the individuals running the scam through the ATM
- Virtual currency ATMs/BTMs may be vulnerable to malware attacks such as Cutlet Maker[11]
- Virtual currency ATMs/BTMs are placed in locations that puts them at a higher risk of exploitation for criminal activity (e.g., strip clubs, marijuana dispensaries)
- Virtual currency ATMS have been extorted by criminal groups and some have been targeted by rival operators through physical vandalism of the VC ATMs
- The use of “ghost machines” – Bitcoin ATMs available only to trusted criminal groups and not openly publicized

Virtual Currency Exchanges

Virtual currency exchanges (VCEs) offer fee-based online services to exchange from legal tender for virtual currency, virtual currency for legal tender, or one virtual currency for another. Some of the most popular VCEs include: Bitstamp (Luxembourg and Slovenia), Kraken (United States), Bitfinex (Hong Kong), Coinbase (United States), and Binance (South Korea). While some VCEs may conduct varying degrees of Know-Your-Customer (KYC) identification (e.g., submitting a photo or taking a photo while holding an identification document), others do not require any KYC and allow individuals to open an account and purchase or sell virtual currency without any prior verification.

There are also informal exchange services that may offer to buy or sell virtual currencies from other virtual currency exchanges or from individuals in the same or a different jurisdiction. Often, informal exchange services do not require face-to-face purchases or conduct Know-Your-Customer (KYC) identification.

More than one FIU reported that criminals have used virtual currency exchanges to launder proceeds of crime, as was the case with BTC-e and MtGox, or to purchase virtual currencies from overseas-based virtual currency exchange businesses. Another FIU reported that an individual received money from a VCE and transferred the funds received to a person imprisoned in another country; the FIU suspected that the transaction could be related to potential drug trafficking in prison.

[10] Fees associated with the conversion of fiat currency to virtual currency may be higher than the fiat currency amount to be converted and deposited into a virtual currency wallet.
[11] Cutlet Maker is an ATM malware that can be easily purchased on the Darknet market for around USD 5,000.

Unlicensed or Unregulated VCEs and Virtual Currency ATMs/BTMs

Most FIUs have indicated in their questionnaire responses that unlicensed or unregulated VCEs and/or individuals operating as VCEs continue to remain a challenge both for them and their law enforcement agency partners. This is because the majority of jurisdictions do not maintain a registry of VCEs or do not yet require VCEs to comply with the regulations of a regulatory body or authority.

In addition, one FIU noted that they identified 32 virtual currency ATMs (kiosks) that remain unregistered despite the regulation in place in the jurisdiction, and are likely intentionally seeking to hide their status as a virtual currency business, and are attempting to avoid their banking institutions due diligence requirements for MSBs. STRs/SARs received from depository institutions banking on these businesses outlined that their these operators often inconsistently identify their business as “vending machine operator”, “electronic kiosk” and “conference call service provider”.

Risks Associated with VCEs

The following are some of the risks associated with VCEs:

- Customers can lose money or virtual currency on an exchange, since VCEs can be hacked
- VCEs have been used in loan-back schemes involving virtual currency to launder proceeds of crime
- In most jurisdictions, VCEs are unsupervised or unregulated and are not required to be registered or conduct KYC client assessments
- VCEs are used to transfer funds quickly either to launder proceeds of crime or as a conduit to purchase virtual currency and conduct illicit activity

Virtual Currency Wallets and Wallet Providers

Virtual currency wallet providers control access to virtual currencies by offering services to hold virtual currency funds in an electronic wallet. Some web-based virtual currency wallet providers, such as Coinbase, also offer virtual currency exchange services.

Users can also create virtual currency wallets using software, such as Electrum, and are accessible online, by mobile device or via desktop. Most wallet providers and wallets require users to trust the counterparty and that the infrastructure offers multiple layers of security to prevent potential hacking or the compromise of data.

The anonymity wallets and certain wallet providers offer continues to remain a challenge for FIUs and law enforcement agencies. Operating systems that offer a certain degree of anonymity, such as Tails, allow a virtual currency wallet (e.g., Electrum) to be embedded within them or allow access to other web-based wallets, such as Coinbase.

Plausible Deniability Mechanisms are used for hardware and bitcoin wallets to store virtual currencies, where a feature is added to allow for the creation of hidden wallets attached to the visible ones (e.g., Digital Bitbox).

Risks Associated with Virtual Currency Wallets and Wallet Providers

Some of the risks associated with virtual currency wallets include:

- Virtual currency wallets and wallet providers can be hacked or compromised
- Virtual currency can be stolen from a wallet
- There are no consumer protections and transactions cannot be reversed

Mixers and Tumblers

Mixers and tumblers are third-party services designed to obfuscate the financial trail of a virtual currency transaction on the blockchain by breaking the links between a sending and receiving addresses.

Mixers and tumblers are usually used in conjunction with the Tor browser to add a layer of anonymity to the online activity, and to reduce the capacity of an external actor to analyze transactions via the blockchain. Once the coins are mixed, they are sent back to the user as clean coins.

There are multiple mixing and tumbling services offered on the web (both dark and surface) with varying capacities (some of which require registration). Some of the popular are Helix (see Box 2 below), Bitcoin Blender, BitMixer.io, Bitcoin Fog, Pay Shield and CoinMixer.se. Privcoin.io is the first mixer to offer mixing services for multiple cryptocurrencies.

Anonymity enhancing cryptocurrencies (AECs) are cryptocurrencies designed to obfuscate transaction information and are increasingly used by transnational criminal organizations (TCOs). These AECs normally have built-in mixing services as part of their blockchain services (e.g., Dash), or can provide anonymity through other features without embedding tumbling services in their design (e.g., Monero).

Other cryptocurrencies (e.g., Bitcoin) are not anonymous or pseudo-anonymous on their own: however, when they are combined with software such as Tor or Tails, it becomes more difficult for law enforcement to trace transactions or activity back to an individual or organization. The use of anonymizing tools such as Tor is common on the Darknet, where cryptocurrencies are used to purchase goods and services.

Nascent technologies, such as Bulletproof, developed by researchers at Stanford and the University College of London[12], can make transactions confidential by hiding transaction amounts from public view (also known as CT), and to reduce transaction fees. Monero, for example, uses stealth addresses[13], ring signatures[14] and confidential transactions to achieve both privacy and anonymity of transactions.

In their questionnaire responses, FIUs indicated that they suspected money laundering related to the use of tumbling or mixing of bitcoins, especially in conjunction with Darknet marketplace activities. One FIU recorded more than 37 reports linking tumbling/mixing services and suspicions of money laundering.

[12] Refer to https://crypto.stanford.edu/bulletproofs/.

[13] Addresses that are used as a decoy on the Monero blockchain. These addresses are generated to receive Monero but cannot be linked back to the true owner.

[14] Ring signatures are digital signatures that allow for the mixing of transactions to mask the origin of a transaction, where a group of possible signers are combined to produce one distinctive signature that can validate a transaction. In the case of Monero, the “ring” is composed of the actual signer (the spend key corresponding to an output from the sender’s wallet) and the non-signers (past transaction outputs from the Monero blockchain), which are all considered to be equal. As such, the “ring” ensures that the inputs cannot be identified by mixing the transactions.

Box 2 – Helix: How the Mixer of Choice of the Dark Web Works

Helix by GRAMS, which be accessed via its .onion or surface web link is one of the most popular mixers used on the dark web.

The mixing process has three (3) simple steps:

1. The user enters the Bitcoin address to which the clean coins are to be sent.
2. Helix provides the user with a Helix address to which to send the "dirty" coins, for a minimum of 0.02 BTC to a maximum of 21 BTC (bitcoins).
3. The clean coins are sent back in one transaction, minus a 2.5% "cleaning up" fee. (This can take a few hours, following the validation of the transaction initiated by the user).

Sources: Deepdotweb, Helix

Risks Associated with Tumblers and Mixers

There are multiple risks associated with tumblers and mixers that can challenge the capabilities of FIUs, financial institutions and law enforcement when tracing transactions on the blockchain or ensuring proper KYC requirements are met.

