MALAYSIA FINANCIAL CRIME
PREVENTION CONFERENCE 2021

Cryptocurrencies in Digital Economy :

Digital Crime Opportunity – What Needs To Be Done

A Collection of Presentations Summary

EDITORS

Sharifah Nurul Asyikin Binti Syed Abdullah & Sarah Khadijah Taylor
Digital Forensics Department, CyberSecurity Malaysia
January, 2022

EVENT ORGANIZED BY:

CyberSecurity MALAYSIA

DISCLAIMER STATEMENT

FULL CITATION

Sharifah Nurul Asyikin Syed Abdullah and Sarah Khadijah Taylor, Cryptocurrencies in Digital Economy : Digital Crime Opportunity – What Needs to Be Done ? A Collection of Presentations Summary (Putrajaya, 2022) <https://sites.google.com/view/mfcpc 2021 /report>.

FULL EVENT AGENDA & SPEAKERS' SLIDES:
https://sites.google.com/view/mfcpc2021/

CONTENT

Overview

Malaysia Financial Crime Prevention Conference 2021 (MFCPC'21) was a conference organized by National Anti-Financial Crime Centre (NFCC) and CyberSecurity Malaysia (CSM), with the objective of creating awareness on cryptocurrencies investigation to law enforcement officers and regulators. Both parties have entered into a Memorandum of Cooperation (MoC) on 27 October 2021 to join effort in mitigating financial crime via mobilizing of knowledge, expertise, and shared experiences of both parties. Cooperation in the aspects of cybersecurity, data analytics and financial technology are among the main fields of focus for both agencies. The MFCPC'21 was conducted from 15 to 17 November 2021 at The Everly Hotel, Putrajaya, attended by 80 officers from 24 agencies in Malaysia.

The emergence of cryptocurrencies a decade ago has challenged the investigation and prosecution of financial crime case. While they have the potential to benefit consumers and investors, they can also be abused by bad actors, posing economic risks to the nation and to the public. The characteristic of cryptocurrencies; being pseudo-anonymous and decentralized, has attracted the criminals to exploit them as a means of committing financial crime. Cryptocurrencies have been used as medium for money laundering, tax evasion and illicit financing [1,2,3]

In view of the increasing growth of cryptocurrencies adoption in Malaysia, MFCPC'21 was introduced with introductory theme entitled "Cryptocurrencies in Digital Economy: Digital Crime Opportunity – What Needs to Be Done?". The conference intended to discuss the use of cryptocurrencies in criminal world, the impact to the digital economy, and ways to mitigate the crime. The conference aimed to tackle these issues from holistic view - investigation, prosecution and from the policy point of view.

The detail of the event is available on this website: https://sites.google.com/view/mfcpc2021/

[1] 'Guidelines for the Seizure and Sale of Virtual Assets' (Singapore: INTERPOL Innovation Centre, 2020), pp. 1–29.
[2] 'Guidance on Financial Investigations Involving Virtual Assets' (Financial Action Task Force(FATF), 2019).
[3] 'The 2020 State of Crypto Crime', Chainalysis, 2020.

Welcoming Remark

Digital Economy: Challenges and Opportunities

YBhg. Dato' Ts. Dr. Haji Amirudin Abdul WahabFASC
Chief Executive Officer (CEO)
CyberSecurity Malaysia

Keypoints:

1. Digital economy inclusion resulted in higher economic results, increase global competitiveness, develop new markets and in turn increase the prosperity of the Rakyat
2. However, Malaysia digital economy needs to be safeguard from cybercriminals
3. The nature of cryptocurrency – pseudo-anonymous, decentralized and fast settlement; provides opportunity to cybercriminal to conduct money laundering, tax evasion and illicit financing
4. To address this challenge, a concentrated effort and collaboration involving enforcement, regulatory and technical agencies are needed to counter measure the criminal activities.
5. MFCPC'21 is aimed to be the platform to open the collaboration among various agencies

The increased use of digital technology nowadays in the wake of the COVID-19 pandemic has led to the occurrence of various cybercrimes across the country. This is evident through the statistics released by the PDRM, where the total loss of Malaysian families as a result of cybercrime since 2017 until now is RM2.23 billion.

The impact of the use of technology provides the benefits of 'digital economy inclusion' for Malaysian families. By leveraging on the digital economy, the country is able to achieve higher economic results, increase global competitiveness, develop new markets and in turn increase the prosperity of the people together.

The use of digital technology, however, has also caused the modus operandi of criminals to become increasingly complex. Criminals now use advanced technologies such as encryption, cloud technology, artificial intelligence and, most recently, cryptocurrency, to avoid detection.

Cryptocurrency, in relation to the MFCPC'21 theme, is pseudo-anonymous and not regulated by a central body (decentralized). Its unique privacy model, where the identities of recipients and senders are not recorded in the ledger (the blockchain) leads to various types of risks for consumers. Meanwhile, monitoring and surveillance on the cryptocurrency market are very difficult to implement because the technology is designed to stand on its own without the need for a centralized body to manage it.

In addition, it was also developed so that the transfer of funds could take place between two entities without intermediaries and across borders in a blink of an eye. Transactions using Ether, for example, can be executed between two countries across the continents in just 1 to 2 minutes.

From the aspect of consumerism, the cryptowallet providers are prone to a cyber-attack. This can be seen when well-known Digital Asset Exchanges(DAX) such as KuCoin, UpBit and BitFinex have been hacked and caused users to suffer losses reaching billions of ringgit. Assets that have been lost are difficult to get back, because, unlike conventional financial system where losses are covered by insurance; cryptocurrency is not covered by any insurance.

The specific features of this cryptocurrency have attracted criminals to use it to carry out criminal activities such as financing terrorism, money laundering and tax evasion.

To address this challenge, a concentrated effort involving enforcement, regulatory and technical agencies are needed to counter measure the criminal activities. This in turn can ensure the safety and prosperity of the digital economy in Malaysia, and hence, benefitted the Rakyat in long terms.

Keynote Speech:

Financial Crime Enforcement and Prevention: Challenges and Effective Action Plans

YBhg. Tan Sri Abu Kassim bin Mohamed
Chairman of Advisory Board,
National Anti-Financial Crime Centre (NFCC)

Keypoints:

1. NFCC aspires to become the Centre of Excellence in combating financial crime
2. Strong collaboration between various law enforcement agencies and subject matter experts is needed to address the challenge
3. Officers conducting investigation and prosecution need to be equipped with knowledge and skills of emerging financial crime trends

YBhg. Tan Sri Abu Kassim highlighted the National Financial Crime Prevention Strategic Plan 2021-2024 is to make the NFCC a Centre of Excellence in combating financial crime and to effectively reduce the threat of financial crime.

