Financial Intelligence Unit

New Zealand Police

Quarterly Typology Report
First Quarter (Q1) FY2016-17

(1 July – 30 September)

CRYPTOCURRENCY

(Issued December 2016)

INTRODUCTION

This report is the first Quarterly Typology Report (QTR) of 2016/2017 produced by the Financial Intelligence Unit (FIU), part of the New Zealand Police Financial Crime Group. As the QTR dissemination goes beyond law enforcement, the basics of money laundering, typologies and indicators will continue to be included to provide context to those new to the topic. **A list of typologies is contained in Annex 1.** This publication is comprised of open source media reporting observed within the last quarter. **Readers are strongly advised to note the caveat below.**

- **The open source nature of the material that this document is based on means that the veracity of the reports within this document may vary**
- **Views expressed within this document may not necessarily be those of the New Zealand Police or of any of its employees**
- **Reports within this document have been précised; additional information can be obtained via the hyperlinks if available**
- **The information contained within this document should NOT be taken out of context**

BACKGROUND

The Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT) Act became law in October 2009. It is the result of a review of AML/CFT legislation and aims to assist in detecting and deterring money laundering, contributing to public confidence in the financial system and achieving compliance with the Financial Action Task Force (FATF) recommendations. The Financial Intelligence Unit produces the QTR as part of its obligations under section 142(b)(i)[1] and section 143(b)[2] of the AML/CFT Act 2009.

PURPOSE

The purpose of the QTR is to provide an accurate picture of current, emerging and longer term factors impacting on the AML/CFT environment. The QTR is intended to do the following:

- Examine money laundering and terrorist financing methods used in New Zealand and overseas
- Provide indicators of money laundering and terrorist financing techniques
- Highlight emerging trends and topics and share information in relation to AML/CFT and financial crime in general
- Provide typology case studies
- Update suspicious transaction reporting and Asset Recovery Unit activity

[1] Section 142(b) Financial intelligence functions of Commissioner: The financial functions of the Commissioner are to - produce guidance material, including: (i) typologies of money laundering and financing of terrorism transactions

[2] Section 143(b) Powers relating to financial intelligence functions of Commissioner: The Commissioner may - (b) share suspicious transaction reports, cash reports, suspicious property reports, and other financial information and intelligence with domestic and international authorities for the purposes of this Act and regulations

SCOPE

The QTR is a law enforcement document. However, it does not include sensitive reporting or restricted information and is published on the FIU website. The QTR is produced using a variety of sources and qualitative/quantitative data.

DEFINITION OF MONEY LAUNDERING

Under New Zealand legislation the money laundering offence is defined in section 243 of the Crimes Act 1961 and section 12b of the Misuse of Drugs Act 1975. The key elements of a money laundering offence are:

- Dealing with, or assisting in dealing with, any property for the purpose of concealing it
- Knowing or believing that such property is the proceeds of a serious offence, or being reckless as to whether it is the proceeds of a serious offence

DEFINITION OF TERRORIST FINANCING

Terrorist financing is criminalised in New Zealand under the Terrorism Suppression Act 2002. Under this legislation it is an offence to:

- Collect funds intended to be used for a terrorist act or intended for an entity known to carry out terrorist acts
- Knowingly deal with any property owned or controlled by a designated terrorist entity
- Make financial services available to a designated terrorist entity

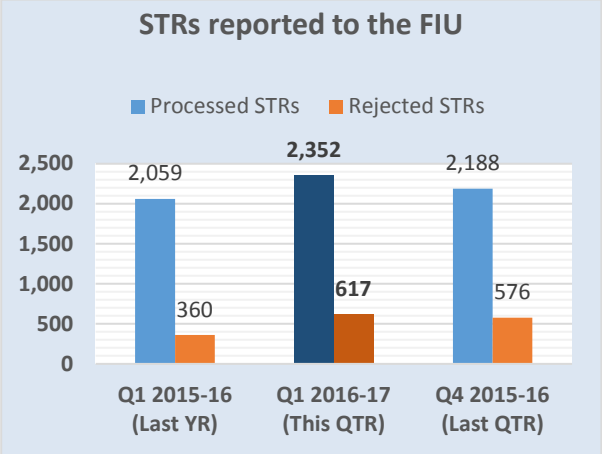
Financial Intelligence Unit updates

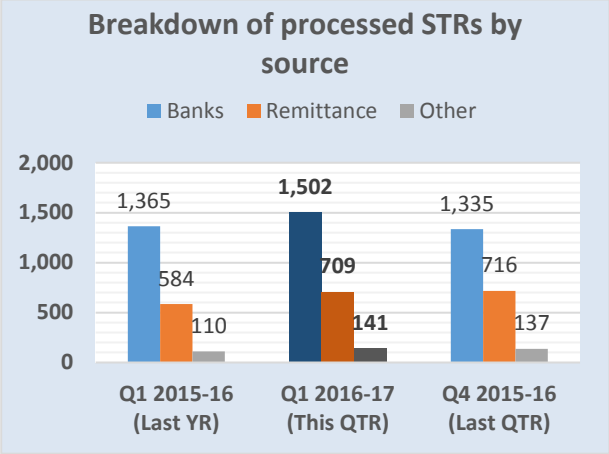
Information on the FIU is provided separately in permanent **Annex 2**.

SUSPICIOUS TRANSACTION REPORTING TO THE FIU

The number of reported suspicious transaction reports (STRs) processed by the FIU in Q1 2016-17 was **2,352**. This total is 164 reports more than in Q4 2015-16, and 293 (14 per cent) more compared to the same Q1 last financial year.

The number of rejected STRs continued to increase in Q1 2016-17 to **617** from 576 in previous quarter. Comparing to the same Q1 last financial year, the FIU rejected about 71 per cent more reports.





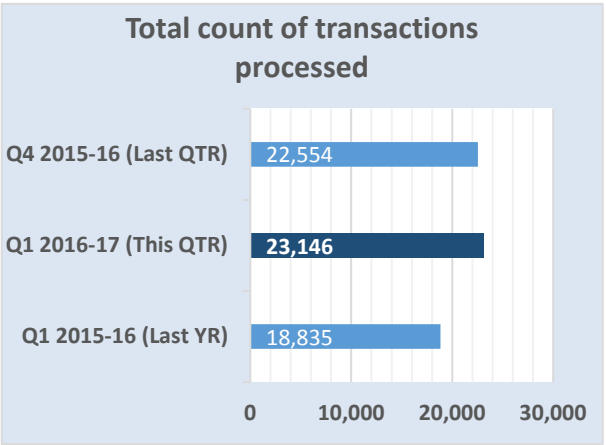
STR SUBMISSION BY SOURCE

The majority of STRs are submitted by banks and remittance service providers. The breakdown of the processed reports for Q1 2016-17 is similar to Q4 2015-16, but with a slightly greater proportion coming from banks versus remittance.

Comparing Q1 number of processed STRs received from money remitters with the same Q1 last financial year, there has been a 21 per cent increase.

TRANSACTIONS IN STRS

In Q1 2016-17, the number of transactions in accepted STRs was **23,146** and has increased by 592 transactions from Q4 2015-16, which is 23 per cent more than in the same Q1 last financial year.