The following are examples of these risks associated with tumblers and mixers:

- Tumblers and mixers are currently not covered by legislation
- Most tumblers and mixers do not require users to sign up for an account, or to show any form of identity verification, and do not conduct KYC protocols
- Tumblers and mixers can be used with other anonymizing tools, such as Tor
- There are no direct links between the "physical" and "virtual" identity of a user

- Some mixers and tumblers have the capacity to randomizes service fees (e.g., 1-3% in the case of Bitcoin Blender) to prevent transaction tracing or to prevent an external party from conducting blockchain analysis
- Some mixers and tumblers gives users the ability to receive funds at multiple addresses and at different times (delay of withdrawals)
- Some mixers and tumblers have built-in features to allow for random delays and random transactions before sending funds to the client
- Pretty Good Privacy key encryption verification (a form of key encryption used to sign message to verify the identity of the sender and the validity of the content)[15] is often not required

Virtual Currencies Indicators and Typologies

General

- Transaction involving one or more virtual currency (e.g., Bitcoin) combined with other suspicious account behaviours or activities
- Excessive number of third-party transfer payments that are rapidly defunded to businesses suspected to be involved with a virtual currency (e.g., Bitcoin)
- Credits to the account are in rounded sums, with account activity indicating that the customer is a middleman processing criminal proceeds into virtual currency (e.g., Bitcoin), to deliberately obfuscate audit trails and attempt to make the funds appear legitimate
- Unusual third-party payments followed by movement of funds into accounts that are then transferred quickly to virtual currency exchange companies
- Virtual currency funds may be linked to hacked accounts
- Account appears to be funded by unknown and unrelated third-party deposits that have no apparent reasoning
- Payments or activity linked to funds from hacked accounts or accounts known to be connected with illegal activities
- Virtual currency transaction is conducted in jurisdiction with limited or no regulation of the virtual currency sector
- Transfers between accounts suspected of illicit activity (e.g., fraud)
- Transfers and deposits involving one or multiple virtual currencies across multiple jurisdictions
- Use of tumbling or mixing services
- Darknet market spends through alternative payment platforms
- Unusual and unexpected third-party payments that are very quickly used for payments to virtual currency exchanges
- Inconsistent explanations as to the source of funds that have been used to transact and purchase virtual currencies
- Payment in virtual currencies to websites known to be associated with illegal activity (e.g., Backpage.com)

[15] Refer to https://support.kraken.com/hc/en-us/articles/201648223-What-is-PGP-encryption-

- Use of Bitcoin or virtual currency ATMs/BTMs[16]
- Virtual currencies sent to wallets known to be associated with illegal activities
- Virtual currency ATMs/BTMs are placed in locations that may have ties to criminal activity (e.g., drug sales, prostitution) such as: convenience stores, gas stations, smoke shops, restaurants, strip clubs, night clubs, shipping stores, marijuana dispensaries, and vape shops

Purchase of virtual currencies (where two or more apply):

- Buyer offers services via the Internet through "supply and demand" websites (e.g., Localbitcoins.com)
- Buyer doesn't establish identity of the seller, or buyer hides their own identity
- Buyer pays in cash to purchase virtual currencies
- Buyer prefers to meet in a public area
- Buyer applies an unusually high commission as an "exchange fee"
- Transaction does not make economic or financial sense
- The amount of virtual currency purchased does not make economic or financial sense, given the average use by the user(s) or individual(s)
- The buyer is not licensed or registered as an official virtual currency money service business or as an exchange office
- The buyer is not compliant with the reporting requirements of tax authorities in the jurisdiction (where virtual currency transactions are regulated by tax authorities)
- Proceeds of the sale of virtual currencies are immediately withdrawn in cash

Initial Coin Offerings (ICOs)

Initial Coin Offerings (ICOs) are unregulated issuances of "cryptocoins" to raise money in bitcoin or other cryptocurrencies.[17] Also known as Initial Token Offerings (ITOs), the coins are digital coupons, or tokens, issued on a distributed ledger or blockchain. They can be traded but do not confer ownership rights[18], and their supply can be modified through a process referred to as coin burning[19].

ICOs do not have the same legal requirements as initial public offerings (IPOs) or a security sale in most jurisdictions, and they are treated as a donation, crowdsale or a form of *caveat emptor* investment.

ICOs are generally announced on cryptocurrency forums such as Bitcointalk, and are typically backed by information on the project, a whitepaper, project goals, timelines, names of the individuals in the team and other details related to the ICO[20].

[16] This indicator should be used with one or more indicator.
[17] Refer to https://www.ft.com/content/ce3ef54e-371b-11e7-bce4-9023f8c0fd2e.
[18] Refer to https://www.economist.com/news/finance-and-economics/21721425-it-may-also-spawn-valuable-innovations-market-initial-coin-offerings.
[19] Also known as "proof of burn", is a protocol used by altcoins to reduce the available supply of a cryptocurrency. Coins are taken out of circulation and placed into an "unspendable" wallet that cannot be accessed by users. This process is recorded on the blockchain as proof that the "burnt coins" cannot be spent again, but they remain part of the overall supply of the cryptocurrency.
[20] Refer to https://www.coinschedule.com/.

A multitude of cryptocurrencies have been developed through an ICO, including Ethereum (raised over USD 15 million), Waves and Mastercoin.[21] Digital tokens may represent ownership or a security interest over an issuer's assets or property, or a debt owed by an issuer. Such tokens may therefore be considered an offer of shares or units in a collective investment scheme, or a debenture. The Howey Test is commonly used to confirm if an asset is a security (see Box 3).

In the last year, multiple ICOs have been associated with Ponzi scheme-style scams and other types of scams, including shilling, which refers to the unsolicited promotion or endorsement of a coin in public. It is usually a type of scam in which a coin or token is promoted as being valuable in the future. As such, regulatory authorities across the globe have issued warnings and concerns about them. Appendix 2 includes a table outlining what the jurisdictions of contributing member FIUs are doing to mitigate the risks of ICOs, including issuing warnings and proposing legislation and regulations.

Case Study – ML Risks Associated with ICOs (Canada)

PlexCorps; PlexCoin; SidePay.ca; Dominic Lacroix; and Sabrina Paradis-Royer rose more than USD 15 million in funds from unlawful activities, by running an ICO scam scheme which promised returns of 1,354 percent in under 29 days.

The two individuals allegedly misappropriated over USD 200,000 of the investments for personal expenditures by raising funds illegally through the unregistered sale of securities called "PlexCoin" or "PlexCoin Tokens". Lacroix was previously banned from dealing in securities for violating Canadian securities law and defrauding previous investors.

The Quebec Superior Court ruled in favour of the Autorité des marchés financiers (AMF), following an order by the securities regulator for Lacroix and Paradis-Royer to stop soliciting investments for PlexCoin. In the U.S., the SEC also obtained an emergency court order and filed charges to freeze PlexCoin, Lacroix et al.'s assets.

Source: Canada (AMF; 2017 QCTMF 88), United States (SEC; CV17-7007-DL-RML)

Risks Associated with ICOs

The following are some of the risks associated with ICOs:

- Multiple ICOs have turned out to be fraud schemes (mostly in the form of Ponzi or pyramid schemes)
- Lack of transparency, including the rights of the holder of tokens, and how financing will be used is described very vaguely or at times, not at all
- The ICO team and promoters suddenly withdraw from the ICO project after the ICO sale has concluded
- Due to their global reach, ICOs can be issued abroad, and are therefore subject to foreign law, making tracking and recovering funds in the case of an ICO collapse very difficult
- There is no legal protection for investors due to lack of regulation in most jurisdictions
-

[21] Refer to https://www.smithandcrown.com/what-is-an-ico/.

Box 3 – Is an ICO a Security? Applying the Howey Test

Under the Howey Test, created by the U.S. Supreme Court in 1946 (SEC v. Howey), a transaction is considered to be an investment (i.e., investment contract, security) in the following circumstances:

1. It is an investment of money (including assets other than money)
2. There is an expectation of profits from the investment
3. The investment of money is in a common enterprise
4. Any profit comes from the efforts of a promoter or third party

If the token ICO/ITO passes the Howey Test, it must be treated as a security (investment contract) and is subject to SEC regulations. The Howey Test is largely considered to be a benchmark for determining whether an ICO may be considered a security under U.S. federal law, as was the case with the SEC decision related to the sale of DAO tokens.

Source: Securities Exchange Commission (SEC) – United States

Initial Coin Offerings Indicators and Typologies

- White paper is of poor quality, incomplete, misleading or only has limited information
- Hype is created around the ICO (e.g., pushy advertisement, celebrity endorsement); also known as “pump and dump” ICOs
- No background checks done on the ICO participants
- The token is listed as an investment instrument, and the platform used is only for secondary trading of the specific token
- The developers are anonymous or information provided is not/cannot be verified
- The project is only at the conceptual phase and there is only limited documentation available which sets out unrealistic objectives (e.g., amount of capital to be raised is disproportionate to the project value creation) and there is no other documentation or information available
- There is no access to the smart contract, code or technical information about the token creation
- The ICO project does not use a decentralized network or a digital ledger technology application, and the ICO is only meant to raise funds
- There is no possibility to sell the investment or exit the project to recover the invested funds
- The technology used to create and distribute the tokens is not tested, or the programs and codes are faulty and lack proper cyber-protection protocols

4. Virtual Currencies: Cases, Trends, Illicit Methods & Activities

This section will feature cases, trends and methods related to virtual currencies, money laundering and terrorist financing activities. Where necessary, the case studies, which were provided by contributing member FIUs, have been sanitized and summarized.