To achieve this aspiration, the NFCC and law enforcement agencies should work together to enhance capabilities in the early detection, sharing intelligence information, conducting joint analysis to identify emerging risks as well as agility in addressing those risks. This will enable integrated action and the implementation of policies or preventive efforts to reduce the negative effects that will arise from these risks.

In line with these efforts, it is imperative that enforcement agencies and governments are equipped with knowledge of emerging financial crime trends. Therefore, YBhg. Tan Sri Abu Kassim emphasized and welcomed the efforts of the NFCC and CyberSecurity Malaysia in organizing the MFCPC 2021 Conference and support the initiative towards the establishment of the MFCPC Working Committee to plan and implement the MFCPC conference in the coming year.

This year's theme is about cryptocurrencies which is a challenge to law enforcement agencies. Cryptocurrencies are often associated with financial crime as well as cybercrime. While cryptocurrencies offer certain conveniences to its users, they also have some features that are attractive to criminals. Among them are volatile prices and difficulty in tracking the funds. Yet, despite the challenges, there are ways and strategies that can address the issues and risks of the investigation. By strengthening knowledge and technical skills, as well as strong collaboration with subject matter experts such as CyberSecurity Malaysia, the issues and risks posed by cryptocurrencies crimes can be addressed effectively and impactfully.

Presentation #1

Fundamental of Cryptocurrency

Ts. Sarah Khadijah Taylor MSc, ISLA, CCFI
Manager, Strategic Planning,
Digital Forensics Department,
CyberSecurity Malaysia (CSM)

Keypoints:

1. Cryptocurrencies are designed to hide the identity of the sender and receiver
2. Unlike investigation on fiat currency where banks can be contacted to freeze account, cryptocurrencies do not have a centralized entity that can be contacted.
3. If suspect is using hosted cryptowallet like Binance, Luno and Coinbase, investigators could contact these exchangers to freeze the account and get suspect information such as names, address and transaction records.
4. But if suspect is using unhosted wallet like Atomic Wallet, Coinomi and Exodus; then suspect information will not be available unless the device installed with the wallet is seized and analyzed.

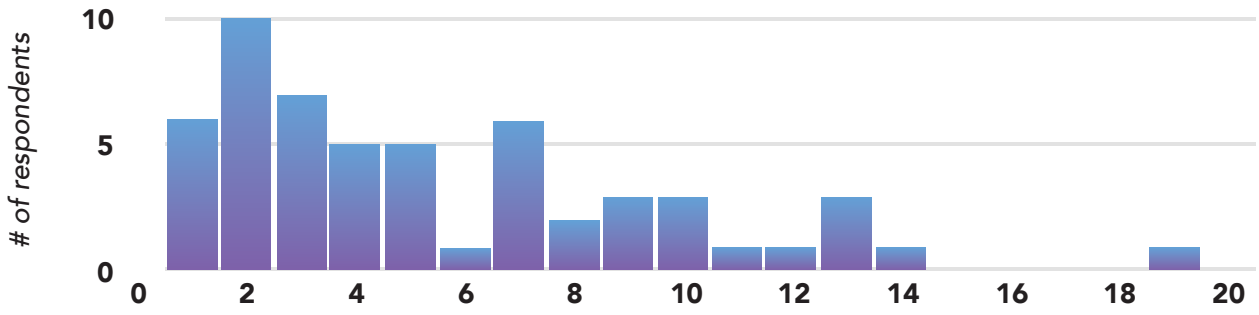
A short introductory course on the fundamental of cryptocurrency was conducted by Sarah Khadijah Taylor from CyberSecurity Malaysia to all MFCPC'21 participants. The half day course was aimed at delivering a baseline knowledge to all law enforcements officers and regulators on how cryptocurrency works. In this session, the concept of cryptowallets, blockchain and cryptomining were introduced to the participants.

To conduct transaction, both sender and receiver must have a cryptowallets. Cryptowallets are apps that user can installed on device such as Facebook apps. Upon sending a Bitcoin, the transaction record will be temporarily stored in memory pool, or better known as mempool. Cryptominer will pick up this transaction record and validate it, before bundling it together with other records in a block. This block will then be appended into the blockchain. Once this process is completed, only then receiver will receive the Bitcoin. The whole process takes about 10 minutes to 30 minutes.

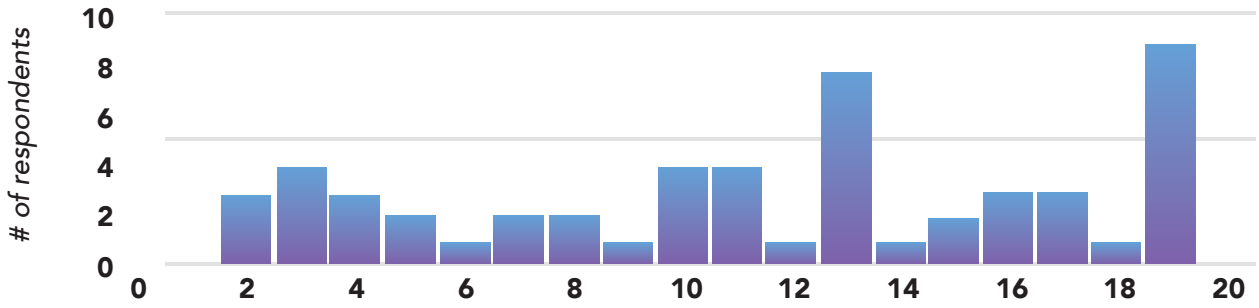
Cryptocurrencies utilize blockchain to store data. With blockchain, data is secured using cryptographic, hence the data cannot be edited. The validation and settlement of transaction is done by the cryptominers using peer to peer network, which does not involve a centralized authority. Because of this, cryptocurrency is also known as decentralized system. Cryptocurrencies are also designed to hide the identity of the sender and receiver, which makes investigation really challenging due to anonymous entities. However, if the suspect is using

hosted cryptowallet like Binance, Luno and Coinbase, investigators could contact these exchangers to get suspect information such as names, address and transaction records.

The purpose of the training was to increase law enforcement officers and regulatory understanding on basic concept of cryptocurrency. Based on the assessment result shown in Figure 1, the Masterclass has achieved its objective.