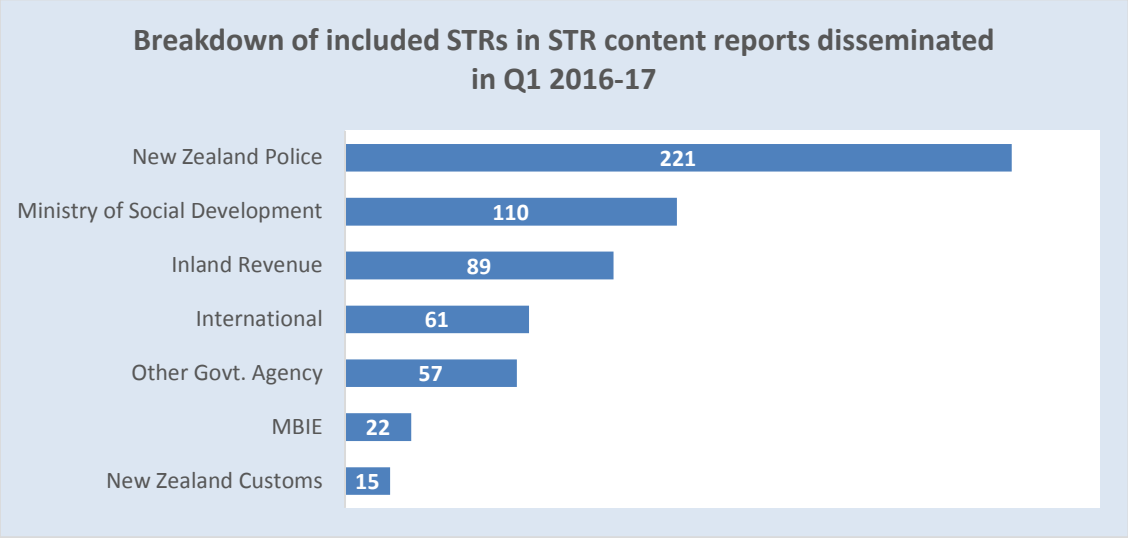


DISSEMINATION OF FIU INTELLIGENCE INFORMATION

The FIU collects and collates information provided by external parties and reporting entities, especially banks and other financial institutions. After the required analysis, intelligence products such as STR content reports, STR spreadsheets and intelligence reports are sent to other investigative and intelligence units within Police, sector supervisors, domestic partner agencies and to relevant international agencies.

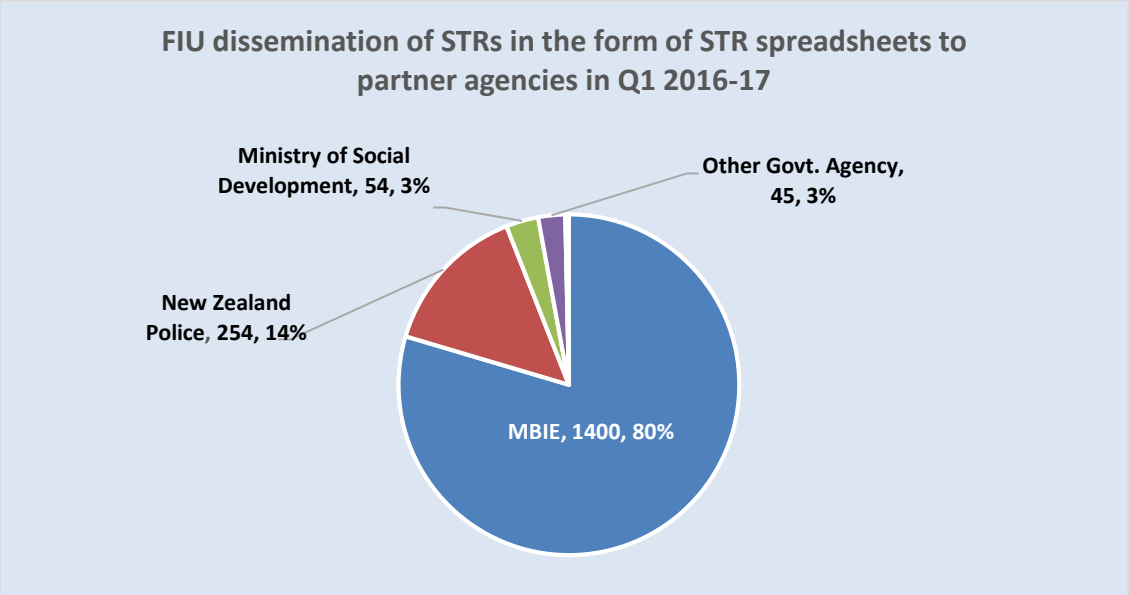
STR content reports are basic intelligence products that comprise of the reporting entities' grounds for suspicion, the reported transactions and biodata. Often the FIU will add additional value to the STR content report by including information held in Police intelligence systems. These STR content reports primarily contain data from the reported relevant STRs, and also border cash reports and suspicious property reports.

In Q1 2016-17, the FIU disseminated a total of **286** STR content reports, 36 per cent of which were sent to various New Zealand Police units. The other recipients included domestic and international law enforcement agencies. There were a total of **575** STRs included in these STR content reports for this quarter.

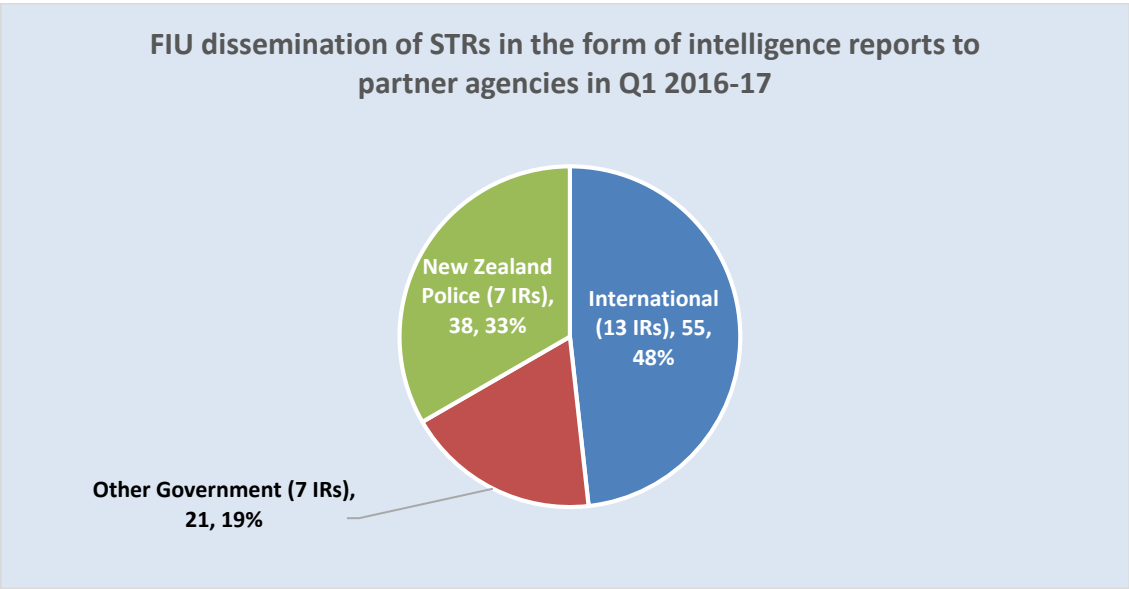


STR spreadsheets are collection documents for the detection, investigation and prosecution of offences by different prosecuting authorities within the New Zealand government. Once the collection phase is completed, the STRs are exported to a spreadsheet in their raw form. With the exception of the Police spreadsheets they do not have any added value from Police intelligence systems.

The FIU distributed **25** STR spreadsheets in Q1 2016-17 to six partner agencies, which included raw data of a total of **1,759** STRs.



Intelligence reports are produced by the FIU intelligence analysts and they involve a wide collection of data including information from the reported STRs. These reports contain data analysis of the STRs, drawn inferences and recommendations made to the intended recipient.



During Q1 2016-17, the FIU has produced **10** intelligence reports. For the same quarter, the FIU has conducted 27 intelligence report disseminations, which contained analysis of a total of **114** STRs.

The disseminated STRs indicated offences including **tax evasion**, **drug dealing**, **money laundering**, **fraud**, **theft**, **people smuggling**, **online child exploitation**, **customs offences**, **immigration offences** and **terrorist financing**.

Asset Recovery Units

The New Zealand Police Asset Recovery Units were established in December 2009 to coincide with the implementation of the Criminal Proceeds (Recovery) Act 2009 (CPRA). The CPRA established a regime for the forfeiture of property that has been directly or indirectly acquired or derived from significant criminal behaviour. It is intended to reduce the possibilities for individuals or groups to profit from criminal behaviour, to reduce the opportunities they have to expand their criminal enterprises, and act as a deterrent for criminal activity. There are four Asset Recovery Units (ARUs), based in Auckland, Hamilton, Wellington and Christchurch.