Key Findings

The following is an overview of key findings resulting from the contributions by the member FIUs:

- Bitcoin continues to be the most prevalent virtual currency used for illicit activities, with other ones including Monero, Dogecoin, Ethereum and Litecoin
- In most jurisdictions, there has been a sharp increase in SAR/STR reporting related to virtual currencies, in particular Bitcoin, in the last three (3) years
- One FIU indicated that they receive little information regarding activity involving AECs from regulated VCEs due to the limited information available on transactions and counterparties, but inversely, receive around 500 reports each month on Bitcoin
- One FIU underlined that reporting by customs in their jurisdiction on offences involving virtual currencies also increased and that this activity was reported more than by police force bodies
- In some jurisdictions, individuals named in SAR/STR reports, or who were disclosure subjects, were aged between 20 and 35 years old
- One FIU noted that on average, the total amounts involved in the reports received involving bitcoin totalled 82.71 BTC[22]
- One FIU noted that it has faced a challenge in assessing which cryptocurrencies are the most commonly used when checking against its database, due to the number of virtual currencies in circulation, and the upkeep required to keep the internal list up-to-date
- Some of the reporting featured individuals or entities buying and selling virtual currencies to generate profits, and the individuals were often unlicensed
- Some of the reporting indicated that individuals or entities conducting virtual currency-related activities for profit subject to income taxes did not report those profits
- Money laundering resulting from drug trafficking, including drug trafficking on the Darknet, and involving virtual currencies, was one of the most prevalent predicate offences FIUs identified
- The majority of FIUs reported criminals use virtual currencies in fraud schemes as a way to avoid being identified and located by their victims
- Individuals (using their own bank account) or unlicensed companies acting as intermediaries in bitcoin transactions used wire transfers to receive funds from third parties and transfer these funds to virtual currency exchange platforms (in the case of companies, the amounts received were large)

[22] Equivalent to more than EUR 500,000 as at March 26, 2018. Refer to www.coinmarketcap.com

- One FIU indicated that the top three (3) virtual currency-related offences recorded by the jurisdiction's customs agency were narcotics offences, smuggling and unlawful use of narcotics, whereas their police bodies reported that fraud, unlawful use of narcotics and narcotics offences were the top three (3) offences
- One FIU indicated that the top six (6) predicate offences were links to the Dark Web, forged documents (e.g., stolen or forged documents), drug trafficking, fraud, cybercrime and KYC issues

Contributing member FIUs reported illicit activities, predicate offences and suspicious activities related to virtual currencies. Most suspicious activities reported involving virtual currencies often involve other suspicious activities as well (e.g., fraud, proceeds of crime, drugs, etc.).

Case Studies

Money Laundering

Case Study – Money Laundering Investigation Related to Virtual Currency Activity

[This an ongoing criminal investigation on the use of virtual currencies for money laundering purposes. The case has been sanitized due to the sensitive nature of the file.]

As part of an ongoing money laundering investigation, Law Enforcement in this jurisdiction carried out multiple searches in multiple cities in the jurisdiction. The inquiry was set up as a result of findings showing that services were provided on the online marketplace *localbitcoins.com* to exchange bitcoins for cash or vice versa. In particular, the account of online Entity A appeared to be active in Country A, as well as two other countries.

The bitcoins could only be exchanged with Entity A for large amounts of cash (minimum of EUR 5,000) or vice versa and against a large commission which is many times higher than the usual commission through the known and smooth channels of online "exchangers".

After an initial contact through the *localbitcoins.com* marketplace, they switched to secure communication channels (such as a mobile application that offers encrypted messaging services) for further discussion.

During the searches, the equivalents of EUR 100,000 in cash and EUR 300,000 on accounts at financial institutions and internet service providers as well as computer equipment were seized. Three (3) individuals were taken in for questioning and appeared before the Judge, and two of the individuals were charged with and arrested for money laundering.

The inquiry revealed serious indication that the two arrested individuals carried out numerous transactions over multiple months, exchanging bitcoins for cash and vice versa, not only in Country A, but also two other countries. These transactions happened during short face-to-face meetings with customers in public places such as car parks, hotels, fast food restaurants, and etc.

During a search in a garage in one of the cities, which was suspected to be a temporary warehouse for cash, more than EUR 90,500 in cash was found under the spare wheel of a stolen vehicle. The police forces in Country B also conducted a house search in a city at the residence of one of another individual at the request of the Judge of a jurisdiction in Country A. This person was suspected to be a customer of the two individuals arrested. During this search, computer equipment was also seized.

Another individual, a citizen of Country B, was also put into custody. He was charged with money laundering.

Sellers and buyers on illegal marketplaces often believe they are untouchable by the police and the law, especially if the trade happens in bitcoins and the exchange of any ‘dirty’ bitcoins for cash is supposedly out of sight of the police and the law through online service providers such as Entity A.

By conducting criminal investigations and prosecuting these criminals, it has become clear that such illegal online services are not as anonymous as these service providers and their customers like to think. In this respect, this inquiry goes hand in hand with the recent taking down of online marketplaces and in the framework of foreign criminal investigations. The inquiry into the online Entity A and the two individuals arrested, and their customers, is ongoing.

Source: FIU from Country A

Case Study – Money Laundering & VCEs (Canada)

Person A, is the director of Company A, which purchased a wire transfer to the benefit of Person B. Person B benefited from EFTs from a foreign digital bank accepting Bitcoin located in Country A as well as some third-party cash and cheque deposits from his own company, Company B, and from a VCE located in Country B (which is owned by Person C).

Person B conducted cash withdrawals and purchased bank drafts to the benefit of car dealership and a real estate company.

An STR was filed against Person B after multiple cash and cheque deposits from Person E, Person F, and Person G who, according to publicly available information, is a manager for a virtual currency exchange (VCE) located in Country B. Cheques were also issued from the same VCE to an account held by Company I, from which wire transfers were then sent to a suspected virtual currency exchange located in Country C.

Company I is the beneficiary of EFTs from a foreign virtual currency exchange located in Country C, which was accused of money laundering. As well, Company I sent EFTs to the benefit of the same virtual currency exchange located in Country C and to another foreign virtual currency exchange also located in Country C. In addition, Company I also sent EFTs to the benefit of a cryptocurrency trading platform located in Country C.

Company I also ordered EFTs to companies involved in cryptocurrency exchanges with an international payments company located in Country D, and a payment service provider dealing with virtual currencies.

Furthermore, Company I ordered EFTs to the benefit of a Country E financial services company, which was responsible for founding a foreign virtual currency exchange, which was suspended by a foreign government for money laundering.

Person A owns Company J (from which he benefited of wire transfers through a payment service provider) and a virtual currency exchange located in Country B; these two companies share the same address.

An STR was submitted for Person H, who according to an STR, is suspected of operating as an unlicensed/unregulated VCE after he purchased wire transfers to the benefit of Company A.

Source: FINTRAC – Canada

Case Study – Money Laundering & Bitcoin ATM (United Kingdom)

[Example of a report made with suspicions of ML]

The Bitcoin user would mainly come into Company A and appeared to be under the influence of drugs. On one occasion the subject tried to get the staff to open the machine after stating that the Bitcoin wallet hadn't been updated, becoming agitated and making threats when this request was refused. The subject then came back on consecutive days to use the Bitcoin ATM, making deposits each time […]

On one occasion the subject tried to state that the wallet had not been updated, however the ATM owner confirmed that this was not the case. On some occasions the subject would enter the shop to use the machine with multiple other subjects. This has led the reporting entity to believe that the subject may be laundering cash through the Bitcoin ATM.

Source: National Crime Agency (NCA) – United Kingdom

Case Study – Movement and Laundering of Funds using a Bitcoin ATM (United States)

1 // A kiosk operator reportedly deposited roughly $300,000 in cash contained inside laptop bags. The filing institution noted the bills had the odor of marijuana.

2 // Twelve (12) transactions facilitated by a Bitcoin kiosk operator in the Eastern United States were associated with suspicious activity. These transactions showed connections with Darknet markets, mixers, a prostitution-related payment processor, and allegedly criminal Bitcoin exchange BTC-e.

Source: FinCEN – United States

Tax Evasion

Case Study – Tax Evasion & Virtual Currency Exchanges (Latvia)

A Latvian national provided agent services for Bitcoin exchange by using an online Bitcoin exchange platform and transferring funds for Bitcoin purchase to a company that is engaged in Bitcoin market, but registered in another country. The subject had failed to report income from Bitcoin trade to tax authorities, and thus the subject had not paid personal income tax and capital income tax. The subject had committed evasion of tax payments on a large scale.

Another Latvian national, after receiving possibly defrauded funds to their bank account, transfer the funds to the other mentioned subject's bank account for Bitcoin purchase. The funds comingled with other funds on the account and were further used for ATM withdrawals, purchases, or various debit transactions.

Source: Office for Prevention of Laundering of Proceeds derived from Criminal Activity (Control Service) (KD) – Latvia

Darknet Markets & Drug Trafficking

While browsing the Dark Web or the Darknet is not a predicate offence, multiple contributing member FIUs reported the use of virtual currencies (mostly Bitcoin) on Darknet marketplaces involving illicit activity. The top Darknet markets listed by a reporting entity reported by one FIU were Agora, AlphaBay, Evolution, Abraxas and Dream Market.

Darknet activity involving the use of virtual currencies revolved mostly around the sale of narcotics and illegal substances, in which buyers and sellers purchased virtual currency for use in the Darknet.

When reporting entities close a subject's bank account(s), they are only able to temporarily disrupt the subject's activities. However, the subject's virtual currency wallets or addresses are often more difficult to link back or to trace, and the "physical" accounts closure is likely to have a minimal impact on the individual's online activities.

Case Study – Darknet Markets, Illicit Drug Activity & VCEs (Belgium)

A suspect and members of the suspect's family hold several bank accounts with different financial institutions. All the bank accounts of the main suspect were opened in September 2015. Similar transactions took place on different bank accounts: these consisted of wire transfers from VCE platforms, subsequently followed by cash withdrawals. The transactions amounted to more than EUR 100,000 between September and December 2015.