Masterclass pre-assessment test result. Most of participants scores were below than average mark (average mark: 10)



Masterclass post-assessment test result. Most of participants scores were above than average mark (average mark: 10)

Figure 1. Score results on Fundamental of Cryptocurrencies, before and after the training course. Result shows scores increased significantly after the class, depicting the increased in understanding among Law Enforcement officers and regulators

Presentation #2

Fundamental of Cryptocurrency Investigation

DSP Suhairon Bin Abdullah
Head, Cryptocurrencies Investigation Unit,
Commercial Crime Investigation Department(CCID),
Polis DiRaja Malaysia(PDRM)

Keypoints:

1. A dedicated Cryptocurrency Investigation Unit was established under the CCID to specifically handle the case
2. Cryptocurrencies crime can fall under several Acts, such as the Capital Market and Services Act 2007, Penal Code (Act 574), Criminal Procedure Code (Act 593) and Computer Crime Act (Act 563)
3. Types of crime investigated were fraud, inexistence investment, crypto wallet hacking, crypto mining scam, ransomware, Initial Coin Offering (ICO) Scam and other crimes such as steal, theft, kidnapping and murder

PDRM has taken an active measure to investigate cryptocurrency crime by creating a dedicated Cryptocurrency Investigation Unit. It was established under the Commercial Crime Investigation Department(CCID) to specifically handle the case, and total staff that they currently have is 17. The unit was divided into two zones, Zone 1 covers cases in Kuala Lumpur, Penang, Negeri Sembilan, Kedah, Perak and Sabah; while Zone 2 covers cases in Selangor, Johor, Kelantan, Terengganu, Pahang, Sarawak and Perlis.

In terms of cases, reported losses to cryptocurrencies crime related case in year 2020 was RM 68.85 million, while losses in 2021 up until October was RM 34.4 million, which amounting to RM103.25 million in just 2 years. For both years, the high number of cases reported were in Selangor, Kuala Lumpur and Sarawak, as shown in Figure 2.

In terms of Act to prosecute case, DSP Suhairon explained that cryptocurrencies crime can fall under several Acts, such as the Capital Market and Services Act 2007, Penal Code (Act 574), Criminal Procedure Code (Act 593) and Computer Crime Act (Act 563). Amongst the type of cryptocurrencies crimes investigated by the Unit are fraud, inexistence investment, crypto wallet hacking, crypto mining scam, ransomware, Initial Coin Offering (ICO) Scam and other crimes such as steal, theft, kidnapping and murder.

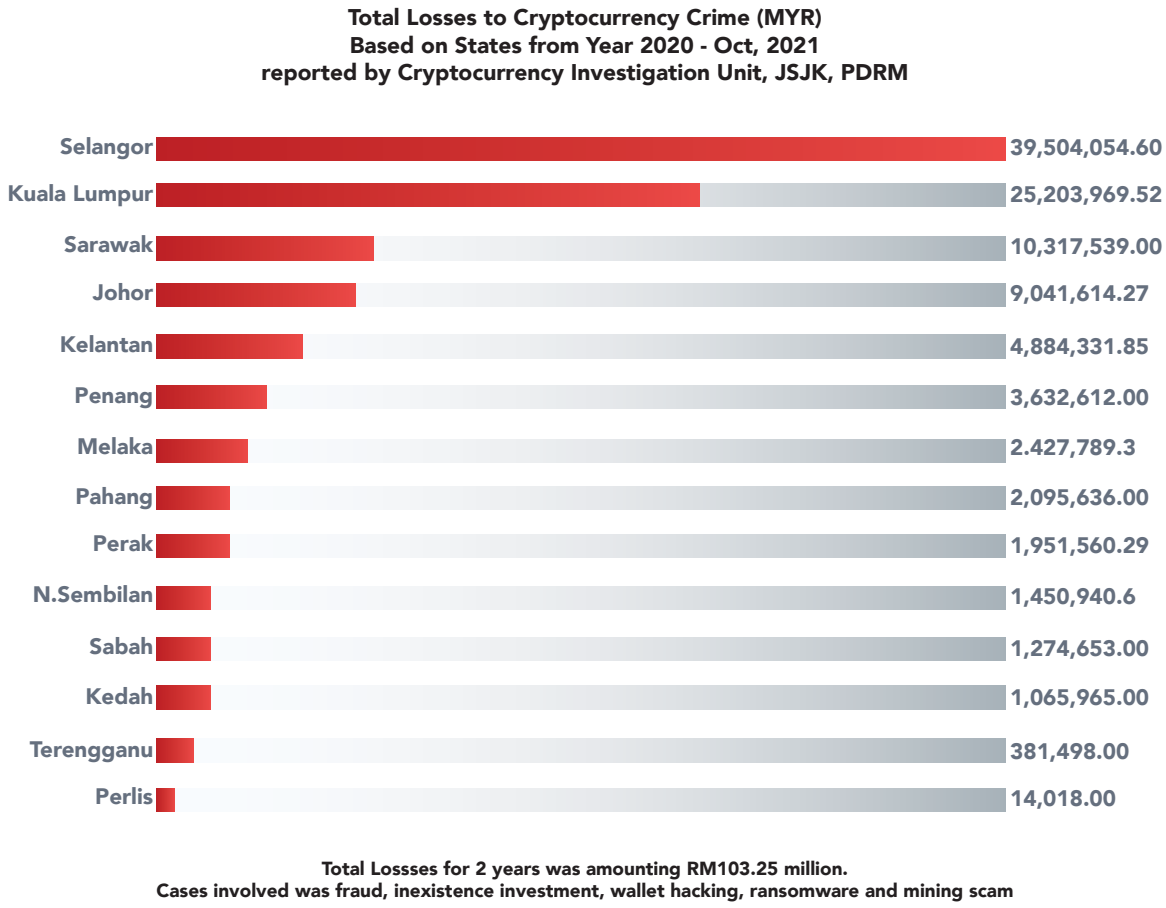


Figure 2. Reported losses from year 2020 to Oct,2021 by Cryptocurrency Investigation Unit, JSJK, PDRM

Presentation #3

A Case Study of Popular P2P Digital Asset Exchanges in Malaysia

Mr Lim Boon Beow
Bank Negara Malaysia seconded in
National Anti-Financial Crime Centre(NFCC)

Keypoints:

1. Analysis on LocalBitcoin cryptocurrency platform discovered staggering amount of local trading volume – RM880million between 2012 to 2019 – with unknown motives
2. Total trading volume for the top 30 LocalBitcoin traders alone amounting to RM347 million
3. Analysis on another popular platform, Remitano, discovered total of trading volumes for just 9 traders were RM400 million
4. Analysis is challenging because of laborious work, unknown traders identity and motives, as well as cross border issue
5. Speaker highlighted the need to have various tracing and analysis tools

There are a lot of cryptocurrencies trading platforms available to Malaysian such as Coinbase, Kucoin, FTX, LocalBitcoin, Remitano and Binance. In the presentation, Mr Lim has focused on one of the popular platform, the LocalBitcoin, a company registered in Finland.