CRIMINAL PROCEEDS (RECOVERY) ACT 2009 (CPRA)

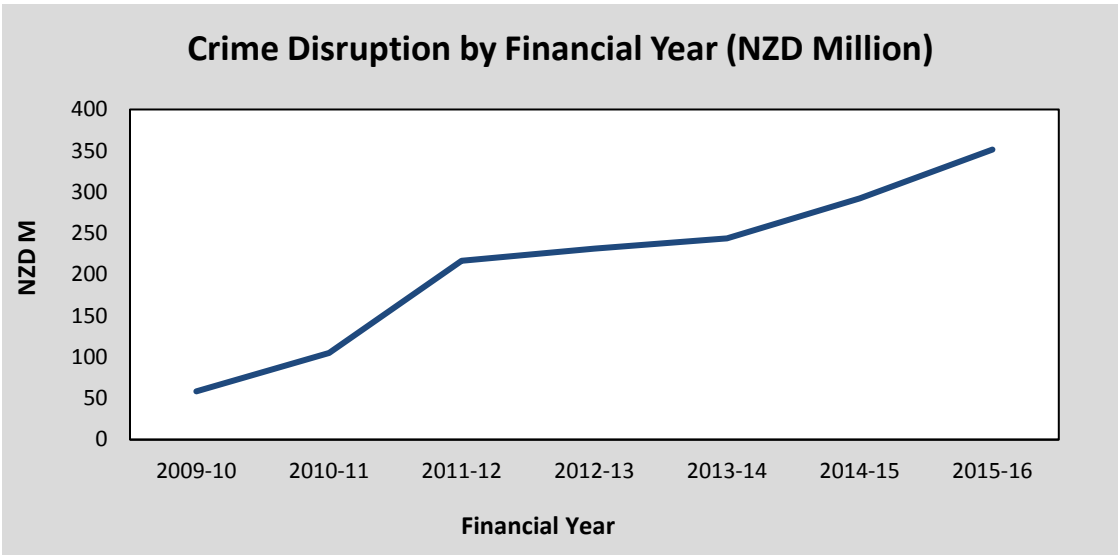
As at 30 September 2016, New Zealand Police held Restraining Orders at over an estimated **NZD229 million** worth of assets. Since CPRA came into effect, an estimated **NZD138 million** worth of assets have been subject to Forfeiture Orders. For the quarterly period ending September 2016, **NZD9.7 million** worth of assets were restrained, and **NZD47.8 million** were forfeited.

NZD Million	As at 30-Sep-16
Value of Forfeitures	**138**
Value of Restraints	**229**
Fraud, Money Laundering & Tax Evasion	92
Drugs & Other Offending	137

Note that these values are drawn from a dynamic database, where information about cases can be continuously updated.

CRIME DISRUPTION

According to the Proceeds of Crime Disruption Index (POCDI), every dollar worth of assets restrained contributes to an estimated NZD3.30 in crime disruption, and NZD3.50 for every dollar worth of assets forfeited. The below graph shows the estimated amount of crime disruption achieved since the CPRA was enacted, by financial year.



CRYPTOCURRENCY

WHAT IS CRYPTOCURRENCY?

The Financial Action Task Force (FATF)[3] in their report on Virtual Currencies published in June 2014 have defined cryptocurrency as

> ***"a math-based, decentralised convertible virtual currency that is protected by cryptography.—i.e., it incorporates principles of cryptography to implement a distributed, decentralised, secure information economy. Cryptocurrency relies on public and private keys to transfer value from one person (individual or entity) to another, and must be cryptographically signed each time it is transferred."***[4]

A cryptocurrency is difficult to counterfeit because of this security feature. Cryptocurrencies can take many forms, but typically, they represent a digital means of exchange not issued by any central authority. Such exchange uses cryptography and peer-to-peer (P2P) technology to regulate the creation of units and allow transactions to occur independently of a traditional middle-man such as a bank.

The anonymous nature of cryptocurrency transactions makes them well-suited for a host of unlawful and criminal activities, such as money laundering and tax evasion.

The first cryptocurrency was Bitcoin, which was launched in 2009 by an individual or group known under the pseudonym Satoshi Nakamoto. By far, Bitcoin is the largest cryptocurrency in terms of users and market capitalisation. As of September 2015, there were over 14.6 million bitcoins in circulation with a total market value of USD3.4 billion. Bitcoin's success has spawned a number of competing cryptocurrencies, such as Litecoin, Namecoin, Ripple and Trump.

A technician maintains Bitcoin mining rigs in a KnCMiner data centre[5]

[3] FATF is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction.

[4] FATF Report. Virtual Currencies – Key definitions and potential AML/CFT Risks. June 2014 http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf

[5] http://www.computerworld.com/article/3014509/data-center/bitcoin-miner-knc-is-planning-another-four-week-data-center-build-out.html

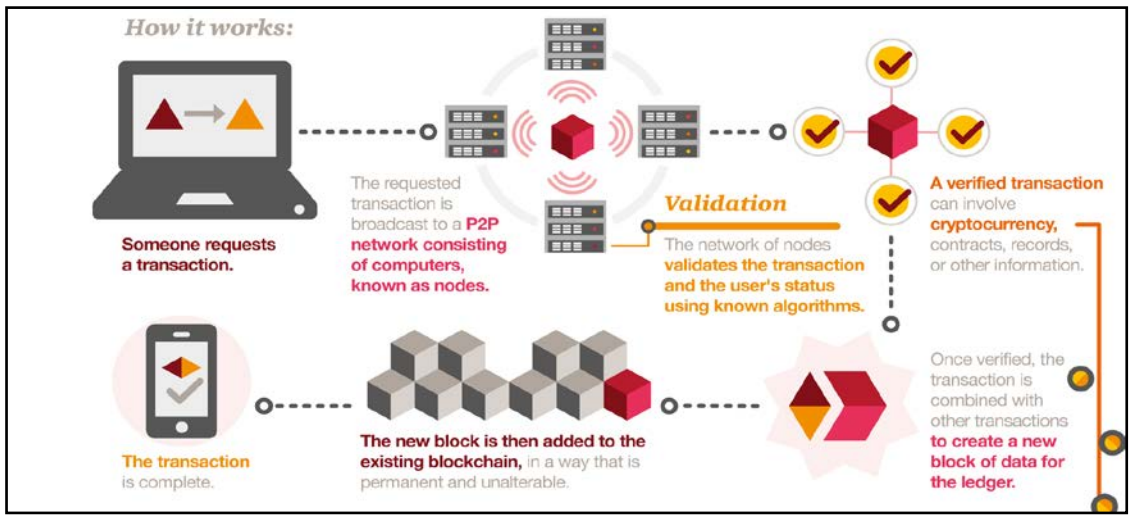
Cryptocurrency can be acquired a number of ways such as purchasing them, accepting them as payment for goods or services, or by 'mining' them. Legitimate purchasing of cryptocurrency is generally done through either an exchange, which generally takes the form of an open market – bringing together buyers and sellers, or a 'storefront' where a single person sells cryptocurrency at a fixed (though overall fluctuating) price. 'Mining', in the case of Bitcoin is both how new coins are generated, as well as providing a reward and incentive for maintaining the network that supports Bitcoin transaction processing.

HOW MANY DIFFERENT CRYPTOCURRENCIES ARE THERE?

In late November 2016, various online cryptocurrency markets, such as CoinMarketCap, CryptoCompare and CryptoTrader, were listing around 650 currencies.

Large multinational companies such as Amazon, PayPal, and Virgin Airlines now accept Bitcoins as payment – helping to establish it in the global commercial environment. In response to the growth, most OECD[6] countries have now provided some guidelines on cryptocurrencies. An additional report by FATF adds to the current understanding.[7]

WHAT IS BLOCKCHAIN?