The suspect limited the amount per transaction to EUR 2,500 to avoid being detected by the financial institutions and split up the transactions between several financial institutions and several family bank accounts.

On one occasion, he transferred the money received from the VCE platform to his mother's bank account before withdrawing the funds in cash. The main suspect led to believe to be working as an IT specialist, but at the same time he was receiving unemployment benefits.

The main suspect featured in a law enforcement investigation related to potential drug trafficking on the internet. A dealer in synthetic drugs (MDMA) was active via an online hidden market place on the Darknet.

Orders of drugs were sent via national and international mail shipments. Payments happened in VCs. The main suspect was providing financial services to the drug dealer converting the VCs into real currencies (EUR). He was holder of a bitcoin account/address linked to one of his bank accounts in Belgium.

Source: Cel voor Financiële Informatieverwerking – Cellule de Traitement des Informations Financières (CTIF-CFI) – Belgium

Case Study – Darknet Markets Activity (United Kingdom)

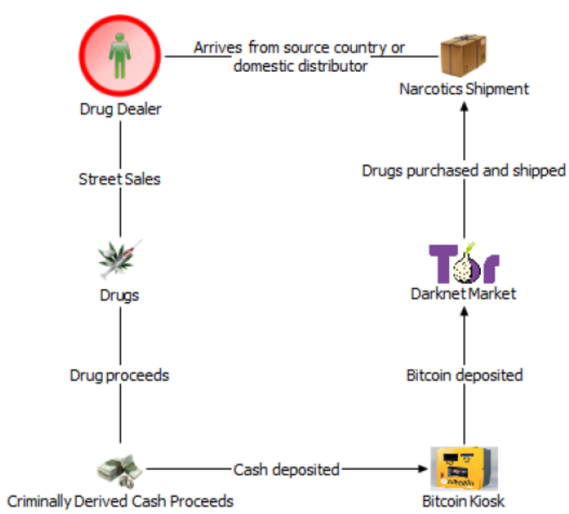
[Example of a report made with suspicions of ML]

The subject was referred for investigation. The primary reason for referral was Darknet activity. A decision to file a SAR was made based on evidence that the customer is engaged in Darknet activity. The subject was notified of the account closure.

Source: National Crime Agency – United Kingdom

Case Study – Drug Activity, Laundering Proceeds & Bitcoin ATMs (United States)

FinCEN, through cooperation with law enforcement, is aware of at least two instances of street level drug dealers using Bitcoin kiosks to purchase bitcoin, which were subsequently used to obtain drugs on Darknet markets. Narcotics were eventually shipped to the dealer through the mail and sold on the street.



Of the two investigations, one connected to a local police department in which Bitcoin kiosk receipts were located on a prescription pills dealer operating at a high school, and the other involved a federal task force operating in a large U.S. city which identified Bitcoin kiosk purchases by a known local drug dealer associated with a street gang.

Source: FinCEN – United States

Case Study – Illicit Activity Drug Trafficking Involving a VCE (New Zealand)

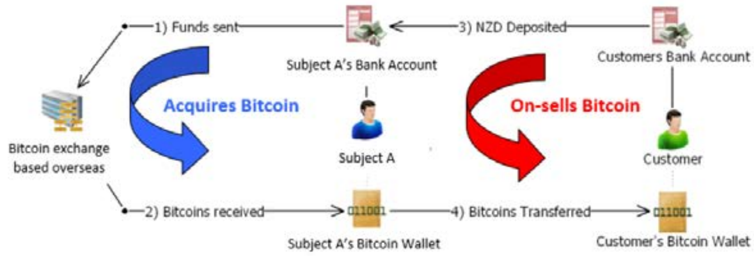
Bank monitoring detected that Subject A, a New Zealand resident, had been purchasing bitcoins in roughly NZD 5,000 amounts six times during one month. Subject A also received numerous payments from third parties into their bank account indicating that Subject A was generating significant profit from selling bitcoins. However, no payments had been made to Inland Revenue.

The typology associated with these suspicious transactions has two phases. First, Subject A is acting as a "middleman", purchasing Bitcoin from an overseas marketplace. These bitcoins are then transferred to a Bitcoin wallet that is controlled by Subject A.

In the second phase, Subject A solicits and receives payments from customers into their bank account, and when these funds have cleared, Subject A transfers bitcoins from their own wallet to the customers' Bitcoin wallet (or wallets). Central to Bitcoin's popularity with drug offending is that wallets are easily [anonymized] and hidden. However, by observing the NZD side, as shown in the top half of the below diagram, the New Zealand FIU was able to infer what Bitcoin transactions were taking place.

The financial analysis of Subject A's bank account records showed that since mid-2012 the account had received increasing amounts of ad hoc, unexplained deposits, to the point where throughout 2013 Subject A's income from the employer was dwarfed. A number of deposits contained reference numbers and [implying] they were related to the purchase of bitcoins.

Further enquiry identified that a number of the people, depositing money to Subject A's bank account, had drug dealing histories and that the likely Bitcoin purchases were consistent with online drug purchases. Enquiries also identified that victims of fraud or ransomware attacks were using Subject A to purchase bitcoins to pay to offenders.



Source: New Zealand Police Financial Intelligence Unit – New Zealand

Case Study – Operation Racecourse (New Zealand)

An investigation entitled Operation Racecourse was conducted by the Palmerston North Police in conjunction with the New Zealand Customs Service, originating from FIU analysis of four Bitcoin related STRs on a previously unknown 20-year old student, Subject C. Operation Racecourse focussed on the drug dealing activities of Subject C, who was believed to be involved in activities related to the importation and supply of Class A and B controlled drugs into New Zealand.

In April 2013, Operation Racecourse was terminated with the execution of Police search warrants and the arrest of the subject. Termination resulted in numerous charges for importation and distribution of cocaine, methamphetamine, ecstasy and LSD, as well as around NZD 130,000 assets seized.

Subject C had been using other people's addresses, to which he had sent packages of drugs he had purchased from Silk Road website. He also used other "dead" addresses where he had packages delivered to. The dead addresses were locations known to Subject C as being unoccupied at specified times, due to their occupants being either on holiday or at work. He would wait on the front porch at the "dead" address for drug courier packages to be delivered there.

Drug purchases were made by Subject C's bitcoin account on Silk Road. The subject also claimed he had another Bitcoin account with Japanese Bitcoin exchange MtGox, which he credited using USD and NZD currency from three of his numerous bank accounts he held in New Zealand.

Subject C had a number of accounts held at various New Zealand banks. None of these accounts showed legitimate income aside from student allowance payments and a small amount of seasonal wages. However, all accounts received significant cash deposits and electronic movement of funds between his bank accounts and/or to MtGox.

Subject C, whenever challenged by banks regarding the source of the cash deposits he was making, stated that he was engaged in the business of buying and selling computers for fellow students. There was no evidence of the trade of computers found on Subject C's TradeMe account, nor there were other business transactions that could explain the amount of income he had earned over the analysed period.

The subject's TradeMe history did detail the purchase of a set of electronic scales, described as "digital 0.01g x 300g." The purchase date of the scales was consistent with Subject C's explanation to Police that his first purchase of controlled drugs was made in that same month. The FIU received several suspicious transaction reports from New Zealand banks about irregularities in his financial activity, and they have contributed to Operation Racecourse.

Source: New Zealand Police Financial Intelligence Unit – New Zealand

Cybercrime

Ransomware and other cyber-enabled crimes often require payment in virtual currencies (e.g., WannCry, Petya), due to ease of access, the degree of anonymity and the ease of payment collection from the hackers. There have been numerous instances in which virtual currencies have been laundered or cashed out following ransomware attacks or other types of cyber-extortion.

Another type of cyber-enabled crime is cryptojacking, which is the malicious use of an individual's or group of individuals' computers to mine cryptocurrency when an infected site is visited for profit. A program or extension is secretly installed to mine cryptocurrency without the knowledge or permission of the victim. This method has been used by countries that are facing economic sanctions such as North Korea[23].

Case Study – Malware & Virtual Currencies (Latvia)

An individual's computer was infected with a virus (via distributed email) that encrypted all the documents leaving instructions on how they could be retrieved. The cost of retrieving the data was requested in the amount of three (3) Bitcoins.

Source: Office for Prevention of Laundering of Proceeds derived from Criminal Activity (Control Service) (KD) – Latvia

Fraud

Contributing member FIUs reported various types of fraud involving virtual currencies, including fake job advertisement, tax scams, and extortion.

Case Study – Fraud Scam Involving Virtual Currencies (United Kingdom)

[Suspicion had been raised on the account of transaction patterns showing that the customer had received funds from several accounts that had been closed for suspected fraud.]

The customer had deposited over $700 on his Company A account in Bitcoin. The primary source of funds on the account is from person-to-person transfers totaling almost $7,000 from other Company A members, based in multiple jurisdictions. The primary source of funds on these accounts is card and bank deposits. There is suspicion that the account has been used for the layering of funds.

Source: National Crime Agency – United Kingdom

Case Study – Use of VCEs, Virtual Currencies & Online Fraud (Belgium)

A Dutch citizen held a bank account in Belgium. He explained to the bank that he occasionally stayed in Belgium and that he therefore needed to have a bank account in Belgium. The transactions on the bank account do not match the customer profile and with the expected use of the bank account.