LocalBitcoin is a peer to peer services, where it meets seller and buyer together. Using the platform, buyer can either deposited MYR using online banking such as Maybank and CIMB to the seller; use cash deposit machine to deposit MYR to seller; or buyer can arrange a meeting with seller to purchase the cryptocurrency.

This platform imposed Know-Your-Customer(KYC) rule since 2016, and user of the platform is required to upload a selfie, IC or driving license, validated email, phone number and real name. If all data is satisfactory, then only can user creates an account.

NFCC has received a total of 67,524 rows of data, involving unique user accounts, from LocalBitcoin from year 2012 to 2019. A total of nearly RM880 million has been traded by Malaysian user using that platform. Based on data analysis, total trading volume for the top 30 traders alone amounting to RM347 million. The amount was 40% from the accumulated total trading volume of 67,524 traders.

Comparison analysis of matching user account for the top 30 traders were also conducted with other popular platform such as Remitano. The comparison analysis has resulted in 9 matches, which showcases that 9 traders are active on both platforms. Further study discovered that total trading volume on Remitano platform for just 9 traders was RM400 millions, which 26% more than the top 30 traders on LocalBitcoins.

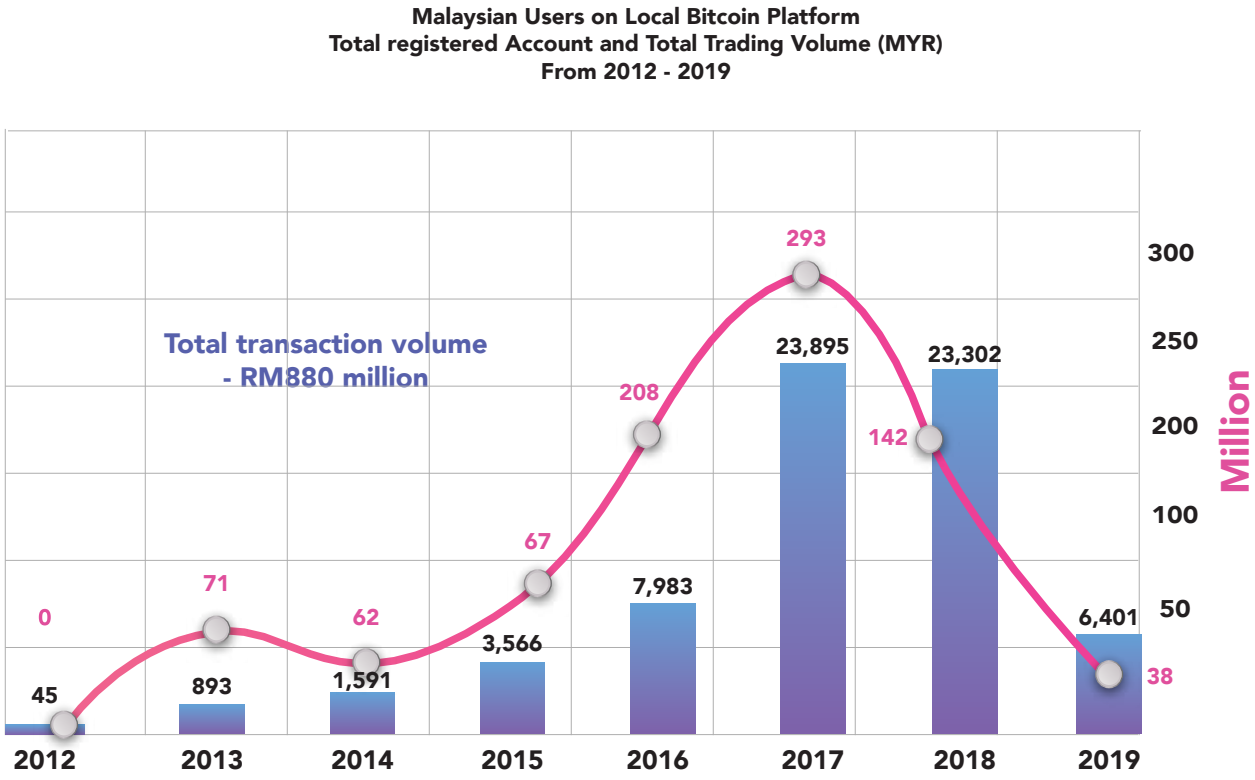


Figure 3. Total Registered Account and Total Trading Volume (MYR) year 2012 – 2019 from LocalBitcoin platform for Malaysian User

The findings based on the analysis are concluded as following:

1. Analysis is still ongoing, but the existing findings were eye opener especially on total local trading volume and the manner of the transactions
2. Buying and selling of cryptocurrencies at your own risk are not an offence under the law, however, whether the transactions were related to criminal activities are unknown, until further investigation can clarify this issue.

On the other hand, investigating cryptocurrencies are not an easy task and the following are the challenges:

1. Cryptocurrency money trail and tracing is possible to be conducted, however, it often involves laborious blockchain analysis with unknown recipients/senders information and unknown purpose of transactions
2. When a particular transaction was originated from or sent to a cryptocurrency exchanger, tracing becomes difficult because of address mixing
3. Lack of access to trader's information as information are held by cross border exchangers

Presentation #4

Cryptocurrency Transaction Analysis

ASP Nur Adli Bin Md Saari
Investigator, Cryptocurrencies Investigation Unit,
Commercial Crime Investigation Department(CCID),
Polis DiRaja Malaysia(PDRM)

Keypoints:

1. Tools are crucial in conducting tracing and transaction analysis
2. By using Chainalysis Reactor, PDRM was able to trace the exchanger that the criminal used, and further action was then taken by contacting the exchanger to request for suspect information
3. However these tools are extremely expensive, and suggestions have been made to MFCPC'21 to create pool resources.

There are several tools available for cryptocurrency transaction analysis, however the one that PDRM owned at the moment is Chainalysis Reactor. The tools was sponsored for a year by United Nations Office on Drugs and Crime (UNODC). By using the tool, PDRM was able to trace the exchanger that the criminal used, and further action was taken by contacting the exchanger and request for suspect information. However these tools are extremely expensive, and suggestions have been made to MFCPC'21 to use pool resources.