Above diagram: Blockchain[8]

Blockchain is the underpinning technology behind cryptocurrencies. It provides a decentralised ledger or list of all transactions across a P2P network. New transactions are then gathered up into a group called a block. Each new block references the one before it, forming a chain. The chain is a permanent record where all transactions ever made can be traced.

[6] OECD – The Organisation for Economic Cooperation and Development http://www.oecd.org/

[7] FATF Report. Virtual Currencies – Key definitions and potential AML/CFT Risks. June 2014 http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf

[8] http://www.pwc.com/us/en/financial-services/fintech/bitcoin-blockchain-cryptocurrency.html

Blockchain is often referred to as a 'distributed ledger' because each of the blocks are validated by a large distributed group of users. The user-community's computers run automated software to reconcile the ledger by validating each and every block through a system that is like voting, where the majority rules. The public ledger is maintained by everyone, but not controlled by a central body or party.

To ensure the resilience of the system, Blockchain networks use a mix of encryption, robust mathematics, and majority-rules principles. These networks also have the potential to be used in a range of mainstream financial services, including:

- Real-time payments
- Cross-border settlements and foreign exchange
- Equities trading without a centralised exchange, where users can buy and sell shares in a company or derivatives through a P2P system

HOW ARE CRYPTOCURRENCIES USED?

Cryptocurrencies can be thought of as similar to 'online cash'. In order to use a cryptocurrency, a 'wallet' must be created. This operates much like a real wallet, being a place where cryptocurrency is held (after purchase), and disbursed (spent) from. However, there are varying degrees of security and access – depending on the wallet selected.

A cryptocurrency wallet is represented by a cryptographic key, one of two central to the distributed operation of any cryptocurrency. The cryptographic key, known as a 'public key' acts in a similar way to an email address for receiving cryptocurrency. When someone is to be paid, their public key is the location of where the funds are to be sent.

In addition to a public key, which is also known to the P2P network at large, a wallet also has an associated private key. This private key is required to authorise the sending of funds out of a wallet to another address. The private key essentially acts as a password.

While the protocol used and precise structure of transactions is complex and varies across different cryptocurrencies – in practical terms (with the correct software) funds can be sent and received online anywhere in the world in the same way as sending an email or, copying and pasting a web address.

Mobile Bitcoin wallet[9]

[9] https://www.wired.com/2014/07/blockchain-back/

VULNERABILITY TO MONEY LAUNDERING AND TERRORIST FINANCING

The dynamic nature of cryptocurrency development offers notable opportunities for criminals to exploit for the purpose of money laundering and terrorist financing the associated systems because:

- New payment technologies allow criminals to exploit developments that breakdown the barriers posed by international borders, or facilitate new anonymous means of payments between individuals
- New payment technologies can exacerbate vulnerabilities by circumventing, hampering or defeating AML/CFT controls – i.e. payments online allowing non-face-to-face transactions
- Technology, that can be accessed remotely to move funds quickly, allows reintegration of proceeds of crime back into the financial system
- New payment technologies increase anonymity by allowing more person-to-person transactions outside of the regulated financial sector and by placing a layer between individuals undertaking transactions and reporting entities
- The speed and convenience of new technology-enabled transactions, supports exploitation of the borderless nature of the Internet where there are difficulties regulating financial services that operate online
- Payment technology vulnerabilities include:
    - Open loop stored value instruments for use overseas
    - Online payment facilities offered by traditional financial sectors where the standard of AML/CFT compliance cannot be maintained
    - Online payment systems that facilitate P2P payments or obscure purchases of valuable assets from financial institutions
    - Remitters offering money transfers to countries that provide e-wallets on phones

REAL VALUE OF CRYPTOCURRENCIES – ANONYMITY

The technology behind cryptocurrencies allows users to transfer value across the Internet without the need for a third party administrator. Instead, an individual's key is used through a string of letters and numbers that acts as an identifier. Transactions are not anonymous but are pseudonymous – that is a transaction is created but identifying information is encrypted and no personal information is shared. Only the geographical origin or endpoint of the transaction is available.

Furthermore, particularly in relation to the challenges associated with AML, cryptocurrencies offer low cost international transactions; they remain unregulated, are largely untraceable, and are becoming increasingly accepted by merchants.

While it is difficult to find concrete evidence of cryptocurrencies used by terrorist groups and their supporters, strong evidence suggests the link to a number of terror attacks in Europe and Indonesia – because they mitigate some of the risks associated with traditional fund transfer methods.[10]

CRYPTOCURRENCIES IN NEW ZEALAND

A small number of domestic exchangers of digital currencies have been identified in New Zealand, including individuals who offer exchange services by selling digital currencies – namely Bitcoin bought from overseas exchanges. There have been a few exchange service providers established in New Zealand that provide the facility of P2P connector rather than an exchange per se (in the same way online auctions connect buyers and sellers that agree on a fixed price and transact with one another in person or online). A true exchange allows traders to 'bid' and 'ask' for trades at a predetermined level then when a bid matches an 'ask', the transaction proceeds.

New Zealand exchangers allow non-face-to-face purchases or sales of digital currencies online, and in the case of one exchanger, through Smart ATMs. The New Zealand FIU is also aware of criminals purchasing cryptocurrencies from overseas-based currency exchange businesses.

A small number of retailers in New Zealand are accepting Bitcoin as payment in their business. Retailers do this by receiving Bitcoin payments directly or via a Bitcoin payment merchant that receives the Bitcoins from the customer in exchange for depositing the NZD equivalent (less a small transaction fee) into the retailer's bank account.

Bitcoin Accepted sign at retailer storefront[11]

New Zealand Customs have intercepted over 500 packages coming into New Zealand that contained illegal items, paid for by Bitcoin.[12] These purchases were carried out via websites such as Silk Road, before it was shut down by the United States FBI.

Currently, Bitcoin is not regulated in New Zealand. The Reserve Bank of New Zealand Act prohibits the issuance of banknotes and coins by any party other than the Reserve Bank. However, the Reserve Bank

[10] The use of cryptocurrencies in funding violent jihad (2016) Journal of Money Laundering Control Vol. 19 No. 4,

[11] http://www.ebay.com/gds/100-Companies-That-Accept-Bitcoins-As-Payment-/10000000206483242/g.html

[12] http://www.stuff.co.nz/technology/digital-living/30008862/bitcoin-beauty-or-bubble

has no direct power over any form of alternative payments medium. Non-banks do not need Reserve Bank approval for schemes that involve the storage and/or transfer of value (such as Bitcoin) – so long as they do not involve the issuance of physical circulating currency (notes and coins).[13]

ONGOING RESEARCH IN NEW ZEALAND

Research, led by the University of Auckland Business School is underway in New Zealand on regulating new cryptocurrencies. The research, which is being carried out by the Law Foundation's NZD2 million Information Law and Policy Project (ILAPP) – titled "Regulating Digital Currencies that use Blockchain Technology" deals with one of the most game-changing and challenging technology innovations in the world of business and finance.

The aim of the research is to develop a legal framework for Blockchain regulation in New Zealand and Australia and to ensure the utmost balance between the interests of Blockchain stakeholders and the interests of regulators.[14]

OVERSEAS CASE STUDIES

- **AUSTRALIA**

In June 2016 Victorian Police, held a global auction to sell off AUD22 million worth of Bitcoins seized as the proceeds of an undisclosed crime. Richard Pollard plead guilty to commercial drug trafficking, and Fairfax Media reported at the time of his arrest that police found three electronic wallets in his possession containing 24,518 Bitcoins (equivalent to AUD22 million).[15]

- **THE NETHERLANDS**

In January 2016, 10 people were arrested in the Netherlands as part of an international investigation into money-laundering through sales of Bitcoin. The men, described in media as all in their 20s and with Dutch nationality, were suspected of using Bitcoin to launder up to EUR20 million of criminal money made from online drug deals at online marketplaces on the "Dark Web."