Although the bank account of the Dutch citizen was not supposed to be used for with commercial activities (the Dutch citizen does not carry out any commercial activities in Belgium), the bank account received by wire transfers from a VC exchange platform in Germany for a total amount of more than EUR 100,000. The funds were subsequently transferred to personal bank accounts in the Netherlands. The Dutch citizen is the owner of a company operating an online website selling goods to the public.Negative information was found on the internet about the Dutch online website indicating that the website was potentially fraudulent. Customers posted many claims on the internet about the website (impossible to contact the owner of the website, no refunds when goods of poor quality are returned, etc.). The FIU suspects that the VCs were used as means of payment on the website and to facilitate the fraud.

[23] Refer to https://www.bloomberg.com/news/articles/2017-09-11/north-korea-hackers-step-up-bitcoin-attacks-amid-rising-tensions.

Source: Cel voor Financiële Informatieverwerking – Cellule de Traitement des Informations Financières (CTIF-CFI) – Belgium

Case Study – Phone Scams & the Use of Wallet Providers (Singapore)

Person A was a victim of a phone scam and provided his internet banking credentials to the purported scammers. As a result, funds of SGD 22,700 were transferred from his account to an account belonging to Person B. Person B was also a victim of a phone scam. Similarly, she had provided her internet banking credentials to the scammers. On the same day, the fraudulent funds were transferred from Person B's account to an account belonging to Company C, which is a bitcoin wallet service provider. It is suspected that proceeds of crime from the scam were converted to Bitcoin.

Source: Suspicious Transaction Reporting Office (STRO) – Singapore

Case Study – Fraud & Bitcoin ATMs (Canada)

More than 40 individuals were defrauded in "tax revenue scams or CRA scams" involving Bitcoin ATMs in Ontario, Canada, sending more than CAD 300,000 to fraudsters. Victims were contacted by phone and told they had outstanding taxes to pay, and threatened with arrests. Victims were told to send their overdue taxes using Bitcoin ATMs. Other scams such as ads online with a promise to make money, job applications (e.g. job scams involving money mules) and bail amounts for a family member in distress have been flagged as fraudulent schemes involving Bitcoin ATMs by law enforcement in Canada.

Sources: York Regional Police (Canada), Durham Regional Police Service (Canada)

Organized Crime

Case Study – Fraudulent VCE, Tax Fraud & Organized Crime (Poland)

A notification was received under Article 16 of the Polish AML law connected with the transfer from the account of Company A (a Polish Limited Liability Company) to the account of Company B, for which the total amount was 18 million PLN Coin that included the conversion of these funds into EUR and attempts to transfer these funds to Dubai (approx. EUR 1.25 million was transferred).

The following day, the account of Company B received another 10 million PLN, which was also supposed to be transferred to Dubai.

The FIU received information from the police that the person ordering the transaction, Person A, is one of the two people possessing a power of attorney to the account of Company B, and is a member of an organized tax fraud group, which has been under investigation for several years.

The FIU submitted a query to Company A for a record of bitcoin wallet transaction of Company B. The analysis covered the over-threshold transactions (over EUR 15,000) from 2012 to May 2017 for the account of Person A, Person B and Person C, and companies related to these individuals. The numerous cash transactions (deposits and withdrawals) with high amounts have been reported along with transfers back and forth between personal and corporate accounts.

The analysis of over-threshold transactions determined that in 2015 and 2016, on behalf of Person B, the chairman of Company B, at least 17.3 million PLN worth of Bitcoins were purchased through other digital currency exchanges.

The income of Person B would not allow the purchase of such a large number of Bitcoins. During the previous few months, Person A's sister, Person C, received over 2.4 million PLN from Company A. In the same period, funds received from Company A, and other sources, have been allocated to the account of Company A (over 2.1 million PLN) in order to purchase Bitcoins.

Three months before the FIU took action, 2 million PLN and 2.9 million PLN were transferred to Company A from the account of Company C associated with Person C. One month before the FIU took action, 0.7 million PLN was returned to Company C from the account of Company A.

When the FIU took action to block the relevant bank accounts, a total of EUR 3 million (after notification under article 16 of the AML law) and 10 million PLN (via the FIUs own initiative) were blocked. A few days after blocking the accounts, the FIU received from Company A the answer to the earlier request.

The chairman of Company A pointed out that the funds of 18 million PLN, which had been blocked by the FIU, came from a Bitcoin loan agreement, where Company B was the borrower, and the aforementioned chairman, the lender.

The bank, which held the account of Company A determined that Person C used to previously run a company in the form of a civil partnership with Person D, Vice President of Company A. The bank concluded that Company A could have been set up specifically to allow the Organized Crime Group to allocate illicit money in Bitcoins. Ten (10) days after the accounts were blocked; the FIU received another notification under Article 16 of the Polish AML law.

The account of Company D (for which, a few days earlier, Person A was appointed with a power of attorney to the account) received funds from Dubai totaling USD 370,000 and EUR 1.57 million. The initiator of the transaction was a company from Dubai – the beneficiary of transfers ordered by Company B (on behalf of which it was possible to transfer EUR 1.25 million abroad before these funds were blocked). These funds have also been blocked by the FIU.

Source: General Inspector of Financial Information (GIFI) – Poland

Case Study – Laundering Proceeds from Dark Web Drug Stores (Russia)

The Russian Ministry of Internal Affairs and FIU conducted an investigation on organised criminal groups selling drugs via the Dark Web. Customers could choose two ways to pay and transfer funds for their order either by an indicated e-wallet or to Bitcoin address. The majority of clients preferred using e-wallets instead of Bitcoins.

The financial scheme for drug stores was arranged and managed by a financier and his network. The ML network was only responsible for moving funds and had no links to drug trafficking. Numerous e-wallets and debit cards were registered in the names of front men.

This usually involved students who issued e-wallets and credit cards and sold them to members of ML network, not being aware of the criminal purpose of their further usage. Some e-wallets were used at the placement stage of the laundering process. Some e-wallets had a limit of 300 thousand USD while other e-wallets had a higher limit.

To simplify the ML process, the network's IT specialists developed a 'transit-panel' that had a user friendly interface and was accessible via the TOR browser. The transit panel automatically changed e-wallets that were used for drug payments and moved funds to another level of mixing e-wallets when the limit was reached. Digital money was automatically moved through a complex chain of different e-wallets.

Money from e-wallets was then transferred to debit cards and withdrawn in cash via ATMs. Withdrawals via ATMs were conducted by "cash coordinators" who had multiple debit cards at hand (all cards were issued to the names of "straw men"). After that, the cash was handed over to interested parties. In order to increase the complexity, proceeds were re-deposited on a new set of debit cards and transferred to the organizers of drug trafficking criminal groups (usually located abroad).

In other schemes funds from e-wallets were exchanged into Bitcoins via virtual currency exchangers. The Bitcoins were used to pay salaries to members of the drug trafficking organisation. This included low-level members such as small dealers and runners who facilitated the sale of drugs. The same financier worked with multiple owners of the Dark Web stores, distributing the laundered funds to the respective OCGs.

Source: Rosfinmonitoring – Russian Federation

Terrorist Financing

FIUs reported few instances of the use of virtual currencies for terrorist activity financing. The main linkages between virtual currencies and terrorist activity financing is the use of Bitcoin to disguise the destination of funding by converting and transferring funds, or transactions in virtual currencies in conjunction with other suspicious activity. This includes payments to a charity believed to be associated to a terrorist group.

It remains difficult for FIUs to establish with certainty that virtual currencies are being used to directly fund terrorist activities.

Case Study – Suspicion of Terrorist Activity Financing Using VCs (United Kingdom)

[Example of a report made with suspicions of TF]

Suspicion surrounds third party cash and faster payment funding into a low interest bearing current account. This is held by an unemployed UK national who has previously been reported by Bank A under the Terrorism Act.

The funding cannot be attributed to a legitimate income and suspicion is heightened by the fact that the majority of the funds have been paid away to a Bitcoin company. Consequently it is suspected that the account has been used to launder, convert and transfer the proceeds of criminal activity.

Source: National Crime Agency – United Kingdom

Suspicious Transactions and Activity Involving Virtual Currencies Exchanges

Case Study – VCE Trends & Activity (Japan)

Client A // Conducts frequent cash deposits through branch ATMs located in large metropolitan areas. Then the money is transmitted to entities related to virtual currency exchanges and the like.

Client B // The entire amount of recent incoming transfers from entities related to virtual currency exchanges was withdrawn in cash. In the same time period, persons presumably related to Client B withdrew large sums of money credited as incoming transfers in cash from other branches located in a large metropolitan area.

Withdrawal of money from incoming transfers from entities related to virtual currency exchanges in the form of cash or cheques continues. Client B is young in age (20s) and the amount involved is considerably large compared to customers in the same age segment.

Client C // Client C is a trader in virtual currency who remits money to a virtual currency exchange related entity based in the U.S. Remittance is very frequent and amounts to a significant sum. Client C is young in age (20s), and the amount involved is considerably large compared to customers in the same age segment.