ASP Nur Adli proceeded to demonstrate few cases involving cryptocurrencies investigation that handled by PDRM. Following the demonstrations, limitations and challenges were then elaborated. Table 1 shows the total request of tracing and the digital asset exchanger involved in the case.

PDRM had also share the challenges and limitation on conducting the tracing, listed as following:

1. Lack of officers to conduct analysis of cryptocurrency transactions. Currently there are 11,000 types of cryptocurrencies, hence dedicated officers are really needed in this area
2. Lack of local expertise for capacity building and discussion
3. The need for a dedicated lab with strong, unfiltered internet connection to conduct tracing and intelligence gathering
4. Cross border jurisdiction issues, where in some countries cryptocurrencies have yet to be regulated
5. Rapid development of cryptocurrency technology - DeFi, Atomic Swap and NFT

Year	Total Request	Crytocurrency Type	Digital Asset Exchanger Involved
2018	2	Bitcoin (BTC),Ethereum(ETH), Cardano(ADA)	Binance, Bitfinex, Bittrex
2019	13	Bitcoin (BTC), Ethereum(ETH), Litecoin(LTC)	Binance, Huobi, LocalBitcoin
2020	14	Bitcoin (BTC), Ethereum(ETH), Tether(USDT) BitcoinCash (BCH)	Binance,Kucoin,Paxful,CEX.IO, Remitano, Luno,LocalBitcoin,BitGo
2021	50	Bitcoin (BTC), Ethereum(ETH), Tether(USDT) Monero(XMR)	Binance, Huobi, Luno, CEX.IO, IndoDax, Remitano, LocalBitcoin, Blockchain.Com

Table 1. Details of cryptocurrency transactions analysis conducted by PDRM

Presentation #5

Cryptocurrency Investigation: Trend & Comparative Study

Ts. Sarah Khadijah Taylor MSc, ISLA, CCFI
Manager, Strategic Planning, Digital Forensics Department,
CyberSecurity Malaysia (CSM)

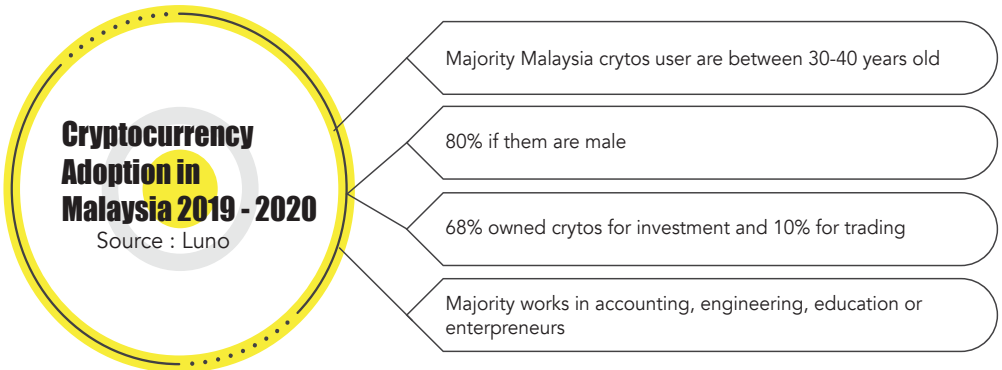
Keypoints:

1. Cryptocurrency adoption is shockingly high in Malaysia
2. Cryptocurrency investigation readiness, however, is still low among investigation officers, prosecutors and policy makers
3. The way forward is to (1) intensify training program; (2) create pool resources for tools; and (3) to create policy & SOP at national level

Cryptocurrency adoption in Malaysia is high and this is evident based on these statistics:

- Luno reported RM827 millions of transactions from 2019 to 2020 have been conducted by Malaysian users.
- LocalBitcoin data of Malaysian users shows total transaction volume from year 2012 to 2019 is reaching RM880 million, with total of transaction volume from the top 30 traders reaches RM350 million
- Sampling of data from Remitano platform for just 9 traders shows total transaction volume of RM400 millions
- Statistic from PDRM shows total losses due to cryptocurrency crime from 2020 to Oct,2021 is RM103.25 million

Cryptocurrency, undeniably, is the new source of wealth generation and can boost self-empowerment to user. Thus, if rightfully used, cryptocurrency can become a medium to elevate Malaysia digital economy. But with the high transaction volume seen from the statistics, one might question the motives behind the strong volumes. According to global study, cryptocurrencies are used in many crimes; money laundering, tax evasion and illicit financing (see section Overview). The investigation and prosecution trend in Malaysia, however, seems not moving as fast as the adoption rate, as currently only PDRM is seen to be actively investigate such cases.



A survey was then conducted among participants of MFCPC'21. 48 officers from 24 agencies of law enforcement and regulation have participated in the survey. The objective of the survey is to understand the state of readiness for cryptocurrency investigation in terms of training, tools and SOP. The results are listed as following and depicted in Figure 5:

The result of cryptocurency investigation readliness are as follows:

- Training – 60% said they have not attended training, while 40% said yes
- Tools – 63% said they did not have tools, while 12% said they have it, while 26% were neutral on this
- SOP – 74% said they did not have SOP in place, while 9% said yes, while 17% were neutral on this
- The neutral responses could be translated as the agencies that the respondents work with did not deal with financial related crime at all, or that the respondents came from regulatory background where tools and SOPs were not needed to perform the work

The result of the survey suggested that cryptocurrency investigation readiness is still low among investigation officers, prosecutors and policy makers.

A comparative study was conducted earlier this year to understand investigation process from two(2) countries; United States of America(USA)[4] and Australia[5]. The process is summarized as follows:

1. Cryptocurrency discovered at crime scene from un-hosted wallet will be seized
2. Process of seizing is by transferring the crypto into Government-controlled wallet
3. For hosted wallet, a legal documentation will be served to the exchanges to freeze suspect's account

The session concluded with the following suggestions as to increase the level of readiness:

1. To intensify training program to all Law Enforcement Agencies and Regulators
2. To have more analysis tools to uncover illicit transactions. However, they are expensive. Solution: to have pool resource
3. To develop policy and SOP at national level on the Government-controlled wallet as well as asset recovery and forfeiture