Fifteen places were raided, resulting in seizure of luxury cars, cash and the ingredients to make ecstasy, as well as bank accounts and bitcoin accounts. The alarm had been raised by banks which had seen "large sums of money" being deposited before being immediately withdrawn at cashpoints.[16]

- **SPAIN**

In early 2016, Spanish police arrested 30 people suspected of illegally distributing pay-TV content and of laundering the proceeds by investing in Bitcoin 'mining' centres for processing transactions in the digital currency, which use intensive computing power to generate more Bitcoins. Six Bitcoin 'mining' centres

[13] http://www.rbnz.govt.nz/faqs/notes-and-coins-faqs

[14] http://www.lawfoundation.org.nz/?p=7309

[15] http://mashable.com/2016/06/27/bitcoin-auction-australia/#K0oTSzjp_aqj

[16] https://www.theguardian.com/technology/2016/jan/20/bitcoin-netherlands-arrests-cars-cash-ecstasy

were seized in the raid with the proceeds allegedly laundered through investments in banking products, luxury cars, as well as property and Bitcoin centres.[17]

- **UNITED STATES**

Bitcoin advocate, early adopter and founding board member of the Bitcoin Foundation, Charlie Shrem was sentenced in December 2014 to two years in prison plus three years of supervised release by a U.S. District Judge. Shrem was arrested in January the same year — along with associate Robert Faiella – accused of selling over USD1 million in bitcoins in a money laundering scheme involving users of Silk Road, the Dark Web black market that was ultimately shut down.[18]

Shrem pleaded guilty to charges of aiding and abetting the operation of an unlicensed money transmitting business, while Faiella pleaded guilty to operating an unlicensed money transfer business. In entering his plea, Shrem told the court that for 11 months in 2012, his company, BitInstant, knowingly helped Faiella, to process Bitcoin that was then used to buy and sell drugs on Silk Road.

Shrem served his sentence at United States Penitentiary Lewisburg, a high-security prison in Pennsylvania and was released from prison in July 2016.

In another United States case, the creator of Silk Road, Ross William Ulbricht, also known as 'Dread Pirate Roberts,' was arrested in San Francisco in 2013 after the website was shut down. Prosecutors seized approximately USD3.6 million worth of Bitcoins in the largest ever seizure of the virtual currency. Ulbricht was sentenced to life in prison in February 2015.[19]

The FBI said the "Silk Road website has served as a sprawling black market bazaar where illegal drugs and other illicit goods and services have been regularly bought and sold by the site's users," The FBI noted that the addition of a Bitcoin "tumbler" to the Silk Road payment system had foiled efforts to trace digital currency back to buyers.

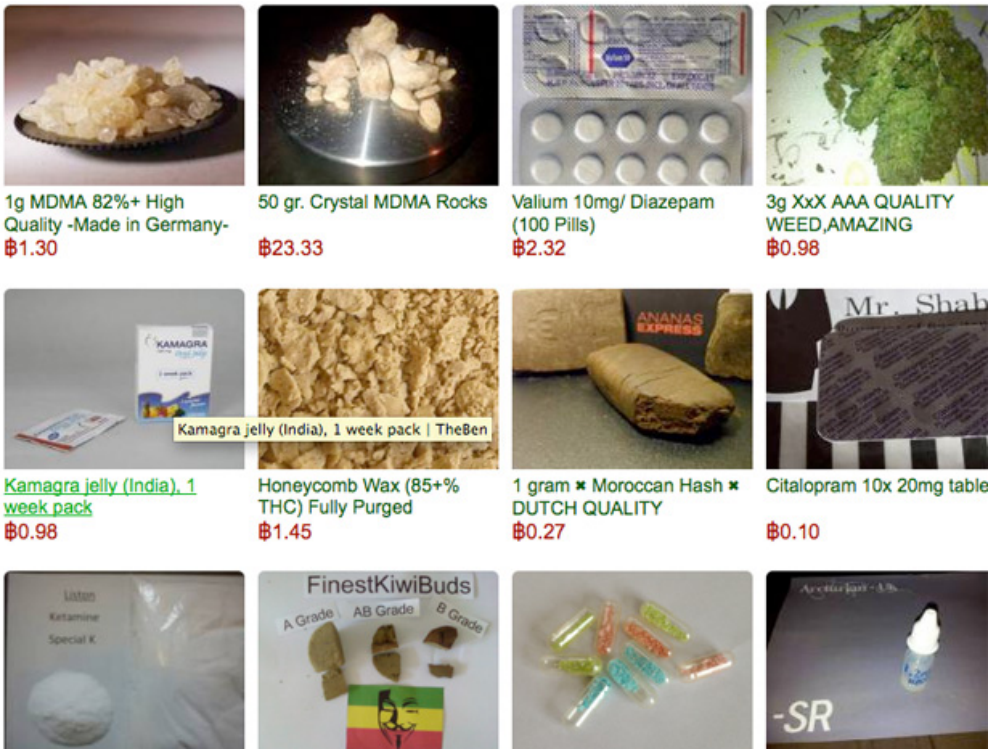
After the down fall of Silk Road, in March 2015, the investigation into Ulbricht revealed huge deposits into the bank accounts of Tomáš Jiříkovský and his family members. These deposits combined with his recent expenses worth over USD800,000 led to the identification and subsequent arrest. The assets of 28-year-old Czech national Jiříkovský were seized. He was suspected of laundering USD40 million in stolen Bitcoins. As of August 2016, Jiřikovský was facing up to 12 years in prison for enabling drug trade and stealing Bitcoin. His wife is also being charged with money laundering and if convicted, she may face 8 years of jail time.[20]

[17] http://www.businessinsider.com/r-spain-arrests-30-suspected-of-laundering-money-in-bitcoin-centers-2016-5?IR=T

[18] https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-charges-against-bitcoin-exchangers-including-ceo

[19] http://www.cnbc.com/2015/05/29/silk-road-creator-ulbricht-sentenced-to-life-in-prison.html

[20] http://www.newsbtc.com/2016/08/28/deep-web-busts-theft-recovery-btc/



Silk Road screenshot[21]

Following the Shrem, Ulbricht and Jiříkovský cases, two more subjects were detained in September 2015: 33-year-old American Trendon Shavers pleaded guilty to running a USD150 million Ponzi scheme – the first Bitcoin securities fraud case – and 30-year-old Frenchman Mark Karpelès was arrested and charged with fraud and embezzlement of USD390 million from the collapsed Bitcoin currency exchange MtGox.

The Shavers case goes back to 2011 when the 33-year-old McKinney, Texas native started his own company, Bitcoin Savings & Trust, and used it to collect bitcoins from prospective investors over the internet, claiming he would pay investors 1 per cent interest on their investment every three days, or 7 per cent a week. Instead, Shavers used most of the bitcoins to pay back older investors – a hallmark of a Ponzi scheme – while spending the rest on a used BMW M5, a USD1,000 Las Vegas steakhouse dinner, and a series of casino outings. Shavers pleaded guilty in Manhattan court to one charge of securities fraud in what is considered the first ever US criminal fraud case related to bitcoin.[22]

Mark Karpelès, who was the head of the collapsed MtGox Bitcoin exchange at the time of his arrest, was investigated by Japanese police over the disappearance of about USD390 million worth of the virtual currency. MtGox, which once boasted of handling about 80 per cent of global Bitcoin transactions, filed for bankruptcy protection soon after the cyber-money went missing, admitting it had lost 850,000 coins

[21] http://www.businessinsider.com.au/silk-road-walkthrough-2013-10#using-a-tor-browser-you-would-have-accessed-silk-road-at-httpsilkroadvb5piz3ronion--but-first-you-need-to-either-create-an-account-or-log-in-1

[22] http://www.theverge.com/2015/9/21/9367707/bitcoin-ponzi-scheme-operator-pleads-guilty

worth USD387 million. Karpelès later said he had found about 200,000 of the lost Bitcoins in a "cold wallet" – a storage device such as a memory stick that is not connected to other computers.[23]