Source: The Bank of Tokyo Mitsubishi UFJ – Japan

Suspicion of Money Mule Account Activity Involving Virtual Currencies

Case Study – Money Mule & Bitcoin Exchanges (New Zealand)

In a fraud scheme, victims (or mules) are instructed to deposit funds to the accounts of New Zealand Bitcoin exchanges along with an address for an anonymous wallet (held by the offender) to which the Bitcoin value is then credited. The funds are converted to Bitcoin and credit to this anonymous wallet.

Source: New Zealand Police Financial Intelligence Unit – New Zealand

Unlicensed & Unregulated Virtual Currency Activity

Case Study – Bitcoin ATM & Unlicensed Virtual Currency Exchange Activity (Belgium)

In 2016, a Belgian citizen bought an existing company and moved its headquarters. The company's corporate goals consisted of buying and selling bitcoins via wire transfers and bitcoin ATMs.

In 2016, cash deposits for more than EUR 360,000 took place on the company's bank account (much more than EUR 70,000 in 2015). Wire transfers for EUR 70,000 were also credited to the bank account. Most of funds were subsequently transferred to a VC exchange platform.

The owner and director of the company explained that the funds came from bitcoin ATMs installed in Belgium.

The origin of the cash was unclear and the risks of ML or TF important even though the company voluntarily adopted AML/CFT internal procedures and imposed cash limits for deposits at the Bitcoin ATMs. The company is not subject to the Belgian AML/CFT framework and has no obligation to implement strong preventive measures, has no reporting obligations and is not supervised by supervisory authorities.

As the activities of the exchange platforms are in Belgium forbidden, illegal underground platforms developed.

Source: Cel voor Financiële Informatieverwerking – Cellule de Traitement des Informations Financières (CTIF-CFI) – Belgium

5. FIU Operational Perspectives on Virtual Currencies

Suspicious Transaction and Activity Reporting

From an operational perspective, contributing member FIUs estimate that they will continue to receive an increasing number of suspicious activity or transaction reports (or their equivalent) related to virtual currencies. FIUs also indicated there has been a sharp increase in reporting related to cryptocurrencies, particularly with regard to transactions and activities involving Bitcoin. One FIU reported that for some of the predicate offences it identified in its analysis, VCEs regulated in its jurisdiction submitted STRs/SARs by request from law enforcement. Another FIU indicated an increase of 243% per year of SARs reported on Bitcoin ATMs between 2013 and 2017.

One FIU reported that transaction records of unregistered vendors or exchanges in its jurisdiction were a great source of information, and that these entities were often reported by their banks due to the suspicious activity on their accounts.

Overview of Identified Risks

Contributing member FIUs have identified multiple methods and mechanisms involving virtual currencies that pose risks and that are often combined with other illicit activities to launder proceeds of crime. Certain attributes of virtual currencies (e.g., anonymity) and mechanisms to conduct transactions involving virtual currencies (e.g., VCEs and virtual currency ATMs) allow individuals to circumvent the traditional financial system, obfuscate the origin or destination of funds, and avoid the scrutiny of reporting entities.

Here are some of the main risks identified by the contributing member FIUs:

- The role of virtual currencies in laundering the proceeds of crime (e.g., fraud schemes, ransomware, drug sales)
- The role of virtual currencies for purchasing or selling illicit goods/services from Darknet marketplaces
- Darknet marketplace transactions being extremely difficult for law enforcement to trace
- Anonymous virtual currency wallets (e.g., Bitcoin wallets) being difficult to trace back to a user, especially when they are used in conjunction with other anonymizing tools
- The use of third-party ATM cash deposits to purchase virtual currencies, since reporting entities are not able to identify the depositors/source of funds
- The use of Bitcoin ATMs has increased significantly due to users' desire to remain anonymous and due to the fact that VC ATMs/BTMs collect little or no personal data on customers
- The gap in regulation and the lack of tools to mitigate the risks associated with virtual currencies are challenges
- Entities offerings virtual currency exchange services, and VCEs being linked with suspicious activities and/or transactions
- The main criminal uses of virtual currencies being for Darknet/Dark Web activities (illicit substance trade or purchase, and cybercrime)

- Vendors or VCEs working without registration, typically with customers having an interest in avoiding KYC requirements

Concerns and Gaps Identified by FIUs

FIUs raised a number of concerns about virtual currencies and virtual currency-related business activities, including the following:

- Reporting of transactional information is inconsistent due to there being no standardized reports to allow for the reporting of virtual currency transactions
- Reporting of transactional information involving Bitcoin but no other suspicious activity is still happening, since reporting entities are still trying to understand the implications of virtual currencies and the KYC requirements
- It is difficult to establish a transactional amount of money laundered through virtual currencies in SAR/STR/SMR reporting, since the values reported are recorded in traditional currency. In addition, the value of the virtual currency fluctuates daily, so the value at the time of reporting needs to be established to estimate the losses associated with potential crime and/or money laundering offences
- A shift away from Bitcoin to AECs would considerably limit FIUs ability to identify and investigate financial crime involving virtual currencies, as no techniques have yet been developed to identify AECs counterparties or to track transactions
- Capacity building is needed for FIUs who do not yet receive reporting on suspicious transactions and activities related to virtual currencies, or who have only recently been exposed to virtual currencies and the risks certain activities may present
- The importance of building a good working relationship between FIUs, virtual currency exchanges, reporting entities and law enforcement agencies for greater information sharing, since VCEs are unregulated in most jurisdictions
- Reporting entities need to be informed of the types of virtual currency use that are of interest to law enforcement agencies and FIUs (versus normal use of virtual currency), in order to make reporting more accurate
- There is a risk that virtual currency exchange businesses and natural persons, with poor or non-existent preventive AML/CFT measures and non-existent AML/CFT supervision, could be used by criminals to launder cash proceeds of criminal activities

Disclosures to Law Enforcement Agencies

A number of contributing FIUs have disclosed analytical cases to the office of the public prosecutor or other law enforcement agencies in their respective jurisdiction. In some instances, arrests were made but no cases are currently before the courts and no conviction have been made. In one instance, two (2) cases were sent to law enforcement, but criminal proceedings were not pursued.

One FIU has worked on six (6) law enforcement cases linking Bitcoin ATMs to potential illicit activity (the analysis was conducted over 637 SARs and outlined the following activities: drug dealers, credit card fraud rings, prostitution rings, and unlicensed peer-to-peer exchanges).

Best Practices

The following are some of the best practices FIUs proposed to mitigate the risks of virtual currencies and virtual currency related business activities:

- Public-private partnerships to assess the ML/TF risks related to new technologies or new payment instruments and their impacts on the stability of the financial systems
- Public-private partnerships in the field of cybercrime (the use of cyber experts to investigate financial transactions in virtual currencies)
- Increased and effective international cooperation between law enforcement authorities and between FIUs
- Increased cross-border dissemination of suspicious transaction activity involving multiple jurisdictions or implementation of matching technologies between FIU databases (e.g., Mat³ch technology developed by FIU-NET, where the 'Cross-Match' function can compare entire databases and find common names)

Regulation

The majority of jurisdictions do not currently regulate virtual currencies and virtual currency exchanges, with many choosing simply to not regulate or enforce existing legislation. This lack of regulation has created challenges for reporting entities with regard to their capacity to share information with FIUs. By extension, this hinders the ability of law enforcement agencies to conduct investigations regarding illicit activity involving virtual currencies or VCEs. Likewise with ICO's, most jurisdictions have simply issued warnings on the risks associated with participating in offerings, but have yet to enforce any regulations.

One FIU, which regulates virtual currency ATMs (due to their MSB-like activity), has signaled that most kiosk operators have registered with the FIU, but many do not have robust checks against suspicious activity, and that many of them do not file STR/SAR reports.

Appendix 2 provides an overview of the current state of regulation of virtual currencies, VCEs and ICOs.

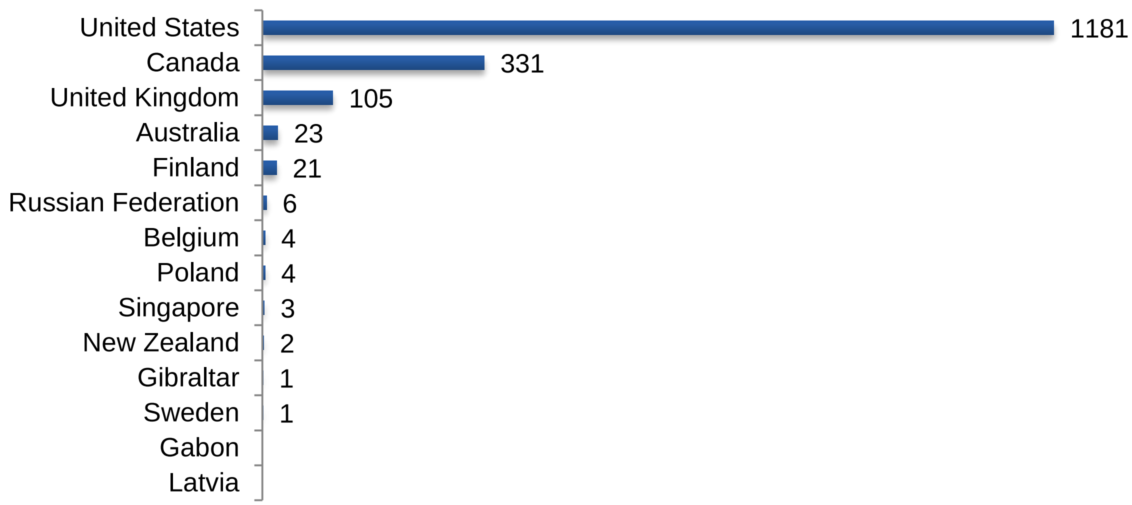
Looking Ahead – Issues for Discussion and Consideration