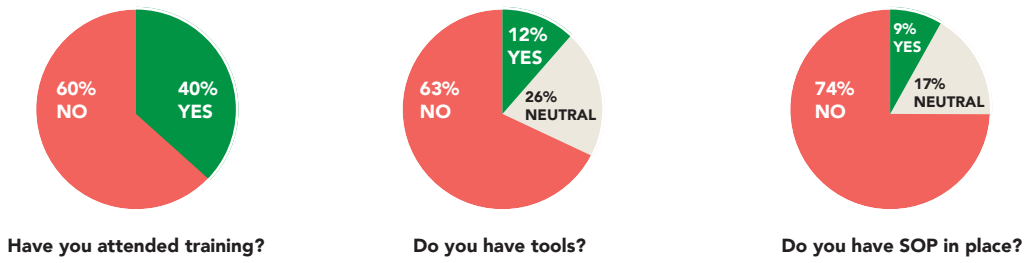


Figure 5. Result of cryptocurrency investigation readiness survey

[4] 'Sarah Khadijah Taylor, *Report on Crytocurrencies Investigation #1: A US Perspective* (Cyberjaya, 2021)
[5] 'Sharifah Nurul Asyikin Syed Abdullah, *Report On Cryptocurrencies Investigation #2: An Australia Perspective* (Cyberjaya, 2021)

Presentation #6

Cryptocurrencies – A Legal Perspective

Dato' Seri Rajan Navaratnam
Consultant, Litigation & Dispute Resolution
Shahrizat Rashid & Lee Advocates & Solicitors

Keypoints:

1. The cryptocurrency market is valued at more than 3 trillion US Dollars and continues to grow. Bitcoin alone today has a market value of 742.3 billion US Dollars
2. Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (AMLATFPUA) is a very powerful Act and can used in almost any criminal situations, including for cryptocurrencies cases.
3. Steps to secure a conviction (1) Check the entry and exit points; (2) Creating a profile for the suspect; (3) Find the devices and extract the evidence; and (4) Use of experts to interpret evidence from blockchain analysis or digital wallets

Cryptocurrency is exploited by criminals to conduct various crimes, including cyber-launder, tax evasion, bribery and ransom. Cyber launder is the act of purchasing cryptocurrencies using illicit obtained money, and then is used to conduct legal businesses, creating a layer that conceals the origins of the money. Cyber-launder happens when at least one of the three phases of laundering takes place; either at the placement stage, layering stage or integration stage. Laundering cryptocurrencies via online exchanges and then converting them to cash is easier with a click of a button than laundering bags of cash.

Cryptocurrency is capable of cutting off the links between illicit proceeds and the alleged crime. This is because the trade and the exchange of cryptocurrency is based on decentralized system, which cannot be intervened by central authority, and almost impossible to be monitored. On top of that, many wallet providers and online crypto exchanges have a few Know Your Customer (KYC) regulations, makes detection of cryptocurrency difficult to trace and prosecute.

To investigate cases, there are three(3) major challenges to LEAs;

1. Geography
2. Anonymity
3. Obfuscation via mixers and tumblers

Mixers and tumblers are operators intended to conceal the cryptocurrency's source and the location by commingling the cryptocurrencies from several users. Currently, there is not laws or regulations for this operator in Malaysia, where they are liable for money laundering.

Regulators of Malaysia can, however, use the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001(AMLATFPUA) to prosecute case. This Act is an extremely powerful piece of law and as it is a comprehensive legislation, which can be used in almost any criminal situations.

**Photo copyright from thevibes.com*

To prosecute case, prosecutors can use these legislations:

1. Money laundering – AMLATFPUA
2. Unlicensed, unregistered or non-compliant exchanges – Securities Commission's Order. Additionally, these operators are considered reporting agencies under AMLATFPUA.
3. Tax evasion - Income Tax Act 1967. Additionally, this offense also comes under the list of schedule offences in AMLATPUA
4. Offence against property under the Penal Code such as Theft

Prior to prosecution, these steps are essential to secure a conviction:

1. Check the entry and exit points
2. Creating suspect's profile to help follow the money trail and ultimately recovering any assets or money.
3. Find the devices and extract the evidence using forensic analysis to reveal cryptocurrency addresses, email addresses and the wallets used to store the account information
4. Use of experts to interpret evidence from blockchain analysis

The possible defences that may be raised by the accused are as follows:

1. Whether correct legal procedures have been adopted – ie. the investigation procedures had breached existing laws and therefore the evidence is inadmissible
2. Whether the accused had actually carried out the acts
3. The possibility of unauthorized use of the account or devices via hacking or 3rd parties,
4. There has been no link or evidence to show any given communication between the accused and any brokers on a platform involving cryptocurrency transactions
5. There is sufficient due diligence conducted prior and after the transactions by the accused - therefore no indication of any wrongdoing or wrongful intention
6. The defence of good faith purchaser - the transaction was undertaken between a willing seller and willing buyer based on the reliance and representations of other 3rd parties whom the accused believed was genuine
7. Issue of jurisdiction - whether the case filed has been brought within the jurisdiction of the Malaysian courts for it may not be classified as a criminal activity overseas where the trades took place
8. Unaware that the transactions conducted by him were illegal and therefore the intention is not present

Presentation #7

Cryptocurrencies – A Regulatory Perspective

Datin Nurshuhaida Zainal Azahar
DPP, Unit Komersil dan Jenayah Siber,
Attorney General Chambers of Malaysia (AGC)

Keypoints:

1. It is important to start investigation process as fast as possible as time is of essence
2. General law such as Criminal Procedure Code(CPC), AMLATFPUA or specific laws governing Law Enforcement Agency can be used to prosecute cryptocurrency case
3. Two important factors in a cryptocurrency investigation: (1) investigation procedures are followed; and (2) the chain of evidence is intact

In cryptocurrency crimes, it is important to start investigation process as fast as possible as time is of essence. Investigators are recommended to have a criminal mind which means to think outside the box in order to be one step ahead of the perpetrators. There is no specific laws on how seized cryptocurrency/crypto wallet should be dealt with. Therefore, the enforcement agency must refer to the general laws i.e. the Criminal Procedure Code(CPC), Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001(AMLATFPUA), or specific laws governing its agency. Two (2) important factors in a cryptocurrency investigation need to be adhered to:

1. Ensure that investigation procedures are followed; and
2. Ensure the chain of evidence is intact

Investigation Officers are advised to follow criminal investigation process in investigating cryptocurrencies as depicted in Figure 6.