As a result of this multi-million dollar embezzlement scandal, Japan passed a law regulating virtual currency in May 2016 to tackle issues of money-laundering and protect users. The new law defines a virtual currency as something with an "asset-like nature" that can be exchanged for goods and services. Digital currency exchanges must now register with the financial watchdog and verify the identity of customers opening accounts.[24]

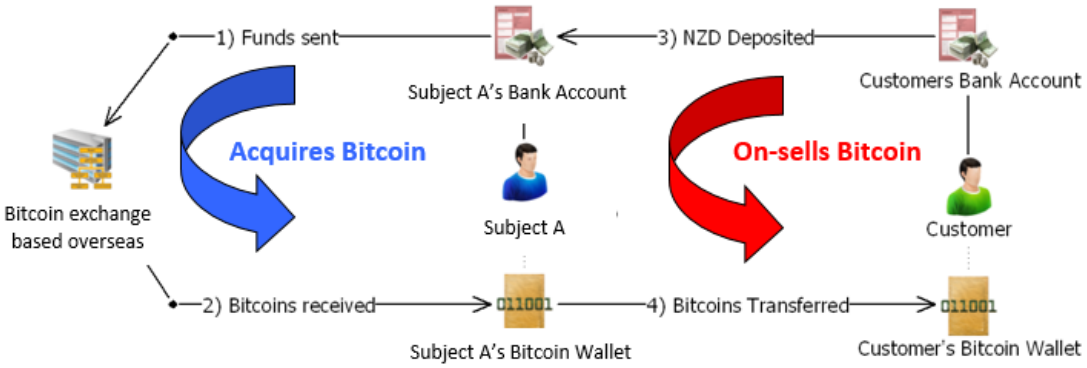
NEW ZEALAND CASE STUDY 1

Bank monitoring detected that a New Zealand resident – Subject A – had been purchasing bitcoins in roughly NZD5,000 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 anonymised 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.



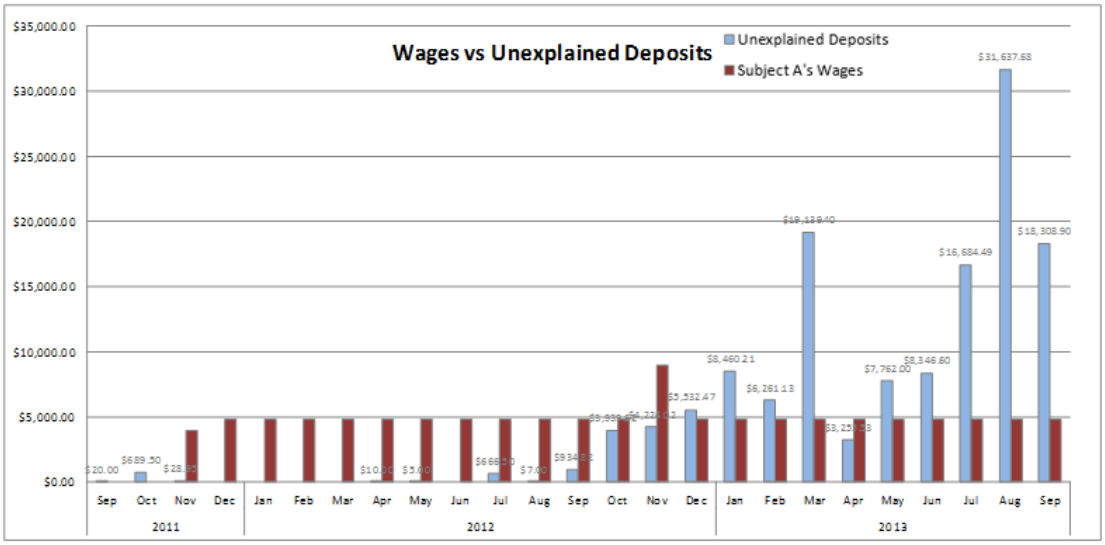
The financial analysis of Subject A's bank account records showed that since mid-2012 the account had received increasing amounts of ad hoc, unexplained deposits, to the point where throughout 2013 Subject A's income from the employer was dwarfed. A number of deposits contained reference numbers and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

[23] https://www.theguardian.com/technology/2015/aug/01/ex-boss-of-mtgox-bitcoin-exchange-arrested-in-japan-over-lost-480m

[24] http://phys.org/news/2016-05-japan-virtual-currency-bitcoin-scandal.html

Enquiries also identified that victims of fraud or ransomware attacks were using Subject A to purchase bitcoins to pay to offenders.



While more Bitcoin dealers are coming to light, the total number operating in New Zealand is likely to be very small. This means there is a "choke-point" in terms of Bitcoin transactions, allowing for efficient monitoring and targeting of offenders.

The popularity of Bitcoin shows a growing trend towards high-value online offending, while much focus is rightly placed on drugs, other offending, from simple theft to Ponzi schemes is becoming more widely reported. The ability to observe Bitcoin purchases at point of sale will become a valuable investigative tool in the future.

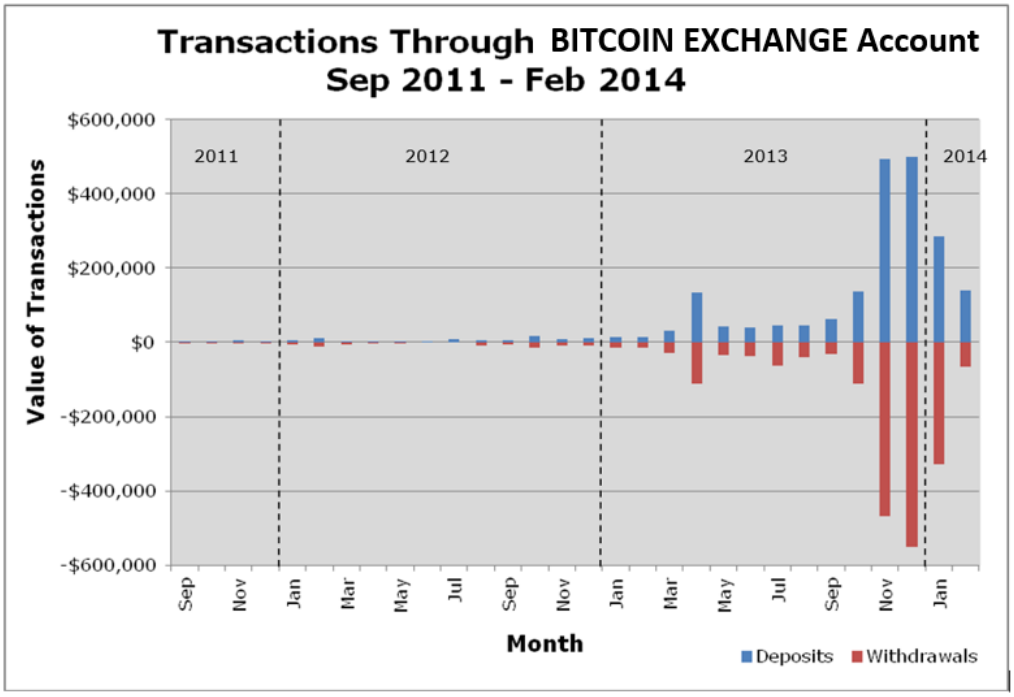
NEW ZEALAND CASE STUDY 2

In 2014, New Zealand FIU identified an account associated with a Bitcoin exchange where bitcoins were traded for New Zealand dollars at the "point-of-purchase". Subject B has a history of hacking, and is currently under investigation for a "ransomware" computer program which locks down a computer and demands payment in Bitcoin.

Subject B was running a Bitcoin business through his personal accounts with one of New Zealand's largest banks. The subject had previously come to the bank's attention for involvement in phishing scams. The subject's transactional history clearly ascertained that a large number of cash deposits had gone through his account and then were paid to third parties which appeared to indicate the buying and selling of Bitcoin.

The cash deposits were made on three separate days and at different bank branches, they were placed into Subject B's account via bank cheques.

The transaction history of the account shows substantial growth in trades over the past year, peaking in December 2013. The pattern of transactions through the Bitcoin exchange account is graphed below. Incoming funds roughly mirror outgoing funds and rapidly and rapidly increased in size, which is consistent with operating a Bitcoin exchange or as a conduit account to facilitate money laundering.