Based on the analysis of the submissions of the member FIUs and the various case studies, there are number of issues that FATF and the Egmont Group could focus their attention:

- Cryptocurrency mining activity for illicit gains, particularly cryptojacking
- Use of cryptocurrency to purchase real estate
- Financial instruments used by cybercriminals and the role of virtual currencies in laundering proceeds of illicit activities
- Expansion of the availability of goods and services that can be purchased by virtual currencies (integration phase of money laundering)
- Use of credit or debit cards in cryptocurrency funds, linked to cryptocurrency wallets or commodities and associated risks
- Virtual currency ATMs and kiosk operators that remain unregistered or intentionally do not properly identify their business to avoid regulation or compliance requirements

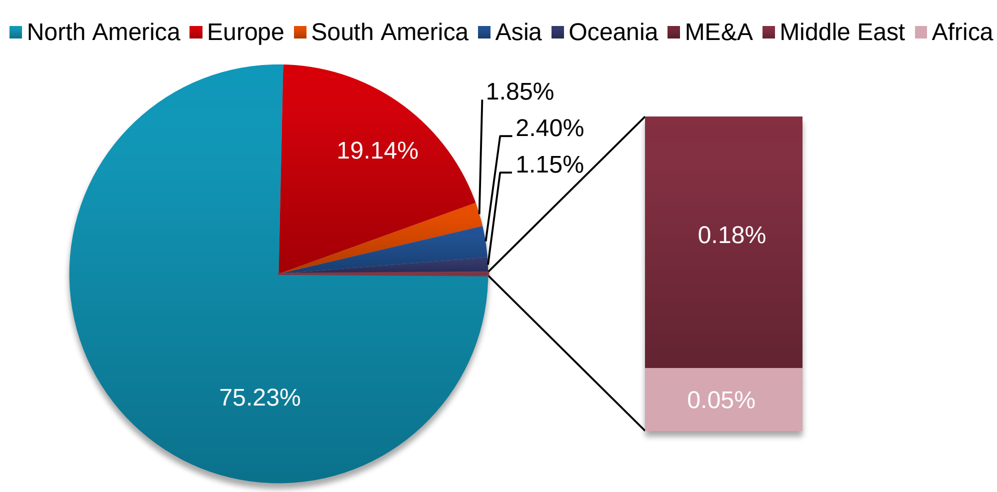
Appendix 1

Virtual Currency ATMs and Tellers by Jurisdiction of Contributing Member FIU



Source: as of January 5, 2018. Based on data from www.coinatmradar.com

ATMs and Tellers Installations by Continent (2018)



Source: as of January 5, 2018. Based on data from www.coinatmradar.com

The figure above shows the share of Bitcoin ATMs and Tellers by continent. The majority of installations are located in North America (1,631) and Europe (415), followed by Asia (52), South America (40), Oceania (25), and the Middle East (4) and Africa (1). Not included in the figure are more than 40,000 Bitcoin-to-cash and cash-to-Bitcoin service providers (e.g., 24nonStop, Flexepin Canada, PolandHalCash, Sweepay and Swiss Railways)[24].

[24] Refer to https://coinatmradar.com/manufacturers/#cash-services.

Appendix 2[25]

Regulation of Virtual Currencies: Review by Jurisdiction

Country	Status of Regulation
Australia	Regulated. In December 2017, Parliament passed legislation to expand the AML/CTF Act to include regulation of digital currency exchange providers. Under the legislation, virtual currency exchange providers will be required to register with AUSTRAC and comply with the following obligations: - perform customer identification and due diligence; - adopt and maintain an AML/CTF program, which includes requirements to identify, manage and mitigate money laundering and terrorism financing (ML/TF) risk; - perform suspicious matter reporting; - report threshold transactions (AUD10,000 and above); and - meet record-keeping requirements.
Belgium	Currently unregulated. Even though the Belgian Minister of Finance is willing to regulate virtual currencies and virtual currency exchange platforms, virtual currencies and virtual currency exchange platforms have, for the time being, no legal basis in Belgium and are consequently not regulated nor supervised.
Canada	Currently unregulated. On June 19, 2014, the *Economic Action Plan 2014 Act, No. 1*, received Royal Assent. The Act contained changes to the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA) that will entail new requirements for money services businesses (MSBs) dealing in virtual currencies. The changes will come into force once regulations are published in the *Canada Gazette*.
Finland	Currently unregulated. Virtual currency is currently treated as a commodity.
Gibraltar	Regulated. A bill was introduced in December 2017 (*The Distributed Technology Regulatory Framework*) to amend the *Financial Services (Investment and Fiduciary Services) Act* to protect customers of cryptocurrency businesses.
Japan	Regulated. In March 2016, Japan introduced a bill to amend the *Payment Services Act* to include virtual currency as a type of payment instrument. AML compliances are mandatory. In addition, there would be additional consumer protection and higher requirements for Japanese payment institutions.
Latvia	Currently unregulated. Virtual currency businesses are not listed as reporting entities pursuant to the AML/CFT Law of Latvia, and are not required to report to any other agency.

[25] The review of regulation is by jurisdiction of contributing member FIUs.

Country	Status of Regulation
	Section 3 *Subjects of the Law*, in Part 4 of the AML/CFT Law provides the following: *In order to prevent activities related to money laundering an terrorism financing, also the persons not indicated in Paragraph one of this Section, as well as State authorities, derived public persons and their authorities, have an obligation to comply with the requirements of this Law in respect of provision of information regarding unusual or suspicious transactions. Legal protection mechanisms, intended for the subjects of the Law shall be applied to the persons referred to in this Paragraph.*
Luxembourg	Currently regulated. VC exchange companies[26] are regulated as payment institutions. The AML/FT applicable regulation (Law of 12 November 2014) requires VCEs to file STRs and respond to requests from the FIU.
New Zealand	Currently unregulated. The Reserve Bank of New Zealand Act prohibits the issuance of banknotes and coins by any party other than the Reserve Bank.
Poland	Currently unregulated. However, there is the project underway to develop a new AML/CTF law that includes the proposal of legal definition of virtual currency and indicates entities offering services in the field of virtual currency exchange and custodian wallet providers as obliged institutions.
Russian Federation	Currently unregulated. The Finance Ministry is currently working on regulations, the Digital Assets Regulations, to regulate cryptocurrency transactions without a full ban or legalization of virtual currency as a method of payment in Russia. The Ministry of Finance also plans to introduce a law that will criminalize the use of cryptocurrencies as money substitutes.
Singapore	Currently unregulated. The Monetary Authority of Singapore (MAS) intends to regulate virtual currency intermediaries for AML/CFT and is currently reviewing legislation that would allow it to do so.
Sweden	Regulated. Virtual currency was treated as a currency by the Swedish Tax Board. The decision was appealed by the Swedish Tax Authority.
United Kingdom	Currently unregulated. Companies with e-money licences are subject to anti-money laundering regulations. An e-money licence is not a regulation of virtual currencies. Rather, it is a regulation on businesses that use platforms in currency, such as pre-paid cards, with which a customer purchases a value in e-money that they can spend.
United States	Regulated. Money services businesses (MSBs) handling virtual currencies are expected

[26] The first regulated VCE was Bitstamp (2016) followed by bitFlyer (2018).

Country	Status of Regulation
	to meet regulatory obligations under the Bank Secrecy Act (BSA). Kiosk operators (operating kiosks or Bitcoin ATMs) fall under FinCEN MSB registration requirements and require developed anti-money laundering policies. Kiosks require varying degrees of KYC information depending on the operator and operator-determined thresholds. Most Bitcoin kiosk operators limit daily per person transaction volumes to under $10,000 and maintain varying layers of identity verification for amount ranges. For example, a Bitcoin kiosk operator with locations mainly in New York City requires all users to complete text-based two-factor authentication for transactions up to $800. For amounts over $800, the operator requires the customer to take a photo through the machine, in addition to providing a government issued identity card.
European Union	Currently unregulated. The EU would like to end anonymity for cryptocurrency traders, citing anti-money laundering and tax evasion crackdowns. In the 5th AML/CFT Directive, the European Commission and the European Parliament included new requirements on the regulation and submission of virtual currency exchange platforms and providers of virtual currency wallets to the AML/CFT framework.