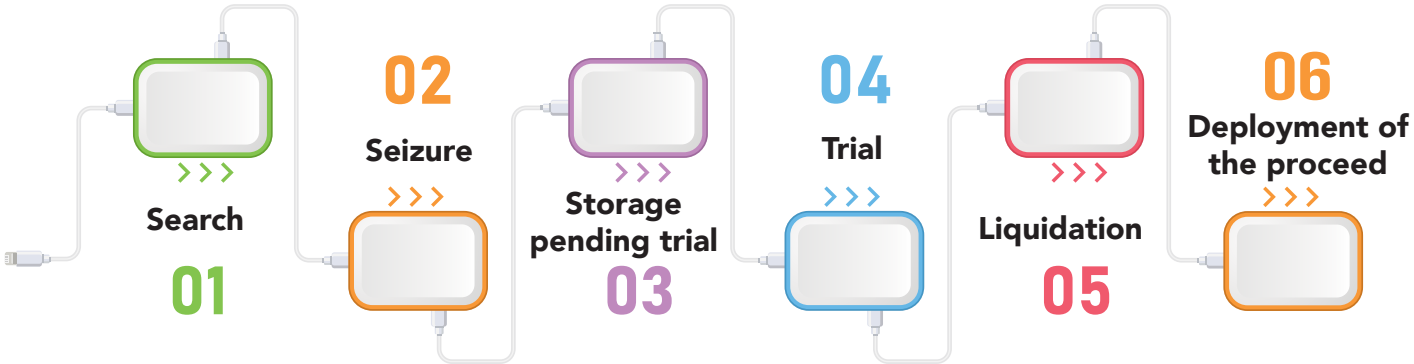


Figure 6. Criminal Investigation Process

When discover that criminal activity may involve bitcoin, Officer determines if it is possible to access the wallet by obtaining passcodes or keys. Access should be restricted to all devices that may contain that cryptocurrency only. Officer then seizes the cryptocurrencies by transferring them to the agency control-cryptowallet. The process is simplified as following:

1. If the bitcoin wallet is not encrypted, Officer has complete access (provided proper warrants have been obtained for the seizure of the device).
2. If the bitcoin wallet is encrypted, get suspect to volunteer to enter its password.
3. If immediate access to the suspect's wallet is not possible, isolate it from network.
4. Once decrypted, Officer can transfer the seized bitcoin to agency wallet.

If suspect does not offer the passwords, an admission that the suspect knows the passwords is helpful to get an order compelling the suspect to unlock the wallet, via CPC Section 116B.

Next, Prosecutor will ensure that due investigation processes are being followed by referring to the right Criminal Procedure Code (CPC). Admissibility of evidence will be taken into account by referring to the Evidence Act 1950. The next step is to check the credibility of evidence by making sure that the evidence was legally obtained and by obtaining expert evidence's report and expert witness testimony. Finally, the weight of evidence will depends on the ability of Law Enforcement Officer to completely explain the narration of crypto-trail and the result of interview with witnesses i.e. raiding officers or digital evidence analysts.

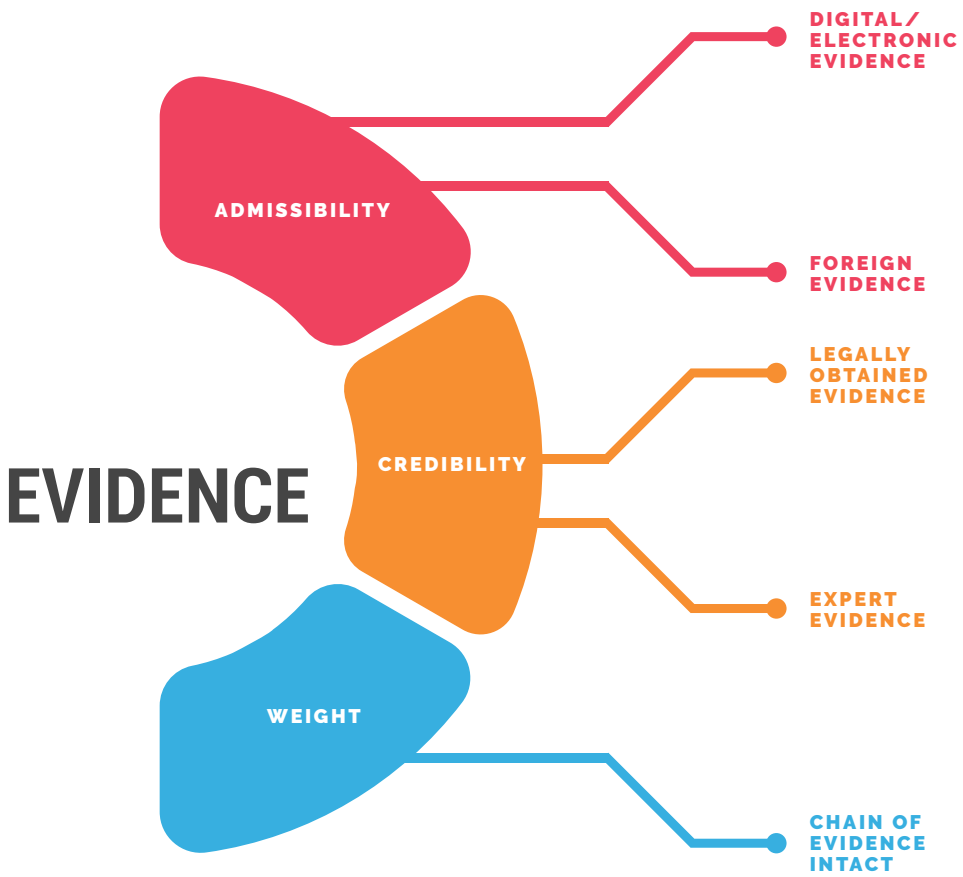


Figure 7. Deputy Public Prosecutor's Checklist

Presentation #8

Cryptocurrencies from Securities Perspective

Mr. Mohamad Nor Azizi Bin Mohd Nasir
Securities Commission (SC)

Suruhanjaya Sekuriti
Securities Commission
Malaysia

Keypoints:

1. Malaysia was among the first few countries in the region that had introduced a specific regulatory framework to facilitate the trading and offering of digital assets
2. Digital Assets are divided into two parts i.e. (1) Digital Currency such as Bitcoin; and (2) Digital Tokens such as NFT
3. In order for digital asset to be regulated in Malaysia, it must be recorded on a distributed ledger.

Malaysia was among the first few countries in the region that had introduced a specific regulatory framework to facilitate the trading and offering of digital assets. The Capital Markets & Services (Prescription of Securities) (Digital Currency and Digital Token) Order 2019 prescribes certain types of digital currency and digital token as "securities". It has come into force on 15 January 2019. Both digital currency and digital token is collectively known as Digital Asset.

The Order has stated that in order for digital asset to be regulated, it must be recorded on a distributed ledger (note: blockchain is a subset of distributed ledger). Crimes not related to the Order, such as cryptomining, does not fall under SC jurisdiction. It is because mining activity itself is a process of mining for digital asset, and not for trading or fundraising purpose.