Analysis of the bank account identified 655 individual accounts transacting with the same Bitcoin exchange, as well as a large number of cash depositors. Of the 655 account holders, 13 per cent had some indication of involvement in illicit drug offending.

NEW ZEALAND CASE STUDY 3

Bitcoin-enabled offenders tend to be young, opportunistic, and have little previous criminal history. These factors mean that such offenders may operate outside traditional criminal networks, and can offend for a significant amount of time, and at a high level, without detection.

In 2013, 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 NZD130,000 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.

Annex 1

THE THREE INTERNATIONALLY ACCEPTED PHASES FOR THE MONEY LAUNDERING PROCESS:

Phase	Description	Example
Placement	Cash enters the financial system.	Proceeds of selling cannabis deposited into a bank account.
Layering	Money is involved in a number of transactions.	Money is transferred into other bank accounts that have been set up and international travel tickets are purchased.
Integration	Money is mixed with lawful funds or integrated back into the economy, with the appearance of legitimacy.	International travel tickets are cancelled, which results in a reimbursement cheque being issued to the suspect, minus cancellation fees. Money is used to buy goods, services, property or investments.

TYPOLOGIES - BASED ON THE ASIA PACIFIC GROUP ON MONEY LAUNDERING DEFINITIONS

- **WIRE TRANSFERS —** transferring proceeds of crime from one person to another via money remittance services.
- **PURCHASE OF VALUABLE COMMODITIES —** laundering proceeds of crime by purchasing valuable commodities, for example, precious metals or gems.
- **PURCHASE OF VALUABLE ASSETS —** laundering proceeds of crime by purchasing valuable assets, for example, property or vehicles.
- **SHELL COMPANIES —** registering companies which have no actual business activity. Internationally based directors/shareholders and offshore bank accounts are used to facilitate money laundering and/or terrorist financing by unverified beneficiaries. In addition, there is also the risk of exploitation of other corporate forms, particularly limited partnerships.
- **NOMINEES, TRUSTS, FAMILY MEMBERS OR THIRD PARTIES** — utilising other people to carry out transactions in order to conceal the true identity of persons controlling proceeds of crime.
- **TRADE-BASED MONEY LAUNDERING —** manipulating invoices, often in connection with international trade, by overstating the value of a shipment providing criminal entities with a paper justification to either launder proceeds of crime and/or send funds overseas to finance terrorism.
- **CANCEL CREDITS OR OVERPAYMENTS —** laundering proceeds of crime by overpaying, then requesting refund cheques for the balance.
- **ELECTRONIC TRANSFERS —** transferring proceeds of crime from one bank account to another via financial institutions.
- **CO-MINGLING —** combining proceeds of crime with legitimate business takings.
- **GATEKEEPERS/PROFESSIONAL SERVICES —** utilising "professionals" to establish seemingly legitimate business activities, for example, lawyers, accountants, brokers, company formation agents.
- **CASH DEPOSITS —** placement of cash into the financial system.
- **SMURFING —** utilising third parties or groups of people to carry out structuring.

- **CREDIT CARDS, CHEQUES, PROMISSORY NOTES —** instruments used to access funds held in a financial institution, often in another jurisdiction.
- **CASH COURIERS —** concealing the movement of currency from one jurisdiction to another using people, luggage, mail or any other mode of shipment, without declaration.
- **STRUCTURING —** separating large transactions into small transactions to avoid scrutiny and detection from financial institutions.
- **ABUSE OF NON-PROFIT ORGANISATIONS —** raising funds to finance terrorism using non-profit organisations (charities) to conceal the source and nature of funds, as well as to facilitate distribution.
- **INVESTMENT IN CAPITAL MARKETS —** laundering proceeds of crime by using any market in which securities are traded, for example, the stock and bond markets, as well as futures trading and currency speculation.
- **OTHER PAYMENT TECHNOLOGIES —** utilising emerging or new payment technologies to facilitate money laundering and/or terrorist financing.
- **UNDERGROUND BANKING/ALTERNATIVE REMITTANCE SERVICES** — transferring proceeds of crime from one person to another via informal banking mechanisms.
- **TRUSTED INSIDERS/CORRUPTION —** collusion, coercion or bribery of financial institution staff by customers, particularly high-profile individuals, for instance, government officials, business executives, celebrities or individuals known or suspected of being involved in serious crime.
- **CASH EXCHANGES —** exchanging low denomination notes for high (also known as refining) as a means to launder proceeds of crime, as well as reduce large volumes of cash obtained from serious crime.
- **CURRENCY CONVERSION —** converting one currency into another as a means to launder proceeds of crime, as well as reduce large volumes of cash obtained from serious crime.

Annex 2

FINANCIAL INTELLIGENCE UNIT

The Financial Intelligence Unit is part of the Financial Crime Group, which is made up of four Asset Recovery Units, a core administrative/analytical team and the Financial Intelligence Unit. The Financial Intelligence Unit has been operational since 1996 and part of its core functions is to receive, collate, analyse and disseminate information contained in Suspicious Transaction Reports, Suspicious Property Reports and Border Cash Reports. It also develops and produces a number of financial intelligence products, training packages and policy advice. The Financial Intelligence Unit also participates in the AML/CFT National Coordination Committee chaired by the Ministry of Justice. It is also a contributing member to international bodies such as the Egmont Group of international financial intelligence units and the Asia/Pacific Group on Money Laundering. The FIU can be contacted at: **fiu@police.govt.nz**

Annex 3

TYPOLOGY INDICATORS

GENERAL INDICATORS

These indicators are present in many of the typologies used in money laundering and terrorist financing.

- Transactions involving locations with poor AML/CFT regimes or high exposure to corruption
- Significant and/or frequent transactions in contrast to known or expected business activity
- Significant and/or frequent transactions in contrast to known employment status
- Ambiguous or inconsistent explanations as to the source and/or purpose of funds
- Where relevant, money presented in unusual condition, for example, damp, odorous or coated with substance
- Where relevant, nervous or uncooperative behaviour exhibited by employees and/or customers

WIRE TRANSFERS — transferring proceeds of crime from one person to another via money remittance services.

Possible indicators (specific)

- Significant and/or frequent cash payments for transfers
- Transfers to or from locations that have poor AML/CFT regimes or high exposure to corruption
- Transfers to high-risk countries or known tax havens
- Transfers to numerous offshore jurisdictions with no business rationale
- Multiple transfers sent to same person overseas by different people
- Same home address provided by multiple remitters
- Departure from New Zealand shortly after transferring funds
- Reluctant to provide retailer with identification details

PURCHASE OF VALUABLE COMMODITIES — laundering proceeds of crime by purchasing valuable commodities, for example, precious metals or gems.

Possible indicators (specific)

- Customers requiring safe custody arrangements with financial institution
- Significant and/or frequent cash purchases of valuable commodities
- Regular buying and selling of valuable commodities that does not make economic sense

PURCHASE OF VALUABLE ASSETS — laundering proceeds of crime by purchasing valuable assets, for example, property or vehicles.

Possible indicators (specific)

- Purchase/sale of real estate above/below market value irrespective of economic disadvantage
- Cash purchases of valuable assets with cash and/or cash deposits for valuable assets
- Low value property purchased with improvements paid for in cash before reselling
- Rapid repayment of loans/mortgages with cash or funds from an unlikely source

SHELL COMPANIES — registering New Zealand companies with internationally based directors and/or shareholders in order to open bank accounts to facilitate money laundering and/or terrorist financing by unverified beneficiaries.

Possible indicators (specific)

- Large numbers of companies registered with the same office address
- Address supplied is a "virtual office"
- Accounts/facilities opened/operated by company formation agents
- Lack of information regarding overseas directors/beneficiaries
- Complex ownership structures
- Structures where there is no apparent legitimate economic or other rational

Additional Indicators:

- The same natural person is the director of a large number of single director companies
- The same person (natural or corporate) is the shareholder of a large number of single-shareholder companies
- Use of one of a small number of New Zealand 'agents' who undertake transactions with the companies register

NOMINEES, TRUSTS, FAMILY MEMBERS OR THIRD PARTIES — utilising other people to carry out transactions in order to conceal the true identity of persons controlling proceeds of crime.