Regulation of Virtual Currency Businesses (e.g. Virtual Currency Exchanges, Tumblers and Mixers): Review by Jurisdiction

Country	Status of Regulation
Australia	Regulated. In December 2017, Parliament passed legislation to expand the AML/CTF Act to include regulation of digital currency exchange providers. Under the legislation, virtual currency exchange providers will be required to register with AUSTRAC and comply with the following obligations: - perform customer identification and due diligence; - adopt and maintain an AML/CTF program, which includes requirements to identify, manage and mitigate money laundering and terrorism financing (ML/TF) risk; - perform suspicious matter reporting; - report threshold transactions (AUD10,000 and above); and meet record-keeping requirements.
Belgium	Currently unregulated. Even though the Belgian Minister of Finance is willing to regulate virtual currencies and virtual currency exchange platforms, virtual currencies and virtual currency exchange platforms have, for the time being, no legal basis in Belgium and are consequently not regulated nor supervised.
Canada	Currently unregulated. On June 19, 2014, the *Economic Action Plan 2014 Act, No. 1*, received Royal Assent. The Act contained changes to the *Proceeds of Crime (Money*

Country	Status of Regulation
	Laundering) and Terrorist Financing Act (PCMLTFA) that will entail new requirements for money services businesses (MSBs) dealing in virtual currencies. The changes will come into force once regulations are published in the *Canada Gazette*.
Finland	Currently unregulated. Refer to European Union.
Gibraltar	Regulated. Since January 2018, the *Distributed Ledger Technology (DLT) Regulatory Framework* has regulated activities of firms that use DLT to store or transmit value belonging to others, such as virtual currency exchanges. In May 2017, the Gibraltar Financial Services Commission proposed to the Minister for Commerce to be the agency to supervise virtual currency transactions done through DLT, for the safeguard and integrity of the economy.
Japan	Regulated. As of October 2017, the Financial Services Agency placed all virtual currency exchanges under full surveillance. If necessary, the agency will conduct on-site examinations of the exchanges.
Latvia	Currently unregulated. Virtual currency businesses are not listed as reporting entities pursuant to the AML/CFT Law of Latvia, and are not required to report to any other agency. Section 3 *Subjects of the Law*, Part 4 of the AML/CFT Law provides the following: *In order to prevent activities related to money laundering an terrorism financing, also the persons not indicated in Paragraph one of this Section, as well as State authorities, derived public persons and their authorities, have an obligation to comply with the requirements of this Law in respect of provision of information regarding unusual or suspicious transactions. Legal protection mechanisms, intended for the subjects of the Law shall be applied to the persons referred to in this Paragraph.*
Luxembourg	Currently regulated. VC exchange companies[27] are regulated as payment institutions. The AML/FT applicable regulation (Law of 12 November 2014) requires VCEs to file STRs and respond to requests from the FIU.
New Zealand	Currently unregulated. In New Zealand, digital currency exchange businesses are not explicitly subject to the AML/CFT Act. Nonetheless, suspicious transactions involving purchases or sales of digital currency appear to be subject to AML/CFT controls.
Poland	Currently unregulated. However, there is the project under way to develop a new AML/CTF law that includes the proposal of legal definition of virtual currency as well as indicates entities offering services in the field of virtual currency exchange and

[27] The first regulated VCE was Bitstamp (2016) followed by bitFlyer (2018).

Country	Status of Regulation
	custodian wallet providers as obliged institutions.
Russian Federation	Currently unregulated. A Digital Assets Regulation draft bill which sets guidelines for cryptocurrencies use in Russia would require cryptocurrency exchanges to comply with KYC requirements and only licensed operators would be allowed to exchange cryptocurrencies into Russian rubles.
Singapore	Currently unregulated. The Monetary Authority of Singapore (MAS) intends to regulate virtual currency intermediaries for AML/CFT and is currently reviewing legislation that will allow it to do so.
Sweden	Regulated. Virtual currency exchangers or venders are required to register with Finansinspektionen, Sweden's financial supervisory authority (i.e., they do not require authorization). They are obliged entities. Tumblers and mixers are not specifically regulated. Considering the purpose of mixers and tumblers (i.e. to disguise the origin of an asset), anyone using or operating them could potentially face money laundering charges. However, no such cases have been processed yet.
United Kingdom	Currently unregulated. May be subject to other regulation. Companies with e-money licences are subject to anti-money laundering regulations. An e-money license is not a regulation of virtual currencies. Rather, it is a regulation on businesses that use platforms in currency, such as pre-paid cards with which customers purchase a value in e-money that they can spend.
United States	Regulated. Money services businesses (MSBs) handling virtual currencies are expected to meet regulatory obligations under the Bank Secrecy Act (BSA). Kiosk operators (operating kiosks or Bitcoin ATMs) fall under FinCEN MSB registration requirements and require developed anti-money laundering policies. Kiosks require varying degrees of KYC information depending on the operator and operator-determined thresholds. Most Bitcoin kiosk operators limit daily per person transaction volumes to under $10,000 and maintain varying layers of identity verification for amount ranges. For example, a Bitcoin kiosk operator with locations mainly in New York City requires all users to complete text-based two-factor authentication for transactions up to $800. For amounts over $800, the operator requires the customer to take a photo through the machine, in addition to providing a government issued identity card.
European Union	The amendment proposed in 2016 states the following: *In respect of designing providers of exchange services between virtual currencies and fiat currencies as obliged entities, the proposed amendments respect the proportionality principle. In order to allow competent authorities to monitor suspicious transactions with virtual currencies, while preserving the innovative advances offered by such currencies, it is appropriate to define as*

Country	Status of Regulation
	obliged entities under the 4AMLD all gatekeepers that control access to virtual currencies, in particular exchange platforms and wallet providers VCEs are not obliged to file STRs at the current moment, however this amendment seeks to impose that to further their fight against ML/TF, in particular France and Germany. In the 5th AML/CFT Directive, the European Commission and the European Parliament included new requirements on the regulation and submission of virtual currency exchange platforms and providers of virtual currency wallets to the AML/CFT framework.

Regulation of ICOs: Review by Jurisdiction

Country	Status of Regulation
Australia	The Australian Securities and Investment Commission (ASIC) released guidance (17-325MR) for ICOs and potential legal obligations, which requires ICOs, where applicable, to comply with the Corporations Act 2001 and other requirements. The government also issued draft laws and conducted a consultation process in regards to the establishment of an enhanced FinTech regulatory sandbox.
Belgium	The Financial Services and Markets Authority (FSMA) has issued a warning to consumers and offerors of ICOs, stating that ICOs may fall under European financial regulations, as determined by the European Securities and Markets Authority (ESMA) (ESMA50-157-828), as well as Belgian regulation such as FSMA Regulation of 3 April 2014, Law of 16 June 2006 and the Law of 18 December 2016.
Canada	The Canadian Securities Administrators (CSA) has determined that Securities laws will apply to cryptocurrency offerings on a case-by-case basis (CSA Staff Notice 46-307 Cryptocurrency Offerings), and also developed, the CSA Regulatory Sandbox, a “regulatory sandbox” for FinTech projects, including ICOs.
Finland	The Financial Supervisory Authority issued a warning on ICOs, labeling them as high-risk investments and outlined that European regulation may apply to ICOs as per the ESMA’s statement.
Gibraltar	Regulation effective from January 2018 (Distributed Ledger Technology Regulatory Framework) which enables creation of an ICO market (the GBX). The Gibraltar Financial Services Commission (GFSC) also published 9 principles for potential ICO licensees.
Japan	Investor warning issued by the Financial Services Agency, which also indicated that ICOs may fall under the scope of the Payment Services Act and/or he Financial Instruments and Exchange Act.
Latvia	Refer to European Union.
Luxembourg	The CSSF, the Commission de Surveillance du Secteur Financier, issued a warning statement (A ICOS 140318) on ICOs and tokens, indicating that ICOs are currently not required to comply with a specific regulation and that this type of investment is highly speculative. The CSSF also refers to the warnings issued by ESMA.
New Zealand	The Financial Markets Authority issued a statement (MR No. 2017 – 46) indicating entities operating in the ICO industry may have legal obligations, and may have to comply with the Financial Markets Conduct Act and register on the Financial Services Providers Register.
Poland	The Polish Financial Supervision Authority (KNF) issued a warning statement on

Country	Status of Regulation
	ITOs and ICOs, outlining that ICOs may be subject to legal requirements. The KNF also supports the ESMA's warnings and statements.
Russian Federation	The Ministry of Finance is preparing a bill that would permit the trade in cryptocurrencies through digital exchanges that meet certain requirements and as well, cover ICOs.
Singapore	The Monetary Authority of Singapore (MAS) published guidance on ICOs, defining the treatment of altcoins and ICOs under existing securities law (Securities and Futures Act). The MAS clarified its regulatory position in assessing how to regulate ICO/ITO activities in relation to ML/TF, in usage other than as virtual currencies.
Sweden	The Financial Supervisory Authority issued a warning on the risks associated with ICOs.
United Kingdom	The Financial Conduct Authority (FCA) issued a warning statement on ICOs indicating that while they are not regulated by the FCA, but some activities may fall within the regulated activities of relevant laws. The FCA is monitoring development in that front, and published a Feedback Statement on DLT.
United States	The SEC, the Security Exchange Commission, has issued a statement on cryptocurrencies and ICOs with regards to ICO or cryptocurrency investment opportunities and laying out guidelines as to if an ICO meets the requirements of a security.
European Union	ESMA has issued statements regarding the applications of various regulations in connection to ICOs, in particular compliance with the Prospectus Directive, the Markets in Financial Instruments Directive, the Alternative Investment Fund Manager Directive and the 4th Anti-Money Laundering Directive.