Digital assets are divided into two categories i.e. (1) Digital Currency; and (2) Digital Tokens. Digital Tokens are further divided into three subcategories; (2.1)Exchange Token, (2.2)Utility Token and (2.3)Asset Token. The following explains the differences:

The following explains the differences between Digital Currency and Digital Token

1. Digital Currency - when it is used for payment purposes, such as Bitcoin
2. Digital Token - is a type of digital asset for fundraising purposes; and the categories are Exchange token, Utility Token and Asset Token:
   - Exchange Token - a means of exchange or value transfer
   - Utility Tokens - provide access digitally to an application or service
   - Asset Tokens - a digital representation of assets or the rights/claim to assets, like NFT

Platform operator who operates a platform for trading of digital asset is required to be registered as a Recognized Market Operator (RMO) under section 34 Capital Market and Services Act (CMSA). An issuer seeking to raise funds through Initial Exchange Offering (IEO) must comply with Guidelines on Digital Assets.

Currently, there are four (4) Digital Asset Exchanges registered with SC. The transaction values of Digital Assets trading across all four exchanges as of 2021 is RM1.5 billion, with 700,000 active accounts. Currently SC only permits five (5) digital currency to be traded using the four (4) exchanges i.e. Bitcoin, Ether, Litecoin, Bitcoin Cash and Ripple.

Presentation #9

Cryptocurrencies from the Perspective of Central Bank of Malaysia

Mr. Yip Kah Kit
Deputy Director, Central Bank of Malaysia (BNM)

BANK NEGARA MALAYSIA
CENTRAL BANK OF MALAYSIA

Keypoints:

1. Cryptocurrencies generally do not fulfil the universal characteristics of money
2. International bodies remain cautious of the risks it imposed on monetary policy, financial stability and financial integrity
3. BNM and SC each regulate specific cryptocurrencies activities to allow innovations while mitigating risks
4. BNM has no immediate plan to issue CBDC. However, it is actively scale up its internal capacity, and to date has embarked exploration on CBDC, starting with Project Dunbar

Crypto-assets such as Bitcoin generally do not fulfil the universal characteristic of money - it has no formal backing of its value, it is volatile in price, it has scalability issue and vulnerable to cyber threats. International bodies such as FATF(Financial Action Task Force), BIS(Bank for International Settlements) and FSB(Financial Stability Board) remain cautious of the crypto-assets risks.

International bodies remains coutious on cryto-assets risk, as following:

1. Monetary stability - crypto-assets may lead to substitute of domestic currency, generating adverse impact to monetary policy
2. Financial stability - vulnerabilities associated with crypto-assets such as cyber threats
3. Financial integrity - pseudo anonymous nature and consumer exploitation (Ponzi scheme & scams)

On regulations, payments matter falls under BNM purview whilst for trading, fundraising and custodian services, it falls under Securities Commission purview. For regulations on payment, crypto-assets are not legal tender in Malaysia and are not regulated payment instrument. However, for stablecoin, its arrangement must comply with BNM's requirement to ensure financial stability and financial integrity.

On Central Bank Digital Currency(CBDC), it differs from crypto-assets as it is a legal tender and backed by claim on the central bank; whereas crypto-assets are not legal tender and have no intrinsic value.

CBDC can be a tool to achieve public policy goals such as enhanced payment efficiency and promote innovations. However, risks need to be managed, ie. cyber risks.

Currently BNM has no immediate plans to issue CBDC - domestic payment systems continue to operate safely and efficiently, while monetary and financial policy tools remain effective. However, BNM is actively scale up internal capacity on CBDC. BNM has also embarked on POC of CBDC via Project Dunbar this year.

Closing Remark

Digital Economy, Digital Crime: Where Do We Go from Here?

YBhg. Dato' Seri Haji Mustafar Haji Ali
Director General ,
National Anti-Financial Crime Centre (NFCC)

Keypoints:

1. The mantra of creating the future by doing it now in combating and prevention of financial crime, need holistic, sustainable and concerted efforts and strategy. National Anti-Financial Crime Strategic Plan 2021 - 2024 is a platform in ensuring the effectiveness.
2. Knowledge and technical know how of cryptocurrencies is critical for the Law Enforcement Agencies (LEAs) and regulators. Capacity building become a significant approach.
3. NFCC and CyberSecurity Malaysia have taken the initiative to organize the MFCPC'21 to keep LEAs and regulators abreast with current and advancement of financial technology and fight against those unscrupulous parties.
4. NFCC and CyberSecutrity Malaysia are committed to provide awareness on emerging financial trends in order to empowering LEAs and regulatory in preventing as well as combating financial crime with all sectors

MFCPC'21 is an inaugural conference that aims to bring together members in the prevention of financial crime in Malaysia which consists of officials from various enforcement agencies and government departments. It is critical for these law enforcement agencies and regulators to be exposed to the knowledge of cryptocurrency, which is gaining popularity, especially among digital economic users.

The Covid-19 epidemic that hit the world has created a new norm of daily life. The implementation of strict movement control since 2020 has accelerated the adoption of technology. Along with this is the trend of consumerism that is increasingly changing to online usage more than ever before. Former YAB Prime Minister, Tan Sri Muhyiddin Yassin, recently at the Cyber Defense and Security Exhibition and Conference 2021 in June stated that the increasing trend in the use of e-commerce and online learning has opened the door to threats and risks to the exploitation of cyber criminals. Among others, cybercrime threats such as hacking, identity fraud and data breaches have caused high losses. According to PDRM statistics, a total of 4,327 police reports were made related to cybercrime in the first quarter of 2021. Meanwhile, the total number of police reports related to cybercrime was 11,875 in 2019 and 14,229 in 2020, with a loss of RM498 million in 2019 and RM413 million in 2020.

Given the seriousness of this situation, it is imperative that enforcement agencies and governments continue to keep abreast of trends in cybercrime and financial crime including the use of cryptocurrencies as intermediaries. Therefore, to support this aspiration, NFCC and CyberSecurity Malaysia took the initiative to organize this year's MFCPC'21 themed on the investigation of financial crimes involving cryptocurrencies. Hopefully, participants of this year's MFCPC Conference will be able to take advantage of the discussion topics that have been prepared and bring the knowledge gained to their respective agencies to continue their efforts to combat financial crime.

Cryptocurrencies in Digital Economy

Digital Crime Opportunity – What Needs To Be Done

A Collection of Presentations Summary

CyberSecurity MALAYSIA