Possible indicators (specific)

- Customers using family members or third parties, including the use of children's accounts
- Transactions where third parties seem to be retaining a portion of funds, for example, "mules"
- Accounts operated by someone other than the account holder
- Many transactions conducted at various financial institutions and/or branches, in one day
- Significant and/or frequent transactions made over a short period of time

TRADE-BASED MONEY LAUNDERING — manipulating invoices, often in connection with international trade, by overstating the value of a shipment providing criminal entities with a paper justification to either launder proceeds of crime and/or send funds overseas to finance terrorism.

Possible indicators (specific)

- Invoice value greater than value of goods
- Discrepancies in domestic and foreign import/export data
- Suspicious cargo movements
- Suspicious domestic import data
- Discrepancies in information regarding the origin, description and value of the goods
- Discrepancies with tax declarations on export declarations
- Sudden increase in online auction sales by particular vendors (online auction sites)
- Unusually frequent purchases between same buyers and vendors (online auction sites)

CANCEL CREDITS OR OVERPAYMENTS — laundering proceeds of crime by overpaying, then requesting refund cheques for the balance.

Possible indicators (specific)

- Casino gaming machines loaded with cash, credits cancelled and a refund cheque requested

- Casino chips purchased, followed by limited or no gambling, then a refund cheque requested
- Frequent cheque deposits issued by casinos
- Significant and/or frequent payments to utility companies, for example, electricity providers
- Frequent cheque deposits issued by utility companies, for example, electricity providers
- Significant and/or frequent payments for purchases from online auction sites
- Frequent personal cheque deposits issued by third parties

ELECTRONIC TRANSFERS — transferring proceeds of crime from one bank account to another via financial institutions.

Possible indicators (specific)

- Transfers to or from locations that have poor AML/CFT regimes or high exposure to corruption
- Transfers involving accounts located in high-risk countries or known tax havens
- Transfers to offshore jurisdictions with no business rationale
- Multiple transfers sent to same person overseas by different people
- Departure from New Zealand shortly after transferring funds
- Transfers of funds between various accounts that show no economic sense (i.e. multiple transfers incurring bank fees where one single transfer would have been sufficient)

CO-MINGLING — combining proceeds of crime with legitimate business takings.

Possible indicators (specific)

- Significant and/or frequent cash deposits when business has EFTPOS facilities
- Large number of accounts held by a customer with the same financial institution
- Accounts operated by someone other than the account holder
- Merging businesses to create layers
- Complex ownership structures
- Regular use of third party accounts

GATEKEEPERS/PROFESSIONAL SERVICES — utilising "professionals" to establish seemingly legitimate business activities, for example, lawyers, accountants, brokers, company formation agents.

Possible indicators (specific)

- Accounts and/or facilities opened and/or operated by company formation agents
- Gatekeepers that appear to have full control
- Known or suspected corrupt professionals offering services to criminal entities
- Accounts operated by someone other than the account holder

CASH DEPOSITS — placement of cash into the financial system.

Possible indicators (specific)

- Large cash deposits followed immediately by withdrawals or electronic transfers

SMURFING — utilising third parties or groups of people to carry out structuring.

Possible indicators (specific)

- Third parties conducting numerous transactions on behalf of other people
- Many transactions conducted at various financial institutions and/or branches, in one day
- Accounts operated by someone other than the account holder

CREDIT CARDS, CHEQUES, PROMISSORY NOTES — instruments used to access funds held in a financial institution, often in another jurisdiction.

Possible indicators (specific)

- Frequent cheque deposits in contrast to known or expected business activity
- Multiple cash advances on credit card facilities
- Credit cards with large credit balances
- Transactions inconsistent with intended purpose of facility

CASH COURIERS — concealing the movement of currency from one jurisdiction to another using people, luggage, mail or any other mode of shipment, without declaration.

Possible indicators (specific)

- Transactions involving locations with poor AML/CFT regimes or high exposure to corruption
- Customers originating from locations with poor AML/CFT regimes/high exposure to corruption
- Significant and/or frequent cash deposits made over a short period of time
- Significant and/or frequent currency exchanges made over a short period of time

STRUCTURING — separating large transactions into small transactions to avoid scrutiny and detection from financial institutions.

Possible indicators (specific)

- Many transactions conducted at various financial institutions and/or branches, in one day
- Small/frequent cash deposits, withdrawals, electronic transfers made over a short time period
- Multiple low value domestic or international transfers

ABUSE OF NON-PROFIT ORGANISATIONS — raising funds to finance terrorism using non-profit organisations (charities) to conceal the source and nature of funds, as well as to facilitate distribution.

Possible indicators (specific)

- Known or suspected criminal entities establishing trust or bank accounts under charity names
- Transfers to or from locations that have poor AML/CFT regimes or high exposure to corruption
- Transfers involving accounts located in high-risk countries or known tax havens
- Transfers to numerous offshore jurisdictions with no business rationale
- Entities that use third parties to distribute funds or have weak financial governance mechanisms

INVESTMENT IN CAPITAL MARKETS — laundering proceeds of crime by using any market in which securities are traded, for example, the stock and bond markets, as well as futures trading and currency speculation.

Possible indicators (specific)

- Securities accounts opened to trade in shares of only one listed company
- Transaction patterns resemble a form of market manipulation, for example, insider trading
- Unusual settlements, for example, cheques requested for no apparent reason, to third parties
- Funds deposited into stockbroker's account followed immediately by requests for repayment
- Limited or no securities transactions recorded before settlement requested

OTHER PAYMENT TECHNOLOGIES — utilising emerging or new payment technologies to facilitate money laundering and/or terrorist financing.

Possible indicators (specific)

- Excessive use of stored value cards
- Significant and/or frequent transactions using mobile telephone services

UNDERGROUND BANKING/ALTERNATIVE REMITTANCE SERVICES — transferring proceeds of crime from one person to another via informal banking mechanisms.

Possible indicators (specific)

- Significant and/or frequent cash payments for transfers
- Cash volumes and transfers in excess of average income of migrant account holders
- Transfers to or from locations that have poor AML/CFT regimes or high exposure to corruption
- Transfers involving accounts located in high-risk countries or known tax havens
- Transfers to countries that are not destination countries or usual remittance corridors
- Large transfers from accounts to potential cash pooling accounts
- Significant and/or frequent transfers recorded informally using unconventional book-keeping
- Significant and/or frequent transfers requested by unknown or intermittent customers
- Numerous deposits to one account followed by numerous payments made to various people

TRUSTED INSIDERS/CORRUPTION — collusion, coercion or bribery of financial institution staff by customers, particularly high-profile individuals, for instance, government officials, business executives, celebrities or individuals known or suspected of being involved in serious crime.

Possible indicators (specific)

- Customers regularly targeting the same employees
- Employees relaxing standard AML/CFT procedures to facilitate transactions
- Employees exhibiting sudden wealth and/or assets in contrast to remuneration
- Employees avoiding taking annual leave
- Sudden improvement in employee's sales performance
- Employees adopting undue levels of secrecy with transactions

- Customers regularly targeting young and/or inexperienced employees

CASH EXCHANGES — exchanging low denomination notes for high (also known as refining) as a means to launder proceeds of crime, as well as reduce large volumes of cash obtained from serious crime.

Possible indicators (specific)

- Significant and/or frequent cash exchanges from small to large denominations (refining)

CURRENCY CONVERSION — converting one currency into another as a means to launder proceeds of crime, as well as reduce large volumes of cash obtained from serious crime.

Current impact on New Zealand assessed as:

Possible indicators (specific)

- Significant and/or frequent New Zealand or foreign currency exchanges
- Opening of foreign currency accounts with no apparent business or economic purpose